Reports of Cases

OPINION OF ADVOCATE GENERAL
PITRUZZELLA
delivered on 21 January 2020[1]

Case C-746/18

H.K.
v
Prokuratuur

(Request for a preliminary ruling from the Riigikohus (Supreme Court, Estonia))

(Reference for a preliminary ruling — The processing of personal data in the electronic communications sector — Confidentiality of the communications — Providers of electronic communications services — General and undifferentiated retention of traffic and location data — Criminal investigations — Access of investigating authorities to data retained for periods of up to one year — Authorisation given by the Public Prosecutor's Office — Use of data in criminal proceedings as evidence — Directive 2002/58/EC — Article 1(3), Article 3 and Article 15(1) — Charter of Fundamental Rights of the European Union — Articles 7, 8, 11 and Article 52(1))

I. Introduction

1. This request for a preliminary ruling concerns the interpretation of Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications),[2] as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009,[3] read in the light of Articles 7, 8, 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union.[4]

2. The request has been made in the context of criminal proceedings brought against H.K., on the ground that he committed several robberies, used a bank card belonging to somebody else and committed acts of violence against parties to court proceedings.

3. The reports underpinning the finding that those criminal offences had been committed were drawn up using personal data obtained in connection with the provision of electronic communications services. The Riigikohus (Supreme Court, Estonia) has reservations as to the compatibility with EU law of the circumstances in which the investigating authorities had access to those data.

1 Original language: French.

2 OJ 2002 L 201, p. 37.

3 OJ 2009 L 337, p. 11 ('Directive 2002/58').

4 'the Charter'.

4. Those doubts concern, in the first place, the question whether the duration of the period in respect of which the investigating authorities had access to the data constitutes a criterion for assessing the seriousness of the interference with the fundamental rights of the persons affected that is associated with that access.

5. In the second place, the referring court asks whether the Prokuratuur (Public Prosecutor's Office, Estonia), in view of the various duties assigned to it under Estonian law, is an 'independent' administrative authority within the meaning of the judgment of 21 December 2016 in *Tele2 Sverige and Watson and Others*.[5]

II. Legal context

A. Directive 2002/58

6. In accordance with Article 1(3) of Directive 2002/58, that directive does 'not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law'.

7. In addition, Article 15(1) of that directive provides that 'Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. [6] To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of [EU] law, including those referred to in Article 6(1) and (2) of the Treaty on European Union'.

B. Estonian law

1. Law on electronic communications

8. The elektroonilise side seadus (Law on electronic communications),[7] of 8 December 2004, in the version applicable to the main proceedings, provides, in Paragraph 111[1], which is headed 'Obligation to retain data':

'…

(2) Providers of telephone and mobile telephone services and of telephone network and mobile telephone network services are obliged to retain the following data:

1) the number of the calling party and the name and address of the subscriber;

5 C-203/15 and C-698/15 ('*Tele2 Sverige and Watson and Others*'), EU:C:2016:970 (paragraph 120 and operative part 2).

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).

7 RT I 2004, 87, 593.

2) the number of the called party and the name and address of the subscriber;

3) when use is made of an additional service, including call forwarding or call transfer, the number dialled and the name and address of the subscriber;

4) the date and time of the start and end of the call;

5) the telephone or mobile telephone service used;

6) the International Mobile Subscriber Identity (IMSI) of the calling and called party;

7) the International Mobile Equipment Identity (IMEI) of the calling and called party;

8) the cell ID at the start of the call;

9) data on the geographical location of the base station by reference to its cell ID during the period for which data are retained;

10) in the case of pre-paid anonymous mobile telephone services, the date and time of the initial activation of the service and the cell ID from which the service was activated;

…

(4) The data referred to in subparagraphs 2 and 3 of this paragraph shall be retained for one year from the time of the communication if those data were generated or processed in the course of providing a communications service. …

…

(11) The data referred to in subparagraphs 2 and 3 of this paragraph shall be forwarded:

1) in accordance with the kriminaalmenetluse seadustik [Code of Criminal Procedure],[8] to an investigating authority, a surveillance authority, the public prosecutor's office and the court;

…'

2. Code of Criminal Procedure

9. Paragraph 17 of the Code of Criminal Procedure, in the version applicable to the main proceedings, which is headed 'Parties to court proceedings', provides in subparagraph 1:

'Parties to court proceedings are the public prosecutor's office …'

10. Under Paragraph 30 of the Code of Criminal Procedure, which is headed 'The public prosecutor's office in criminal proceedings':

'(1) The public prosecutor's office shall direct the pre-trial procedure, guaranteeing its lawfulness and effectiveness, and represent the public prosecution before the court.

8 RT I 2003, 27, 166.

(2) The powers of the public prosecutor's office in criminal proceedings shall be exercised in the name of the public prosecutor's office by a public prosecutor who acts independently and is only bound by the law.'

11. Paragraph 90[1] of the Code of Criminal Procedure, which is headed 'Requesting of data from a communications undertaking', provides, in subparagraphs 2 and 3:

'(2) The investigating authority may, in the pre-trial procedure with the authorisation of the public prosecutor's office or in judicial proceedings with the authorisation of the court, ask an electronic communications undertaking for the data listed in Paragraph 111[1](2) and (3) of the Law on Electronic Communications which are not specified in subparagraph 1 of this paragraph. The approval of the request shall note the period for which the data request is allowed with precise date indications.

(3) A request may be made pursuant to this paragraph only where this is essential for achieving the objective of the criminal proceedings.'

12. Paragraph 211 of the Code of Criminal Procedure, which is headed 'Objective of the pre-trial procedure', is worded as follows:

'(1) The objective of the pre-trial procedure is to gather evidence and create the other conditions for judicial proceedings.

(2) In the pre-trial procedure, the investigating authority and the public prosecutor's office shall ascertain the circumstances exonerating and incriminating the suspect or accused.'

3. Law on the Public Prosecutor's Office

13. The prokuratuuriseadus (Law on the Public Prosecutor's Office),[9] of 22 April 1998, in the version applicable to the main proceedings, provides, in Section 1, which is headed 'Public Prosecutor's Office':

'(1) The public prosecutor's office is a government authority falling under the jurisdiction of the Justiitsministeeriumi [Ministry of Justice, Estonia] which participates in planning the monitoring activities necessary for fighting and investigating criminal offences, directs the pre-trial procedure, guaranteeing its lawfulness and effectiveness, represents the public prosecution before the court, and performs other duties assigned to the prosecutor's office by law.

