Reports of Cases

OPINION OF ADVOCATE GENERAL
CAMPOS SÁNCHEZ-BORDONA
delivered on 30 March 2023 [1]

Case C-162/22

A.G.
other party:
Lietuvos Respublikos generalinė prokuratūra

(Request for a preliminary ruling from the Lietuvos vyriausiasis administracinis teismas (Supreme Administrative Court of Lithuania))

(Reference for a preliminary ruling – Telecommunications – Processing of personal data – Directive 2002/58/EC – Scope – Article 15(1) – Access to data retained by providers of electronic communications services and collected in criminal investigations – Subsequent use of data in an investigation into misconduct)

1. This reference for a preliminary ruling raises the question whether, in essence, personal data obtained in a criminal investigation may subsequently be used in disciplinary proceedings of an administrative nature against a public official.

2. The answer to that question affords the Court of Justice a further opportunity to rule on the scope of Directive 2002/58/EC, [2] on the one hand, and the scope of Directive (EU) 2016/680 [3] and Regulation (EU) 2016/679, [4] on the other.

3. As regards Directive 2002/58, the Court has delivered a consistent line of decisions concerning when and under what conditions Member States may restrict the scope of the rights and obligations established by that directive. [5]

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 on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016 L 119, p. 89).

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 leading cases in that line of decisions include, but are not limited to, the judgments of 8 April 2014, *Digital Rights Ireland and Others* (C-293/12 and C-594/12, EU:C:2014:238); of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970); 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*'); of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)* (C-746/18, EU:C:2021:152); and of 5 April 2022, *Commissioner of An Garda Síochána and Others* (C-140/20, EU:C:2022:258) ('the judgment in *Commissioner of An Garda Síochána*').

I. Legal context

A. European Union law

1. Directive 2002/58

4. Article 1 ('Scope and aim') provides:

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

2. The provisions of this Directive particularise and complement Directive 95/46/EC [6] for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.

3. This Directive shall not apply to activities which fall outside the scope of the [TFEU], such as those covered by Titles V and VI of the Treaty on European Union [(TEU)], 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.'

5. Article 5 ('Confidentiality of the communications') provides, in paragraph 1 thereof:

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

6. Article 15 ('Application of certain provisions of Directive 95/46/EC') states:

'1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. 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

[6] 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).

paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) [TEU].

…

2. The provisions of Chapter III on judicial remedies, liability and sanctions of Directive 95/46/EC shall apply with regard to national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive.

…'

2. The GDPR

7. Article 2 ('Material scope') provides:

'1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

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

(a) in the course of an activity which falls outside the scope of Union law;

…

(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.

…'

8. Article 5 ('Principles relating to processing of personal data') provides:

'1. Personal data shall be:

…

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ("purpose limitation");

…'

9. Article 6 ('Lawfulness of processing') reads as follows:

'1. Processing shall be lawful only if and to the extent that at least one of the following applies:

…

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

…

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

(a) Union law; or

(b) Member State law to which the controller is subject.

…

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

(d) the possible consequences of the intended further processing for data subjects;

…'

3. Directive 2016/680

10. Article 1 ('Subject-matter and objectives') provides, in paragraph 1 thereof:

'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, 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.'

11. Article 2 ('Scope') states, in paragraph 1 thereof:

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

12. Under Article 4 ('Principles relating to processing of personal data'):

'1. Member States shall provide for personal data to be:

…

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

…

2. Processing by the same or another controller for any of the purposes set out in Article 1(1) other than that for which the personal data are collected shall be permitted in so far as:

(a) the controller is authorised to process such personal data for such a purpose in accordance with Union or Member State law; and

(b) processing is necessary and proportionate to that other purpose in accordance with Union or Member State law.

…'

13. Article 9 ('Specific processing conditions') provides, in paragraph 1 thereof:

'Personal data collected by competent authorities for the purposes set out in Article 1(1) shall not be processed for purposes other than those set out in Article 1(1) unless such processing is authorised by Union or Member State law. Where personal data are processed for such other purposes, [the GDPR] shall apply unless the processing is carried out in an activity which falls outside the scope of Union law.'

B. National law

1. Lietuvos Respublikos elektroninių ryšių įstatymas [7]

14. Article 65(2) requires providers of electronic communications services to retain the data listed in Annex 1 to that law and, where appropriate, to make those data available to the competent authorities for use in combating serious crime. [8]

15. Under Article 77(1), providers of electronic communications services must allow the competent authorities access to information which is lawfully in their possession and is necessary, inter alia, for the prevention, detection and prosecution of criminal offences.