(1[1]) The public prosecutor's office performs its statutory duties independently and acts in accordance with the present law, other laws and legislation adopted on the basis of those laws.

…'

14. Paragraph 2 of the Law on the Public Prosecutor's Office, which is headed 'Public Prosecutor', provides in subparagraph 2:

'The public prosecutor performs his duties independently and acts exclusively according to the law and his convictions.'

9 RT I 1998, 41, 625.

III. Facts, the main proceedings, and the questions referred for a preliminary ruling

15. By decision of 6 April 2017 of the Viru Maakohus (Viru Court of First Instance, Estonia), H.K. was sentenced to two years' imprisonment for committing, in the period from 4 August 2015 to 1 February 2016, eight counts of theft of food and other material goods with a value between EUR 3 and EUR 40 and sums of money between EUR 5.20 and EUR 2 100, for using another person's bank card to withdraw money from a cash machine, causing that person damage totalling EUR 3 941.28, and for committing acts of violence against parties to court proceedings. [10]

16. The Viru Maakohus (Viru Court of First Instance) based H.K.'s conviction on, inter alia, reports which were drawn up using data relating to electronic communications, referred to in Paragraph 111^1 (2) of the Law on electronic communications, which the investigating authority had obtained from a telecommunications service provider in the pre-trial procedure, after having been granted authorisation from an assistant public prosecutor of the Viru Ringkonnaprokuratuur (Viru District Public Prosecutor's Office, Estonia) in accordance with Paragraph 901(2) of the Code of Criminal Procedure.

17. Accordingly, on 2 November 2015, an assistant public prosecutor of the Viru District Public Prosecutor's Office granted the investigating authority authorisation to require the operator of an electronic communications undertaking to provide the data referred to in Paragraph 111^1(2) of the Law on electronic communications, in order to establish, by means of two mobile telephone numbers of H.K., the fact of the transmission of calls and messages, their duration and method, and the personal data and location of the sender and the receiver on 21 September 2015.

18. On 4 November 2015, in relation to the data obtained from the communications undertaking on the basis of this authorisation, the investigating authority drew up a report indicating the ranges of transmitter masts in which the subscriber number used by H.K. was used after 7 p.m. on 21 September 2015. The prosecutor wished to use that report, together with other evidence, to prove before the court that H.K. committed the theft perpetrated on 21 September 2015.

19. On 25 February 2016, an assistant public prosecutor of the Viru District Public Prosecutor's Office granted the investigating authority authorisation to require the electronic communications undertaking to provide the data referred to in Paragraph 111^1(2) of the Law on electronic communications data in relation to seven subscriber numbers used by H.K. for the period from 1 March 2015 until 19 February 2016, in order to investigate a criminal offence under Paragraph 303(1) of the Karistusseadustik (Criminal Code). [11]

20. On 15 March 2016, in relation to the data obtained from the communications undertaking on the basis of this authorisation, the investigating authority drew up a report indicating the days on which H.K. called, and received calls from, the co-defendants and sent messages to and received messages from them. The prosecutor wished to use that report, together with other evidence, to prove that H.K. repeatedly threatened the co-defendants by telephone from spring 2015.

10 The referring court notes that this was combined with a period of imprisonment of four years and seven months imposed by the Viru Maakohus (Viru Court of First Instance) by judgment of 22 March 2016 and a period of imprisonment of five years and one month was imposed on H.K. as a final aggregate penalty.

11 The offence of exerting an influence on the administration of justice. I note that the facts alleged against H.K. have been, in that regard, reclassified by the Viru Maakohus (Viru Court of First Instance) under Paragraph 323(1) of the Criminal Code as the offence of violence against parties to court proceedings.

21. On 20 April and 6 May 2016, the investigating authority also drew up reports in relation to the data likewise obtained from the communications operator on the basis of this authorisation. The reports note the base stations in whose range calls were made from and received on the six subscriber numbers used by H.K. on 4, 27 and 31 August and from 1 to 3 September 2015. The prosecutor wished to use the reports, together with other evidence, to prove before the court that H.K. committed the six thefts perpetrated on the days mentioned.

22. On 20 April 2016, the investigating authority drew up a report in which data regarding two subscriber numbers used by H.K. was reproduced. Specifically, the report reveals the base stations in whose range calls were made from and received on these subscriber numbers in the period from 16 to 19 January 2015. The prosecutor wished to use that report, together with other evidence, to prove that H.K. was the person who withdrew cash from a cash machine using the victim's bank card from 17 to 19 January 2015.

23. The data forming the basis of the report were obtained from the communications undertaking on the basis of authorisations which had been granted by a senior public prosecutor of the Viru District Public Prosecutor's Office on 28 January and 2 February 2015 in another criminal case. That criminal case concerned criminal offences under Paragraph 200(2), points 7, 8 and 9 of the Criminal Code, namely two robberies committed on 23 and 27 January 2015 by a group using firearms and by means of breaking and entering. Those authorisations allowed the investigating authority to require the communications undertaking to provide data under Paragraph 111^1(2) of the Law on electronic communications regarding two subscriber numbers and various IMEI codes of H.K. from 1 January to 2 February 2015.

24. It is clear from the above description of the facts in the main proceedings that the public prosecutor's office granted the investigating authority authorisations to request data from a communications undertaking in the pre-trial procedure pursuant to Paragraph 90^1(2) of the Code of Criminal Procedure. The authorisations were granted in relation to data regarding the subscriber numbers of the person accused for the purpose of investigating various criminal offences for a duration, depending on the relevant offence, of one day, approximately one month and approximately one year.

25. H.K. lodged an appeal against the judgment of the Viru Maakohus (Viru Court of First Instance) before the Tartu Ringkonnakohus (Tartu Court of Appeal, Estonia), which dismissed that appeal by decision of 17 November 2017. H.K. then lodged an appeal on a point of law before the Riigikohus (Supreme Court) requesting that the judgments of the Court of First Instance and the Court of Appeal be set aside, the criminal proceedings terminated and that he be acquitted.

26. H.K. claims that the reports in which the data obtained from the communications undertaking are reproduced are not admissible evidence and his conviction on the basis of them is unfounded. In accordance with *Tele2 Sverige and Watson and Others*, the rules of Paragraph 111^1 of the Law on electronic communications which oblige service providers to retain communications data and the use of those data for the conviction of H.K. are contrary to Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8, 11 and Article 52(1) of the Charter.

27. According to the referring court, the question therefore arises whether the reports in question, which were drawn up by the investigating authority on the basis of data under Paragraph 111^1(2) of the Law on electronic communications requested from a communications undertaking on the basis of an authorisation by the public prosecutor's office, may be regarded as admissible evidence.

28. The data which providers of electronic communications services must retain for one year include, inter alia, the number of the calling and called party, the name and address of the subscriber, the date and time of the start and end of a call, the telephone or mobile telephone service used, the International Mobile Subscriber Identity and International Mobile Equipment Identity of the calling

and called party, as well as the cell ID at the start of the call and data on the geographical location of the base station. The referring court notes that these are data which relate to the fact that a transmission of calls and messages via telephone and mobile telephone takes place and to the location where a mobile terminal is used, but do not provide information about the content of the messages.

29. As is apparent from the judgment in *Tele2 Sverige and Watson and Others* and the judgment of 2 October 2018 in *Ministerio Fiscal*,[12] rules of national law which govern the retention of traffic and location data and the access to those data in criminal proceedings, such as Paragraph 111^{1}(2) and (4) of the Law on electronic communications and Paragraph 90^{1}(2) of the Code of Criminal Procedure, fall within the scope of Directive 2002/58.

30. The admissibility of evidence depends on compliance with the procedural rules on the gathering of evidence. Therefore, when assessing whether the reports at issue in the main proceedings are admissible as evidence, it is necessary to determine to what extent the gathering of data from the communications undertaking, on which the reports were based, was in conformity with Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8, 11 and Article 52(1) of the Charter.

31. Having regard to the judgments in *Tele2 Sverige and Watson and Others*[13] and *Ministerio Fiscal*,[14] the referring court asks whether Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8, 11 and Article 52(1) of the Charter, is to be interpreted as meaning that the access of State authorities to data making it possible to establish the start and end point, the date, the time and the duration, the type of communications service, the terminal used and the location of use of a mobile terminal in relation to a telephone or mobile telephone communication of a suspect entails interference with the fundamental rights enshrined in those articles of the Charter which is so serious that such access must be restricted to combating serious crime, regardless of the period for which the State authorities have sought access to the retained data.

32. In that regard, the referring court considers that the period in respect of which the data in question are requested is an essential fact which is to be taken into consideration when assessing the seriousness of the interference with fundamental rights that is associated with the request for the data at issue. Therefore, it is possible that an interference with fundamental rights is not sufficiently serious to the extent that the data are requested for only a brief period, such as one day. In that case, it is generally not possible on the basis of those data to draw clear conclusions regarding the private life of the person in question, which is why the access of the State authorities to the data could be justified by the objective of prosecuting and investigating criminal offences generally.

33. In addition, the referring court asks whether access to data such as the data at issue in the main proceedings may, in the light of *Ministerio Fiscal*,[15] be justified by that same objective, if the amount of data to which those authorities have access is small and the interference with the fundamental rights in question is therefore not serious. As regards the amount of data, it is essential to take account of both the type of data (such as the recipient of the communication and location of the terminal equipment) and the temporal extent (for example, one day, month or year). According to the referring court, the more serious the criminal offence, the more serious the interference with fundamental rights that is allowed in the proceedings and the larger the amount of data to which the State authorities are permitted to have access.

12 C-207/16 (‘*Ministerio Fiscal*’), EU:C:2018:788.

13 Operative part 2 of that judgment.

14 Paragraphs 53 and 57 of that judgment.

15 Paragraphs 55 to 57 of that judgment.

34. Lastly, the referring court asks whether the public prosecutor's office may be regarded as an 'independent' administrative authority within the meaning of *Tele2 Sverige and Watson and Others*.[16] It notes that, in Estonia, the public prosecutor's office directs the pre-trial procedure, the objective of which is, inter alia, to gather evidence. It also observes that the investigating authority and the public prosecutor's office have to ascertain the circumstances exonerating and incriminating the suspect. Finally, it notes that the powers of the public prosecutor's office in criminal proceedings are exercised in the name of the public prosecutor's office by a public prosecutor who performs his duties independently, as stated in Paragraph 30(1) and (2) of the Code of Criminal Procedure and Paragraph 1(1) and (1^1) and Paragraph 2(2) of the Law on the Public Prosecutor's Office.

35. In that context, the referring court notes that its doubts as to the requirement of independence under EU law are mainly on account of the fact that, following the pre-trial procedure, the public prosecutor's office issues an indictment against a person if it is convinced that all the necessary evidence is gathered and there is reason to do so. The referring court observes that, in that case, the public prosecutor's office brings the public prosecution before the court and is therefore also a party to the court proceedings. In addition, the referring court notes that the European Court of Human Rights has already accepted that, in certain circumstances, surveillance activities may be performed without prior judicial review having been carried out provided a judicial review takes place later.[17]

36. In those circumstances, the Riigikohus (Supreme Court) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

'1. Is Article 15(1) of Directive [2002/58], in conjunction with Articles 7, 8, 11 and 52(1) of the [Charter], to be interpreted as meaning that in criminal proceedings the access of State authorities to data making it possible to establish the start and end point, the date, the time and the duration, the type of communications service, the terminal used and the location of use of a mobile terminal in relation to a telephone or mobile telephone communication of a suspect constitutes so serious an interference with the fundamental rights enshrined in those articles of the Charter that that access in the area of prevention, investigation, detection and prosecution of criminal offences must be restricted to the fighting of serious crime, regardless of the period to which the retained data to which the State authorities have access relate?

2. Is Article 15(1) of Directive [2002/58], on the basis of the principle of proportionality expressed in [*Ministerio Fiscal*], paragraphs 55 to 57, to be interpreted as meaning that, if the amount of data mentioned in the first question, to which the State authorities have access, is not large (both in terms of the type of data and in terms of [the] temporal extent), the associated interference with fundamental rights is justified by the objective of prevention, investigation, detection and prosecution of criminal offences generally, and that the greater the amount of data to which the State authorities have access, the more serious the criminal offences which are intended to be fought by the interference must be?

3. Does the requirement mentioned in [*Tele2 Sverige and Watson and Others*], second point of the operative part, that the data access of the competent State authorities must be subject to prior review by a court or an independent administrative authority mean that Article 15(1) of Directive [2002/58] must be interpreted as meaning that the public prosecutor's office which directs the pre-trial procedure, with it being obliged by law to act independently and only being bound by the law, and ascertains the circumstances both incriminating and exonerating the accused in the pre-trial procedure, but later represents the public prosecution in the judicial proceedings, may be regarded as an independent administrative authority?'