[7] Law of the Republic of Lithuania on electronic communications, in the version of Law No IX-2135 of 15 April 2004, as amended by Law No XIII-2172 of 6 June 2019; 'the LEC'.

[8] The data listed in that annex ('Categories of data to be protected') are those necessary to identify the source and destination of a communication, its date, time, length and type, and the location of the users' communication (including mobile communication) hardware.

16. In accordance with Article 77(4), where there is a reasoned court order or other legal basis established by law, providers of electronic communications services must make it technically possible, in particular for criminal investigation bodies and pre-trial investigation bodies, in accordance with the detailed rules laid down in criminal procedural legislation, to monitor the content of communications transmitted over electronic communications networks.

2. Lietuvos Respublikos kriminalinės žvalgybos įstatymas [9]

17. Under point 1 of Article 6(3), if the conditions laid down in the LCI are met and subject to prior authorisation from the public prosecutor's office or a court, criminal investigation bodies [10] may collect information from providers of electronic communications services.

18. Under Article 8(1) and (3), criminal investigation bodies are to act as soon as information comes to light concerning the preparation or commission of a very serious, serious or less serious criminal offence and, if the investigation reveals the existence of a criminal offence, a pre-trial investigation is to be initiated immediately.

19. Point 5 of Article 19(1) provides that information from criminal investigation operations may be used in the situations referred to in paragraphs 3 and 4 of that article and in other situations provided for by law.

20. In accordance with Article 19(3), information relating to acts having the characteristics of a corruption-related offence may be declassified, with the agreement of the public prosecutor's office, and used in the investigation of disciplinary misconduct or misconduct in office.

3. Lietuvos Respublikos baudžiamojo proceso kodeksas [11]

21. Article 154 ('Monitoring, recording and retention of information transmitted over electronic communications networks') provides, in paragraph 1 thereof, that an investigator may, by decision of an investigating judge taken at the request of the public prosecutor's office, listen to, record and store conversations transmitted over electronic communications networks if there is reason to believe that data may be obtained concerning a very serious or serious offence that is being prepared, is being committed or has already been committed, or concerning a less serious or non-serious offence.

22. Article 177 ('Non-disclosure of pre-trial investigation data') provides, in paragraph 1 thereof, that investigation data are confidential and, until the case is examined by a court, may be disclosed only with the authorisation of the public prosecutor's office and in so far as such disclosure is justified. [12]

[9] Law of the Republic of Lithuania on criminal intelligence, in the version of Law No XI-2234 of 2 October 2012, as amended by Law No XIII-1837 of 20 December 2018; 'the LCI'.

[10] I will use the term 'information' rather than 'intelligence' to refer to the services that conduct the relevant investigations.

[11] Code of Criminal Procedure of the Republic of Lithuania of 14 March 2002, in the version applicable to the main proceedings; 'the CCP'.

[12] According to the Ikiteisminio tyrimo duomenų teikimo ir panaudojimo ne baudžiamojo persekiojimo tikslais ir ikiteisminio tyrimo duomenų apsaugos rekomendajos (Recommendations on the provision and use of pre-trial investigation data for non-prosecution purposes and the protection of pre-trial investigation data) approved by Decree No 1 279 of the Prosecutor General of 17 August 2017, as amended by Decree No 1 211 of 25 June 2018, in particular paragraph 23 thereof, upon receiving a request for access to investigation data, the public prosecutor is to decide whether such data should be provided. If so, the public prosecutor must specify the extent to which they may be provided.

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

23. The Lietuvos Respublikos generalinė prokuratūra (Prosecutor General's Office of the Republic of Lithuania; 'the Prosecutor General's Office') initiated an internal investigation into the actions of A.G., who at the time was a public prosecutor in an Apygardos prokuratūra (Regional Public Prosecutor's Office), in the light of evidence of misconduct in office.

24. The Commission of the Prosecutor General's Office found that A.G. had engaged in misconduct in office and proposed that the disciplinary measure of dismissal from service be imposed on him.

25. The evidence of misconduct took the form of information, obtained in the administrative proceedings, deriving from the actions of the criminal information services, the explanations of other officials and of the appellant in the main proceedings, and the findings of two pre-trial investigations.