16 Paragraph 120 and operative part 2 of that judgment.

17 The referring court cites, in that regard, the judgments of the European Court of Human Rights of 2 September 2010, *Uzun v. Germany* (CE:ECHR:2010:0902JUD003562305, §§ 71 to 74), and of 12 January 2016, *Szabó and Vissy v. Hungary* (CE:ECHR:2016:0112JUD003713814, § 77).

IV. Analysis

37. By its first and second questions, the referring court asks, in essence, whether Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8, 11 and Article 52(1) of the Charter, must be interpreted as meaning that the categories of data concerned and the duration of the period in respect of which access is sought are included amongst the criteria for assessing the seriousness of the interference with fundamental rights that is associated with the access by competent national authorities to the personal data that providers of electronic communications services are obliged to retain under national legislation.

38. Before answering that question, I will make two series of preliminary observations allowing me to respond, first, to the arguments raised by certain Member States regarding the scope of Directive 2002/58 and, second, to the suggestion made by the European Commission to examine, in the context of this reference for a preliminary ruling, the compatibility with EU law of Estonian legislation, in so far as it requires providers of electronic communications services to retain several categories of personal data generated in the course of providing those services.

A. Preliminary observations

1. Scope of Directive 2002/58

39. The Irish, Hungarian and Polish Governments raise questions as to the scope of Directive 2002/58.

40. The Irish Government seems to consider that, pursuant to Article 1(3) of Directive 2002/58, national legislation relating to the access of competent authorities to retained data in criminal matters falls outside the scope of the directive.

41. In accordance with the Court's case-law, namely the judgments in *Tele2 Sverige and Watson and Others* and *Ministerio Fiscal*, that argument must be rejected.

42. It should be noted, in that regard, that the Court held that the legislative measures referred to in Article 15(1) of Directive 2002/58 'come within the scope of that directive, even if they concern activities characteristic of States or State authorities, and are unrelated to fields in which individuals are active, and even if the objectives that such measures must pursue overlap substantially with the objectives pursued by the activities referred to in Article 1(3) of Directive 2002/58'.[18] The Court took the view that 'Article 15(1) necessarily presupposes that the national measures referred to therein fall within the scope of that directive, since it expressly authorises the Member States to adopt them only if the conditions laid down in the directive are met. Further, the legislative measures referred to in Article 15(1) of Directive 2002/58 govern, for the purposes mentioned in that provision, the activity of providers of electronic communications services'.[19]

43. The Court concluded that 'Article 15(1), read in conjunction with Article 3 of Directive 2002/58, must be interpreted as meaning that the scope of the directive extends not only to a legislative measure that requires providers of electronic communications services to retain traffic and location data, but also to a legislative measure relating to the access of the national authorities to the data retained by those providers'.[20]

18 *Ministerio Fiscal* (paragraph 34 and the case-law cited).

19 Idem.

20 *Ministerio Fiscal* (paragraph 35 and the case-law cited).

44. 'The protection of the confidentiality of electronic communications and related traffic data, guaranteed by Article 5(1) of Directive 2002/58, applies to the measures taken by all persons other than users, whether private persons or bodies or State bodies. As confirmed in recital 21 of that directive, the aim of the directive is to prevent unauthorised access to communications, including "any data related to such communications", in order to protect the confidentiality of electronic communications'. [21]

45. To those arguments, the Court added that 'legislative measures requiring providers of electronic communications services to retain personal data or to grant competent national authorities access to those data necessarily involve the processing, by those providers, of the data …. Such measures, to the extent that they regulate the activities of such providers, cannot be regarded as activities characteristic of States, referred to in Article 1(3) of Directive 2002/58'. [22]

46. As the Court held in *Ministerio Fiscal*, [23] it should be inferred from all of those arguments that a request for access to personal data retained by providers of electronic communications services, made in connection with a criminal investigation, falls within the scope of Directive 2002/58.

47. In addition, the Hungarian and Polish Governments put forward the argument that EU law does not govern the admissibility of evidence in criminal proceedings.

48. Although EU law, as it currently stands, does not govern the admissibility of evidence in criminal proceedings, the referring court has nevertheless clearly indicated how the interpretation of EU law that it seeks is necessary in order to enable it to rule on the admissibility of evidence. The admissibility of evidence depends on compliance with the conditions and procedural rules on the gathering of such evidence. Accordingly, when assessing whether the reports at issue in the main proceedings are admissible as evidence, the referring court must first determine the extent to which the gathering of the data from the communications undertaking, on which the reports were based, was in conformity with Article 15(1) of Directive 2002/58, read in conjunction with Articles 7, 8, 11 and Article 52(1) of the Charter. As I noted above, one aspect of that question is governed by EU law. In that regard, the national rules applicable to the taking of evidence must comply with the requirements arising from the fundamental rights guaranteed by EU law. [24] In those circumstances, I take the view that the argument put forward by the Hungarian and Polish Governments is irrelevant.

2. Retention of traffic and location data

49. Even though the questions referred for a preliminary ruling by the referring court concern the conditions for access to data, the Commission also asks the Court to rule, in the context of the present reference for a preliminary ruling, on the issue of retention of data. In that regard, it observes, in essence, that lawful access to retained data requires that the national legislation pursuant to which providers of electronic communications services must retain data generated in the course of providing those services must meet the requirements laid down in Article 15(1) of Directive 2002/58, read in the light of the Charter, or that the data in question have been retained by those providers on their own initiative, in particular for commercial purposes, in accordance with that directive.

21 *Ministerio Fiscal* (paragraph 36 and the case-law cited).

22 *Ministerio Fiscal* (paragraph 37 and the case-law cited).

23 See *Ministerio Fiscal* (paragraphs 38 and 39).

24 See, inter alia, by analogy, judgment of 10 April 2003, *Steffensen* (C-276/01, EU:C:2003:228, paragraph 71). In that judgment, the Court also addressed this issue in the light of the principle of effectiveness as a limit to the procedural autonomy of the Member States (paragraphs 66 to 68 of that judgment).