26. In particular, there was evidence of telephone communications between A.G. and a suspect's lawyer, in a pre-trial investigation conducted by A.G. concerning cases in which that lawyer had acted as defence counsel. [13]

27. The monitoring and recording of information transmitted over electronic communications networks had been authorised by court orders.

28. The Prosecutor General imposed the penalty of dismissal from service on A.G., who brought an action before the Vilniaus apygardos administracinis teismas (Regional Administrative Court, Vilnius, Lithuania) seeking annulment of the penalty.

29. That action was dismissed by judgment of 16 July 2021 on the ground that, in the view of the court of first instance, the actions of the criminal information services had been lawful, as had the use, in the disciplinary proceedings, of the data obtained by those services.

30. A.G lodged an appeal against the first-instance judgment before the Lietuvos vyriausiasis administracinis teismas (Supreme Administrative Court of Lithuania), which has submitted the following question to the Court of Justice for a preliminary ruling:

'Must Article 15(1) of [Directive 2002/58] …, read in conjunction with Articles 7, 8, 11 and 52(1) of the Charter of Fundamental Rights of the European Union [(the Charter)], be interpreted as prohibiting the competent public authorities from using data retained by providers of electronic communications services which may provide information on the data of, and communications made by, a user of a means of electronic communications, in investigations into corruption-related misconduct in office, irrespective of whether access to those data has been granted, in the particular case, for the purposes of combating serious crime and preventing serious threats to public security?'

III. Procedure before the Court of Justice

31. The request for a preliminary ruling was received at the Court on 3 March 2022.

[13] As stated at the hearing, the respective criminal proceedings against A.G. and the lawyer for those acts are still ongoing.

32. A.G., the Czech, Estonian, Hungarian, Italian and Lithuanian Governments, Ireland and the European Commission submitted written observations.

33. A.G., the French, Hungarian and Lithuanian Governments, Ireland and the Commission were present at the hearing held on 2 February 2023.

IV. Analysis

A. Admissibility. Delimitation of the answer to the question referred for a preliminary ruling

34. The referring court is an administrative court with jurisdiction to review decisions of an administrative nature. That is also the nature of the decision adopted by the Prosecutor General, who imposed the penalty of dismissal from service on an official of a Regional Public Prosecutor's Office for acts constituting misconduct.

35. The main proceedings do not therefore concern decisions of the criminal courts. Although such decisions coexist alongside the (disciplinary) administrative proceedings which led to the official's dismissal,[14] it should be noted that the dispute relates only to the matter of dismissal.

36. That being so, it is apparent from the order for reference that the facts of the dispute, which lay the foundations for the question referred for a preliminary ruling, are somewhat imprecise.

37. As the Czech Government and the Commission have pointed out, it is not possible to establish with certainty, on the basis of the order for reference, whether the competent authorities: (a) approached providers of electronic communications services in order to obtain the data at issue; or (b) obtained those data themselves directly.

38. That is by no means a trivial matter. It is decisive for identifying which EU legislation is relevant for answering the question referred for a preliminary ruling. Depending on how events transpired, it would be necessary to apply:

– Directive 2002/58, if the data were obtained as a result of a processing obligation imposed on providers of electronic communications services; or

– Directive 2016/680, if the data were obtained directly by public authorities, without imposing obligations on those providers.

39. In the second scenario, the protection of personal data would be governed by national law, subject to the application of Directive 2016/680.[15] Accordingly, by focusing on Directive 2002/58, the approach taken in the question referred for a preliminary ruling is skewed.

40. The Hungarian Government – convinced that the personal data were obtained by telephone tapping carried out by the criminal information services – questions the admissibility of the reference for a preliminary ruling, as Directive 2002/58 would thus be inapplicable.

[14] See footnote 13 to this Opinion.

[15] Judgment in *La Quadrature du Net*, paragraph 103: '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]'.

41. The Commission, however, takes the following view.

– Directive 2016/680 would apply, in so far as the case at hand involves the use, in a subsequent investigation, of personal data collected and retained directly by the authorities in a prior criminal investigation.

– Directive 2002/58 would apply if, as the referring court has stated,[16] at least some of the data were collected and retained pursuant to a national provision adopted under Article 15(1) thereof. Directive 2002/58 would therefore be relevant to the outcome of the dispute.

42. I agree with the Commission's approach, which, moreover, is the only approach capable of assuaging the (justified) misgivings caused by the order for reference's admissibility.

43. If the question referred is thus construed, the relevance of Directive 2002/58 to the answer thereto:

– derives from the presumption inherent in any request for a preliminary ruling that there is a need for it to be made, which is a matter for the referring court to determine;[17]

– may be accepted in so far as the Court's interpretation is sought only in relation to Directive 2002/58, which the referring court considers to be essential for the resolution of the dispute.[18]

44. According to the referring court, the following matters are relevant to the proceedings on which it has to adjudicate:

'(i) the access to *data retained by providers of electronic communications services*, not only for the purpose of combating serious crime and preventing serious threats to public security; and

(ii) the *use of retained data* obtained for the purpose of combating serious crime and preventing serious threats to public security in investigating corruption-related misconduct in office.'[19]

45. Everything therefore seems to suggest that, aside from the possible presence of personal data the processing of which could not fall within the scope of Directive 2002/58 (but could fall within the scope of Directive 2016/680), the investigation leading to the imposition of the penalty made use of personal data collected from providers of electronic communications services.

46. The Court must limit its answer to the referring court's request as formulated by it. It will therefore be necessary to determine whether the personal data obtained and processed under Article 15(1) of Directive 2002/58 in a criminal investigation may subsequently be used in (administrative) proceedings of a disciplinary nature against a public official.

16 Paragraph 37 of the order for reference.

17 Judgments of 4 December 2018, *Minister for Justice and Equality and Commissioner of An Garda Síochána* (C-378/17, EU:C:2018:979, paragraph 26), and of 22 December 2022, *Airbnb Ireland and Airbnb Payments UK* (C-83/21, EU:C:2022:1018, paragraph 82).

18 The clear reference to Directive 2002/58 in the operative part of the order for reference and the fact that the legal reasoning in that order is silent on Directive 2016/680 militate in favour of the same conclusion. The fact remains, however, that the Court – without overstepping the boundaries of the question – may provide the referring court with useful guidance for its ruling, possibly invoking other provisions of EU law. See, to that effect, judgment of 18 September 2019, *VIPA* (C-222/18, EU:C:2019:751, paragraph 50 and the case-law cited).

19 Paragraph 35 of the order for reference. Emphasis added.

47. Having thus delimited the terms of the reference for a preliminary ruling, the corollary of the above is that the following matters fall outside its scope.

– In the first place, those relating to the lawfulness of the *initial collection* of personal data under Article 15(1) of Directive 2002/58. The referring court's question is limited to the *subsequent use* of those data in disciplinary proceedings and does not cast doubt on the lawfulness of their initial collection. [20]

– In the second place, those relating to the use of data obtained and processed directly by public authorities in previous criminal investigations. The referring court does not raise any concerns on that point either, which is governed by national law and by Directive 2016/680.

48. In short, the considerations set out below on the substance of the case will have to leave aside the interpretation of Directive 2016/680. [21] Those considerations will be confined, as regards Directive 2002/58, to the use of personal data obtained under that directive by means of processing operations the original lawfulness of which must be presumed, inasmuch as it is not disputed in the main proceedings.

B. Substance

1. Summary of the Court's case-law on the application of Directive 2002/58

49. It is apparent from the first sentence of Article 15(1) of Directive 2002/58 that Member States may adopt a measure derogating from the principle of confidentiality enshrined in Article 5(1) of that directive where it is 'necessary, appropriate and proportionate … within a democratic society' and is 'strictly' proportionate to the intended purpose. [22]

50. In particular, whether Member States may justify a limitation on the rights and obligations laid down in Articles 5, 6 and 9 of Directive 2002/58 must be assessed in the light of the seriousness of the interference entailed by such a limitation and by verifying that the importance of the public interest objective pursued by that limitation is proportionate to that seriousness. [23]

51. 'In order to satisfy the requirement of proportionality, the national legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data are affected have sufficient guarantees that those data will be effectively protected against the risk of abuse. That legislation must be legally binding under domestic law and, in particular, must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted …'. [24]

[20] It is therefore not necessary for the Court to rule on the lawfulness of those previous operations. If it were to do so, it would have to repeat that *access* to data held by providers of electronic communications services may be granted only if the *retention* of those data complied with Article 15(1) of Directive 2002/58. See, to that effect, the judgment in *La Quadrature du Net*, paragraph 167. That provision, read in the light of Article 7, Article 8, Article 11 and Article 52(1) of the Charter, precludes legislative measures which, for such purposes, provide, as a preventive measure, for the general and indiscriminate retention of traffic and location data (the judgment in *La Quadrature du Net*, paragraph 168).