50. With regard to the case in the main proceedings, the Commission observes that the data to which the investigating authority had access had been retained by the providers of electronic communications services, not on their own initiative for commercial purposes, but in accordance with the obligation to retain data under Paragraph 111[1] of the Law on electronic communications. It also notes that H.K. disputes the lawfulness of the national legislation concerning access to data and the retention of those data. [25]

51. That said, I note that, as was the case in the reference for a preliminary ruling which gave rise to the judgment in *Ministerio Fiscal*, [26] the questions asked by the referring court in the present case are not intended to determine whether the personal data at issue in the main proceedings were retained by the providers of electronic communications services in conformity with the requirements laid down in Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8, 11 and Article 52(1) of the Charter. The questions referred relate only to the issue of whether the conditions under which national investigating authorities are granted access to those data pursuant to Estonian legislation are compatible with those provisions. That is why the dispute before the Court concerns almost exclusively the conditions of access to data.

52. In any event, the referring court may rely on the case-law following *Tele2 Sverige and Watson and Others* if it considers it necessary to rule on the compatibility with EU law of Paragraph 111[1] of the Law on electronic communications in order to resolve the dispute in the main proceedings.

53. In that regard, I will merely point out that, according to the Court, 'Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication'. [27]

54. It is for the referring court to verify, if necessary, whether Estonian legislation imposes on providers of electronic communications services an obligation relating to the retention of data that is general and indiscriminate, and to draw the necessary conclusions in order to resolve the dispute in the main proceedings. If Estonian rules relating to the retention of data were to be considered inconsistent with EU law, in so far as they are disproportionate in the light of the objective pursued, that same objective could not be used to justify access to the retained data.

55. Only if the obligation relating to the retention of data is subject to appropriate limitations, in particular with regard to the categories of data concerned and the data retention period, applying a differentiated regime according to the objective pursued and whether it is strictly necessary to achieve that objective, will it be compatible with the principle of proportionality.

56. I will not expand any further in this Opinion on the concept of 'limited data retention' which is examined in detail by Advocate General Campos Sánchez-Bordona in his Opinion delivered on 15 January 2020 in *Ordre des barreaux francophones and germanophone*. [28]

25 The Commission points out, in that regard, that the present case can be distinguished from that giving rise to *Ministerio Fiscal*.

26 See *Ministerio Fiscal* (paragraphs 49 and 50).

27 *Tele2 Sverige and Watson and Others* (paragraph 112).

28 C-520/18, EU:C:2020:7. See, in particular, points 72 to 107 of this Opinion.

B. Access of the competent national authorities to the retained data

1. Lessons learned from Tele2 Sverige and Watson and Others

57. The Court addresses the issue relating to access of the competent national authorities to the retained data 'regardless of the extent of the obligation to retain data that is imposed on providers of electronic communications services' and, in particular, irrespective of whether retention of data is generalised or targeted.[29] That statement relates to the fact that the Court considers the retention of data and access to those data to be two separate interferences with the fundamental rights protected by the Charter.

58. Access to the retained data 'must correspond, genuinely and strictly, to one of [the] objectives' set out in the first sentence of Article 15(1) of Directive 2002/58. Moreover, the seriousness of the interference must be consistent with the objective pursued. Where the interference is considered to be 'serious', only the objective of combating serious crime is capable of justifying such a measure.[30]

59. As is the case with regard to the retention of data, access to the retained data by the competent national authorities is granted only where it does not exceed the limits of what is strictly necessary.[31] Further, the legislative measures must 'lay down clear and precise rules indicating in what circumstances and under which conditions the providers of electronic communications services must grant the competent national authorities access to the data. Likewise, a measure of that kind must be legally binding under domestic law'.[32] Specifically, national legislation must 'lay down the substantive and procedural conditions governing the access of the competent national authorities to the retained data'.[33]

60. In view of the above, 'general access to all retained data, regardless of whether there is any link, at least indirect, with the intended purpose, cannot be regarded as limited to what is strictly necessary'.[34]

61. According to the Court, 'the national legislation concerned must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data of subscribers or registered users. In that regard, access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime'.[35]

62. In other words, the scope of the national legislation granting the competent national authorities access to the retained data must be sufficiently circumscribed in order to prevent the likelihood of such access applying to a significant number of individuals, if not all individuals, to all types of electronic communication and to all of the retained data. The Court therefore put forward the requirement of establishing a link between the persons concerned and the objective pursued.

63. In addition, the Court laid down the conditions under which the competent national authorities may be granted access to retained data.

29 See *Tele2 Sverige and Watson and Others* (paragraph 113).
30 See *Tele2 Sverige and Watson and Others* (paragraph 115).
31 See *Tele2 Sverige and Watson and Others* (paragraph 116).
32 *Tele2 Sverige and Watson and Others* (paragraph 117).
33 *Tele2 Sverige and Watson and Others* (paragraph 118).
34 *Tele2 Sverige and Watson and Others* (paragraph 119).
35 Idem.

64. First of all, access by the competent national authorities to retained data should, 'as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body'.[36] The decision of that court or body should 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'.[37]

65. Next, the Court takes the view that 'the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities'.[38]

66. Lastly, Member States must adopt rules relating to the security and protection of data retained by providers of electronic communications services so as to protect against misuse and against any unlawful access to those data.[39]

2. Lessons learned from Ministerio Fiscal

67. In *Ministerio Fiscal*, the Court was required to consider the compatibility with Article 15(1) of Directive 2002/58, read in the light of Articles 7 and 8 of the Charter, of national legislation which allowed the competent national authorities, such as the police, to access data relating to the identity of owners of certain SIM cards.

68. In its judgment, the Court noted that, as regards the objective of preventing, investigating, detecting and prosecuting criminal offences, the wording of the first sentence of Article 15(1) of Directive 2002/58 does not limit that objective to combating only serious crime, but refers to 'criminal offences' generally.[40]

69. The reasoning developed by the Court clarifies the fact that, so far as concerns the access by competent national authorities to data, there must be a correlation between the seriousness of the interference and the seriousness of the offences at issue.