[21] I will, however, refer to that directive in the alternative in the last part of this Opinion.

[22] The judgment in *La Quadrature du Net*, paragraph 129.

[23] The judgment in *La Quadrature du Net*, paragraph 131 and the case-law cited.

[24] The judgment in *Commissioner of An Garda Síochána*, paragraph 54.

52. As regards the public interest objectives that may justify a measure taken pursuant to Article 15(1) of Directive 2002/58, in accordance with the principle of proportionality, there is a hierarchy of objectives based on their respective importance: the importance of the objective pursued by such a measure must be proportionate to the seriousness of the interference. [25]

53. In that hierarchy of objectives, safeguarding national security, read in the light of Article 4(2) TEU, ranks higher than safeguarding the other interests referred to in Article 15(1) of Directive 2002/58, namely defence, public security and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system. The objective of combating crime in general, even serious crime, and of safeguarding public security, falls within that second category. [26]

54. It follows from that categorisation of objectives that:

– the objective of safeguarding national security, ranked first in the order of precedence indicated by the Court, permits interferences as serious as those entailed by legislative measures allowing for the imposition on providers of electronic communications services of an obligation to retain, generally and indiscriminately, traffic and location data; [27]

– the next-ranked objective, namely combating serious crime, may justify interferences such as, for example, the targeted retention of traffic and location data or IP addresses assigned to the source of a connection, for a period that is limited in time to what is strictly necessary. [28]

2. Application of that case-law to the present reference for a preliminary ruling

55. According to the referring court, the data at issue were obtained by means of serious interferences with the rights guaranteed by Articles 7, 8 and 11 of the Charter. [29]

56. The question here, I repeat, is not whether the collection of those data was initially lawful, that is to say, whether the interference was sufficiently justified in the light of the seriousness of the criminal offence targeted.

57. The referring court has taken a view on those two points (seriousness of the interference and seriousness of the offence) in terms which are not disputed in the main proceedings and are therefore not relevant to the reference for a preliminary ruling.

[25] The judgment in *Commissioner of An Garda Síochána*, paragraph 56.

[26] The judgment in *La Quadrature du Net*, paragraphs 135 and 136, in which the Court explained that national security is the sole responsibility of the State, a responsibility corresponding to the primary interest in protecting the essential functions of the State and the fundamental interests of society against activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities. Those threats can be distinguished, by their nature and particular seriousness, from the general risk that tensions or disturbances, even of a serious nature, affecting public security will arise. Accordingly, the objective of safeguarding national security is capable of justifying measures entailing more serious interferences with fundamental rights than those which might be warranted by those other objectives.

[27] The judgment in *Commissioner of An Garda Síochána*, paragraph 58.

[28] The judgment in *La Quadrature du Net*, paragraph 168.

[29] That is clear from paragraph 46 of the order for reference, alluding to data which may provide information regarding the communications made by a user of a means of electronic communication or regarding the location of the terminal equipment which he or she uses, and which allow precise conclusions to be drawn concerning the private lives of the persons concerned.

58. What matters at this juncture, according to the referring court, is whether those data: (a) may also be used in subsequent investigations aimed at combating crime in general (assuming that that concept covers the conduct to which the disciplinary measure at issue relates); or (b) may be used only in investigations aimed at combating serious crime.

59. The Czech Government and Ireland have examined whether or not the conduct at issue before the referring court should be classified as a 'serious offence' and have concluded that it should.

60. In my view, however, this is a matter on which the Court need not rule because the classification of the conduct is a matter for the referring court.

61. The referring court states that, if the use of data obtained by means of a serious interference with fundamental rights can be justified only in connection with combating serious crime and preventing serious threats to public security, such data cannot be used in investigations into corruption-related disciplinary offences, [30] in other words, in investigations such as the one at issue here.

62. Based on that assessment, what needs to be ascertained is whether disciplinary offences in respect of which action is to be taken using certain personal data must be qualitatively equivalent, as regards their seriousness, to the offences which justified the collection of those data. [31]

63. At the hearing, the Lithuanian Government acknowledged that the public prosecutor had been dismissed for professional misconduct. Whether that misconduct (leaking information about a pre-trial investigation) may be equated with a serious criminal offence or whether it presents a serious risk to the safeguarding of public security depends on a number of factors which only the referring court is in a position to verify. [32]

64. During the hearing, numerous references were made to combating corruption, as the phenomenon underlying conduct such as that at issue here. Any debate on that point would require considerable fine-tuning, in the interests of the exactitude demanded of all expressions of the State's power to punish. It would be necessary to determine, for instance, whether the term 'corruption' is used in a generic sense or whether it refers to a specific type of conduct within which, in the abstract, it would perhaps be unreasonable to include mere breach of the duty of secrecy without a corresponding advantage in favour of the official. [33]

[30] Order for reference, paragraph 46, *in fine*.

[31] The judgment of the European Court of Human Rights (ECtHR) of 18 January 2022, *Adomaitis v. Lithuania* (CE:ECHR:2022:0118JUD001483318; 'the ECtHR judgment in *Adomaitis*'), concerning the interception of electronic communications in a case involving a continued abuse of power by a prison governor, provides some guidance in assessing that equivalence.

[32] Punishable conduct tried in criminal proceedings and purely professional misconduct in respect of which a penalty is handed down in disciplinary proceedings cannot, in principle, be equated. Criminal proceedings and disciplinary proceedings differ, in terms of their subject matter, as to the nature and seriousness of the conduct in question. The diverse nature of proceedings is, in that regard, indicative of the varying degrees of seriousness of the subject matter involved.

[33] The Convention drawn up on the basis of Article K.3(2)(c) of the Treaty on European Union on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union (OJ 1997 C 195, p. 2) makes provision for passive corruption ('the deliberate action of an official, who, directly or through an intermediary, requests or receives advantages of any kind whatsoever, for himself or for a third party, or accepts a promise of such an advantage, to act or refrain from acting in accordance with his duty or in the exercise of his functions in breach of his official duties') and active corruption ('the deliberate action of whosoever promises or gives, directly or through an intermediary, an advantage of any kind whatsoever to an official for himself or for a third party for him to act or refrain from acting in accordance with his duty or in the exercise of his functions in breach of his official duties'), both of which must be made a criminal offence.

65. In any event, if the referring court were to take the view that the professional misconduct punished in this case is less serious than the criminal offence whose investigation justified the measure taken under Article 15 of Directive 2002/58, the answer to the question referred for a preliminary ruling would be apparent from the following findings of the Court.

– '… access to traffic and location data retained by providers in accordance with a measure taken under Article 15(1) of Directive 2002/58, which must be given effect in full compliance with the conditions resulting from the case-law interpreting Directive 2002/58, may, in principle, be justified only by the public interest objective for which those providers were ordered to retain those data. It is otherwise only if the importance of the objective pursued by access is greater than that of the objective which justified retention …'. [34]

– '… in particular … access to such data for the purpose of prosecuting and punishing an ordinary criminal offence may in no event be granted where the retention of such data has been justified by the objective of combating serious crime or, a fortiori, by the objective of safeguarding national security'. [35]

66. Accordingly, in that respect, a kind of principle of equivalence applies between, on the one hand, the public interest objectives justifying the *collection* of personal data and, on the other, those warranting the subsequent *use* of those data. The only exception to that principle is, as I have just mentioned, where the importance of the objective pursued by access is greater than that of the objective which justified retention.

67. Any other interpretation would effectively distort the system of safeguards under Directive 2002/58. The rights safeguarded could be seriously interfered with outside of the situations provided for in Article 15 and the conditions determined by the case-law of the Court.

68. In particular, the protection of the right to confidentiality of communications may be legitimately removed only on the basis of the specific public interest objective pursued by such removal. That is why the legitimacy of access to retained data must be assessed on a case-by-case basis, whereby the seriousness of the interference is weighed against the importance of the public interest objective pursued by that interference.

69. What cannot be accepted is an interpretation of Directive 2002/58 according to which the grant of access in a first scenario where such access is properly justified clears the way for subsequent access (in actual fact, reuse of the data obtained) based on a lower-ranking objective than the objective pursued in the first scenario.

70. In that connection, the requirements for initial access (including the requirements established by the Court as regards authorisation of such access) [36] are capable of being applied to the subsequent use of the same data by other authorities.

[34] The judgment in *Commissioner of An Garda Síochána*, paragraph 98.