70. The Court thus recalls, referring to paragraph 99 of *Tele2 Sverige and Watson and Others*, that it has admittedly held that, 'in areas of prevention, investigation, detection and prosecution of criminal offences, only the objective of fighting serious crime is capable of justifying public authorities' access to personal data retained by providers of electronic communications services which, taken as a whole, allow precise conclusions to be drawn concerning the private lives of the persons whose data is concerned'.[41]

71. However, the Court points out that it 'explained its interpretation by reference to the fact that the objective pursued by legislation governing that access must be proportionate to the seriousness of the interference with the fundamental rights in question that that access entails'.[42]

72. Indeed, 'in accordance with the principle of proportionality, serious interference can be justified, in areas of prevention, investigation, detection and prosecution of criminal offences, only by the objective of fighting crime which must also be defined as "serious"'.[43]

36 *Tele2 Sverige and Watson and Others* (paragraph 120).
37 Idem.
38 *Tele2 Sverige and Watson and Others* (paragraph 121).
39 See *Tele2 Sverige and Watson and Others* (paragraph 122).
40 See *Ministerio Fiscal* (paragraph 53).
41 *Ministerio Fiscal* (paragraph 54).
42 *Ministerio Fiscal* (paragraph 55).
43 *Ministerio Fiscal* (paragraph 56).

73. By contrast, 'when the interference that such access entails is not serious, that access is capable of being justified by the objective of preventing, investigating, detecting and prosecuting "criminal offences" generally'. [44]

74. Those considerations therefore called for an assessment of whether, in the light of the circumstances of the case, the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter that police access to the data in question in the main proceedings would entail should be regarded as 'serious'.

75. Unlike in the case giving rise to the judgment in *Tele2 Sverige and Watson and Others*, the interference with the rights protected by Articles 7 and 8 of the Charter that is associated with access to the data at issue could not be defined as 'serious' by the Court. [45] The 'sole purpose of the request … [was] to identify the owners of SIM cards activated over a period of 12 days with the [International Mobile Equipment Identity] code of the stolen mobile telephone'. [46] The request sought access 'to only the telephone numbers corresponding to those SIM cards and to the data relating to the identity of the owners of those cards, such as their surnames, forenames and, if need be, addresses. By contrast, those data do not concern … the communications carried out with the stolen mobile telephone or its location.' [47]

76. The Court concluded that 'the data concerned by the request for access at issue in the main proceedings only enables the SIM card or cards activated with the stolen mobile telephone to be linked, during a specific period, with the identity of the owners of those SIM cards. Without those data being cross-referenced with the data pertaining to the communications with those SIM cards and the location data, those data do not make it possible to ascertain the date, time, duration and recipients of the communications made with the SIM card or cards in question, nor the locations where those communications took place or the frequency of those communications with specific people during a given period. Those data do not therefore allow precise conclusions to be drawn concerning the private lives of the persons whose data is concerned'. [48]

77. Having found that there was no 'serious interference', the Court was able to hold that the objective of preventing, investigating, detecting and prosecuting 'criminal offences' generally, even if not serious offences, could be relied upon to justify the interference at issue. [49]

78. It is in the light of that case-law that the referring court asks its first and second questions for the purpose of assessing the seriousness of the interference that is associated with the access to data in the criminal proceedings at issue in the main proceedings. Specifically, it seeks to determine whether the categories of data concerned and the duration of the period in respect of which access to those data is sought constitute, from that point of view, relevant criteria.

3. Criteria for assessing the seriousness of the interference

79. As is apparent from the Court's case-law, the more categories of data there are to which access is requested, the more likely the interference is to be considered 'serious'.

44 *Ministerio Fiscal* (paragraph 57).
45 *Ministerio Fiscal* (paragraph 61).
46 *Ministerio Fiscal* (paragraph 59).
47 Idem.
48 *Ministerio Fiscal* (paragraph 60).
49 *Ministerio Fiscal* (paragraph 62).

80. Nonetheless, the first and second questions asked by the referring court will lead the Court to determine whether, in addition to the categories of data in question, the temporal extent of the period covered by that access also plays a role in determining the seriousness of the interference.

81. In my opinion, the answer should be in the affirmative. In addition, I note that, in *Ministerio Fiscal*, the Court also took account of the duration of the period covered by the access in making its assessment, that is to say 12 days in that case. [50]

82. The seriousness of the interference is determined by taking account of the type of data concerned combined with the duration of the period covered by the access. These two considerations make it possible to assess whether the criterion determining the seriousness of the interference has been met, that is to say whether access to the data in question is likely to allow precise conclusions to be drawn by the competent national authorities concerning the private life of the person whose data are concerned by the access. In order to build an accurate profile of someone, it is necessary not only that the access concerns several categories of data, such as identification, traffic and location data, but also that the access covers a period long enough to ascertain with sufficient precision the main features of a person's life.

83. As with the number of categories concerned, the duration of the period in respect of which data are required in accordance with the authorisation for access therefore constitutes an essential element in assessing the seriousness of the interference with the fundamental rights of the persons affected. As the Commission points out, the multiplicity of applications for access relating to a single person must also be taken into account, even if they concern short periods.

84. As is apparent from the order for reference, the data to which the investigating authority had access are listed in Paragraph 111^{1}(2) of the Law on electronic communications. Those data make it possible to establish the start and end point, the date, the time and the duration, the type of communications service, the terminal used and the location of use of a mobile terminal in relation to a telephone or mobile telephone communication of a person. Those data were transmitted to the investigating authority in respect of periods of one day, one month and almost a year.

85. The assessment of the degree of interference with fundamental rights that is associated with the competent national authorities' access to the retained personal data is the result of a detailed examination of the specific circumstances of each case. In each case it is for the referring court to assess whether the data to which access has been authorised are such as to allow, depending on the type and duration of the period covered by that access, precise conclusions to be drawn concerning the private lives of the persons concerned.

86. If that is the case, the interference must be considered to be 'serious' within the meaning of the Court's case-law and thus can be justified, in areas of prevention, investigation, detection and prosecution of criminal offences, only by the objective of combating crime which must also be considered as 'serious'. [51]

4. Correlation between the seriousness of the interference and the objective pursued

87. It follows from the Court's case-law that greater justification is required in respect of an interference with fundamental rights which is considered to be 'serious'.

50 See *Ministerio Fiscal*. See, to the same effect, the Opinion of Advocate General Saugmandsgaard Øe in *Ministerio Fiscal* (C-207/16, EU:C:2018:300), who observes that the police authorities' request concerned 'a clearly defined period of short duration, namely around 12 days' (points 33 and 84).

51 *Ministerio Fiscal* (paragraph 56).