[35] The judgment in *La Quadrature du Net*, paragraph 166.

[36] The judgment in *Commissioner of An Garda Síochána*, paragraph 106, citing the judgment in *Prokuratuur*, paragraph 51.

C. In the alternative: effect of Directive 2016/680

71. I have set out above what I consider to be the most appropriate way of answering the request for a preliminary ruling as it is worded, that is to say, by providing the referring court with an interpretation of Directive 2002/58, as sought by it.

72. If the data at issue in this case had been obtained not on the basis of Article 15(1) of Directive 2002/58 but directly by the criminal information services of the Member State in criminal proceedings, the situation would be different.

73. In those circumstances, the provisions of national law would come into play, subject to the application of Directive 2016/680 as regards the processing of personal data obtained in a criminal investigation. I have assumed that the actions of the criminal information services in cases like the present one fall within the scope of Directive 2016/680. That was confirmed at the hearing.

74. As I explained in my Opinion in *Inspektor* v *Inspektorata kam Visshia sadeben savet (Purposes of processing personal data – Criminal investigation)*,[37] 'the GDPR and Directive 2016/680 form a cohesive system in which:

– the role of the GDPR is to lay down *general rules* on the protection of natural persons with regard to the processing of their personal data;

– Directive 2016/680 lays down *specific rules* on the processing of such data in the area of judicial cooperation in criminal matters and police cooperation'.[38]

75. I made the following observations in that Opinion.[39]

– 'The protection afforded by the body of rules established by both provisions is based on the principles of lawfulness, fairness, transparency and, in so far as is relevant for the present purposes, on the principle of the strict limitation of the collection and processing of data to the purposes laid down by law'.

– 'In particular, Article 5(1)(b) of the GDPR provides that data is to be "collected for specified, explicit and legitimate purposes and *not further processed in a manner that is incompatible with those purposes*". Article 4(1)(b) of Directive 2016/680, as *lex specialis*, is also worded in those terms'.

– 'Therefore, personal data may not be collected or processed on a general basis but rather only by reference to certain specified purposes and subject to the conditions of lawfulness stipulated by the EU legislature'.[40]

– 'The principle that the collection and processing of data, on the one hand, must be strictly linked to the purposes that both operations must serve, on the other, is not absolute, since both the GDPR and Directive 2016/680 allow a degree of flexibility …'.

[37] C-180/21 (EU:C:2022:406); 'the Opinion in *Inspektor* v *Inspektorata*'.

[38] The Opinion in *Inspektor* v *Inspektorata*, point 35.

[39] The Opinion in *Inspektor* v *Inspektorata*, points 36 to 39.

[40] Article 5(1)(a) of the GDPR (Article 4(1)(a) of Directive 2016/680) establishes the 'lawfulness' requirement and Article 6 thereof lists the conditions for such lawfulness. For the present purposes and under Article 6(1)(e) of the GDPR, the processing must be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

76. In view of how the Court has interpreted Article 4(2) of Directive 2016/680,[41] it would be difficult to accept that personal data collected in criminal proceedings could be used *for the same purpose* in subsequent disciplinary proceedings against a public official.

77. I should point out, however, that under Article 4(2) of Directive 2016/680, 'processing by the same or another controller for any of the purposes set out in Article 1(1) other than that for which the personal data are collected shall be permitted in so far as:

(a) the controller is authorised to process such personal data for such a purpose in accordance with Union or Member State law; and

(b) processing is necessary and proportionate to that other purpose in accordance with Union or Member State law'.

78. It is on the basis of that premiss that the referring court will have to examine whether or not the (*different*) purpose of the further processing is among the purposes laid down in Article 1(1) of Directive 2016/680.

– If it is (reassignment *ad intra*), the referring court will have to determine whether the two requirements laid down in Article 4(2) of Directive 2016/680 are met.

– If it is not (reassignment *ad extra*), Article 9(1) of Directive 2016/680 will apply.