88. So far as concerns the seriousness of the alleged criminal offences in respect of which access to data has been granted, the Commission observes that the national legislation at issue in the main proceedings authorises, inter alia, access for the purpose of fighting crime generally. [52]

89. It is for the referring court to assess, depending on the circumstances of each individual case, whether access to data such as those at issue in the main proceedings genuinely meets in the strictest sense one of the objectives set out in Article 15(1) of Directive 2002/58. It should be borne in mind, in that regard, that that provision does not limit the objective of preventing, investigating, detecting and prosecuting criminal offences to combating only serious crime, but refers to 'criminal offences' generally. [53]

90. If the referring court concludes that the interference must be considered to be 'serious', it must assess whether the offence in question can also be considered to be 'serious' under national criminal law.

91. In that regard, I take the view that the definition of what may be considered to be 'serious crime' should be left to the discretion of the Member States.

92. Depending on the national legal system, the same offence may be penalised more or less severely. What constitutes aggravating circumstances may also vary between the Member States.

93. As the Estonian Government rightly points out, in order to assess the seriousness of offences, the penalty applicable to those offences is not the only criterion. It is also necessary to take account of the nature of the offence, the damage caused to society, the detriment to legal interests and the overall effects the offence has on the national legal system and the values of a democratic society. The specific historic, economic and social context of each Member State also plays a role in that regard. In addition, under the heading of aggravating circumstances, it should be considered whether the criminal offences have been committed repeatedly, for example, or in respect of vulnerable persons.

94. In order to assess the proportionality of the access, account should also be taken of the fact that, in accordance with Paragraph 90^{1}(3) of the Code of Criminal Procedure, 'a request may be made … only where this is essential for achieving the objective of the criminal proceedings'. As the Estonian Government states, the criterion of absolute necessity [54] requires the investigating authorities and the persons responsible for granting authorisation to consider and assess what data are necessary for conducting criminal proceedings and, in the context of a given case, for making it possible to ascertain the truth or apprehend an alleged offender or criminal.

95. I add that, as the French Government was correct to point out, the degree of seriousness of an offence, or even the exact legal classification thereof, cannot always be determined precisely where authorisation to access the retained data is granted at an early stage of the investigation, such that it might seem premature at that stage to consider the offence in question as either a serious crime or as a general criminal offence. That uncertainty, which is inherent in criminal investigations the very purpose of which is to ascertain the truth, must be taken into account by the referring court in its assessment of whether the access is proportionate.

52 Paragraph 111^{1}(11) of the Law on electronic communications and Paragraph 90^{1} of the Code of Criminal Procedure.

53 See *Ministerio Fiscal* (paragraph 53).

54 Also referred to as the '*ultima ratio* principle'.

96. That being said, the uncertainty that may therefore exist at the start of the criminal investigation with regard to those considerations cannot eliminate the requirement that each request for access must be justified by the need to search for evidence of specific criminal behaviour, on the basis of a suspicion substantiated by objective evidence. Accordingly, a request for access should not have the purpose of examining, in respect of a given period, a person's actions in order to detect possible offences. In addition, if new facts come to light in the course of the investigation, the access to data to establish those facts should be made subject to a new authorisation.

97. In view of the foregoing, I propose that the Court rule that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8, 11 and Article 52(1) of the Charter, must be interpreted as meaning that the categories of data concerned and the duration of the period in respect of which access is sought should be included amongst the criteria for assessing the seriousness of the interference with fundamental rights that is associated with the access by competent national authorities to the personal data that providers of electronic communications services are obliged to retain under national legislation. It is for the referring court to assess, depending on the seriousness of the interference, whether that access was strictly necessary to achieve the objective of preventing, investigating, detecting and prosecuting criminal offences.

C. Prior review by a court or an independent administrative authority

98. In order to ensure that the access by the competent national authorities to retained data is limited to what is strictly necessary to achieve the objective pursued, the Court has held that it is essential that that access 'should, as a general rule, except in cases of validly established urgency, 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 should 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'. [55]

99. By its third question, the referring court invites the Court to clarify the requirements that must be met by an administrative authority in order to be considered 'independent' within the meaning of *Tele2 Sverige and Watson and Others*. Specifically, the referring court asks whether the public prosecutor's office, in so far as it directs the pre-trial procedure and represents the public prosecution in the judicial proceedings, may be regarded as an independent administrative body.

100. In order to answer that question, I take the view that it is pertinent to take into account two branches of the Court's case-law, namely, on the one hand, the case-law relating to the independence of national data protection supervisory authorities and, on the other, the case-law relating to the independence of the issuing judicial authority in the context of the European Arrest Warrant.

101. According to the Court, independence is an essential characteristic, as stated, inter alia, in Article 8(3) of the Charter, of public authorities responsible for monitoring compliance with EU rules on the protection of individuals with regard to the processing of personal data in order to ensure the effectiveness and reliability of the monitoring and to strengthen the protection of individuals affected by the decisions of those authorities. [56]

55 *Tele2 Sverige and Watson and Others* (paragraph 120 and the case-law cited), italics added. See, to the same effect, Opinion 1/15 (*EU-Canada PNR Agreement*) of 26 July 2017 (EU:C:2017:592, paragraphs 202 and 208).

56 See, inter alia, judgment of 6 October 2015, *Schrems* (C-362/14, EU:C:2015:650, paragraphs 40 and 41 and the case-law cited). See, also, Opinion 1/15 (*EU-Canada PNR Agreement*) of 26 July 2017 (EU:C:2017:592, paragraph 229).

102. The Court has held, with regard to the second subparagraph of Article 28(1) of Directive 95/46, that 'the supervisory authorities responsible for supervising the processing of personal data must enjoy an independence allowing them to perform their duties free from external influence. That independence precludes inter alia any directions or any other external influence in whatever form, whether direct or indirect, which may have an effect on their decisions and which could call into question the performance by those authorities of their task of striking a fair balance between the protection of the right to private life and the free movement of personal data'. [57]

103. The Court has also emphasised the requirement that, in view of their role as guardians of the right to private life, those supervisory authorities must be 'above all suspicion of partiality'. [58]

104. In so far as the referring court's third question concerns the public prosecutor's office, it is also relevant to take into account the criteria developed by the Court in its case-law relating to the independence of the issuing judicial authority in the context of the European Arrest Warrant. Thus, according to the Court, the review carried out at the time of adoption of an arrest warrant 'must be exercised objectively, taking into account all incriminatory and exculpatory evidence, and independently, which presupposes the existence of statutory rules and an institutional framework capable of excluding any risk that the adoption of a decision to issue such an arrest warrant be subject to external instructions, in particular from the executive'. [59] It is important to bear in mind, however, that in each case the Court's specific assessment of whether the public prosecutor's office [60] met the criteria was made in the particular context of the issuing of a European Arrest Warrant and cannot, therefore, be applied automatically to other areas, such as the protection of personal data.