1. Use of data under Article 4(2) of Directive 2016/680

79. The *first* of the two requirements established by that provision will be met only if the Member State law takes the form of legislation[42] governing the circumstances in which the controller is permitted to process personal data. That legislation must, moreover, contain binding rules that are clear and precise.[43]

80. However, that is, of course, a matter for the referring court to determine, after examining Article 177 of the CCP, Article 19(3) of the LCI and the Recommendations of the Prosecutor General's Office.[44] On the basis of those factors, the referring court will have to gauge the extent to which national law allows information obtained in criminal proceedings to be used, subject to certain conditions, in an investigation into disciplinary offences. In that determination, the findings set out in the ECtHR judgment in *Adomaitis* may prove useful.[45]

[41] Judgment of 8 December 2022, *Inspektor* v *Inspektorata kam Visshia sadeben savet (Purposes of processing personal data – Criminal investigation)*, C-180/21 (EU:C:2022:967); 'the judgment in *Inspektor* v *Inspektorata*'.

[42] I share the Commission's view that, since the subsequent use of personal data obtained in a criminal investigation interferes with the fundamental rights guaranteed by Articles 7 and 8 of the Charter, it is imperative, under Article 52(1) of the Charter, that such interference be provided for by law.

[43] Point 51 of this Opinion.

[44] Footnote 12 to this Opinion.

[45] In § 83 of that judgment, the ECtHR found that the guarantee of legality of the interference ensured by national legislative provisions and by the case-law of the Constitutional Court of Lithuania was sufficient.

81. As regards the *second* requirement, the referring court will have to assess whether, in the data processing at issue in this case, the interference was necessary and proportionate. [46]

82. Again, the guidance provided in the ECtHR judgment in *Adomaitis* may assist in that assessment.

– As regards the issue of necessity, consideration will have to be given to whether it was actually necessary, owing to the inadequate evidential value of other data available in the disciplinary proceedings, for the data at issue to be used, in order to ensure the success of the investigation under way. [47]

– As regards the issue of proportionality, the seriousness of the offence giving rise to the disciplinary proceedings will have to be assessed, on the understanding that, as the Lithuanian Government has argued and as is apparent from the ECtHR judgment in *Adomaitis*, [48] the use of personal data is restricted to offences attracting the most severe disciplinary penalty, namely dismissal.

2. Use of data under Article 9 of Directive 2016/680

83. Under Article 9(1) of Directive 2016/680, personal data collected by competent authorities for the purposes set out in Article 1(1) thereof may be processed for purposes other than those set out in Article 1(1) if such processing is authorised by EU or Member State law. In those circumstances, the GDPR will apply unless the processing is carried out in the course of an activity which falls outside the scope of EU law. [49]

84. If the referring court considers Article 4(2) of Directive 2016/680 to be inapplicable, it will have to have recourse to the GDPR. In accordance with the GDPR, it will have to determine whether, in addition to the legal basis, at least one of the conditions for lawful processing of personal data listed exhaustively in Article 6(1) thereof is met.

V. Conclusion

85. In the light of the foregoing considerations, I propose that the Court of Justice give the following reply to the Lietuvos vyriausiasis administracinis teismas (Supreme Administrative Court of Lithuania):

1. 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), read in conjunction with Article 7, Article 8, Article 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union,

[46] As the Commission points out, the present case is not very different from the one examined in the judgment of the ECtHR of 16 June 2016, *Versini-Campinchi and Crasnianski v. France* (CE:ECHR:2016:0616JUD004917611). In § 57 of that judgment, the ECtHR held that the use, in disciplinary proceedings for breach of professional secrecy, of communications intercepted in the course of criminal proceedings pursues a legitimate aim under Article 8 of the ECHR. The close substantive overlap between the subject matter of criminal proceedings and that of disciplinary proceedings means that the legitimacy of the aims of both sets of proceedings converge.

[47] The ECtHR judgment in *Adomaitis*, § 85.

[48] The ECtHR judgment in *Adomaitis*, § 87.

[49] That exception was interpreted restrictively in the judgment of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)* (C-439/19, EU:C:2021:504, paragraph 66).

must be interpreted as meaning that it does not allow the competent public authorities to collect data retained by providers of electronic communications services which may provide detailed information about a user and to use those data in investigations into conduct constituting less serious offences than the offences whose investigation may have justified access to those data at the time.

2. In the alternative:

Article 9(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 on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, read in conjunction with Articles 6 and 10 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, in the light of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union,

must be interpreted as not precluding the use, in administrative proceedings of a disciplinary nature, of personal data obtained lawfully and directly by public authorities in a criminal investigation, provided that, in accordance with clear, precise and binding rules of national law, those proceedings and that investigation are linked and in so far as the use of the data pursues a legitimate aim and is necessary and proportionate, which is a matter for the referring court to determine.