105. That said, the two branches of the Court's case-law are consistent in emphasising, in each of the areas concerned, that the national authority responsible for monitoring compliance with EU rules must be independent, which covers two requirements. [61] First, that authority should not be subject to external directions or pressure liable to influence its decisions. Second, that authority should, by virtue of its legal position and the duties assigned to it, meet a condition of objectivity when carrying out its review, that is to say it must offer guarantees of impartiality. Specifically, the assessment carried out by an administrative authority of the proportionality of the access to retained data requires a balance to be struck between the interests related to the effectiveness of the investigation in the context of combating crime and those related to the protection of the personal data of the persons affected by the access. In relation to the latter, the requirement of impartiality is therefore inherent in the concept of 'independent administrative authority' emphasised by the Court in *Tele2 Sverige and Watson and Others*.

106. It is necessary to verify whether the public prosecutor's office, in view of the various duties assigned to it under Estonian law, meets that requirement of independence in both its forms when it assesses whether the access to data is strictly necessary. Accordingly, the concept of 'independence' that should characterise the administrative authority responsible for such a review has a functional element to it, in that it is in the light of the specific objective of the review that it is necessary to

57 Judgment of 8 April 2014, *Commission* v *Hungary* (C-288/12, EU:C:2014:237, paragraph 51 and the case-law cited).

58 Judgment of 8 April 2014, *Commission* v *Hungary* (C-288/12, EU:C:2014:237 paragraph 53 and the case-law cited).

59 See judgment of 9 October 2019, NJ (Public Prosecutor's Office, Vienna (C-489/19 PPU, EU:C:2019:849, paragraph 38 and the case-law cited).

60 See, most recently, judgment of 12 December 2019, *JR and YC (Procureurs de Lyon et Tours and Procureurs de Lyon et de Tours)*, C-566/19 PPU and C-626/19 PPU, EU:C:2019:1077, in which the Court found, inter alia, that the evidence presented to it was sufficient to demonstrate that 'in France, public prosecutors have the power independently to assess, particularly in relation to the executive, whether the issuing of a European Arrest Warrant is necessary and proportionate, and exercise that power objectively, taking into account all of the inculpatory and exculpatory evidence' (paragraph 55 of the judgment).

61 On the two aspects of the requirement of independence see, by analogy, with regard to national courts called upon to rule on issues relating to the interpretation and application of EU law, judgment of 5 November 2019, *Commission* v *Poland (Independence of ordinary courts)* (C-192/18, EU:C:2019:924, paragraphs 108 to 110 and the case-law cited).

assess whether the authority is able to act without external interference or pressure liable to influence its decisions, objectively and with strict application of the rule of law. In summary, the concept of 'independent administrative authority' within the meaning of *Tele2 Sverige and Watson and Others* is intended to guarantee the objectivity, reliability and effectiveness of the review.

107. It means examining whether the rules of Estonian law which set out the legal position and duties assigned to the public prosecutor's office is likely to create legitimate doubts, in the minds of the persons concerned, as to the imperviousness of the public prosecutor to external influences and its neutrality with regard to the conflicting interests involved when carrying out a prior review of whether the access to data is proportionate.

108. The public prosecutor's office plays an essential role in the conduct of criminal proceedings, since it directs pre-trial criminal investigations and has the power to prosecute a person suspected of having committed a criminal offence so that that person may be brought before a court. To that extent, it must be regarded as being an authority which participates in the administration of criminal justice. [62]

109. As stated by the Court with regard to the Procura della Repubblica (Office of the Public Prosecutor, Italy) and pursuant to a formula which I believe could be adopted in the present case, the role of the public prosecutor 'is not to rule on an issue in complete independence but, acting as prosecutor in the proceedings, to submit that issue, if appropriate, for consideration by the competent judicial body'. [63]

110. Whilst the public prosecutor's office has, in terms of its legal position and the duties assigned to it, special characteristics which distinguish it from a court and which justify its classification as an 'authority participating in the administration of criminal justice in the Member States', the fact remains that, from a functional point of view, where national law provides that the authority which carries out a prior review of the proportionality of the access, as required by *Tele2 Sverige and Watson and Others*, is the public prosecutor's office, the latter must, in this particular regard, demonstrate a degree of independence similar to that of a court. The exercise of that function by an administrative authority rather than by a court must not affect the objectivity, reliability and effectiveness of the review.

111. In that regard, it should be borne in mind that, in accordance with Paragraph 90^{1}(2) of the Code of Criminal Procedure, the investigating authority may, with the authorisation of the public prosecutor's office in the pre-trial procedure or with the authorisation of the court in judicial proceedings, ask an electronic communications undertaking for the data listed in Paragraph 111^{1}(2) and (3) of the Law on electronic communications.

112. In addition, it is apparent from the Estonian legislation that the public prosecutor's office directs the pre-trial procedure in criminal cases, the aim of which is to gather evidence and create the other conditions necessary for judicial proceedings to be held. Moreover, in the pre-trial procedure, the investigating authority and the public prosecutor's office ascertain the circumstances exonerating and incriminating the suspect or accused. The public prosecutor's office issues an indictment against a person if it is convinced that all the necessary evidence is gathered and there is reason to do so. In that case, the public prosecutor's office brings the public prosecution before the court.

62 See, inter alia, judgment of 27 May 2019, *PF (Prosecutor General of Lithuania)* (C-509/18, EU:C:2019:457, paragraphs 39 and 40).
63 Judgment of 12 December 1996, *X* (C-74/95 and C-129/95, EU:C:1996:491, paragraph 19).

113. The referring court also observes that although the public prosecutor's office must obtain the authorisation of an investigating judge for measures which constitute the most serious interference with a person's fundamental rights (for instance, most surveillance activities, arrest), the powers of the public prosecutor's office also include deciding on some procedural measures which severely interfere with several fundamental rights. [64]

114. The doubts expressed by the referring court as to whether the public prosecutor's office meets the criterion of an 'independent administrative authority' within the meaning of *Tele2 Sverige and Watson and Others* are mainly based on the fact that, following the pre-trial procedure, the public prosecutor's office issues an indictment against the person in question if it is convinced that all the necessary evidence is gathered in the criminal matter and there is reason to do so. In that case, the public prosecutor's office brings the public prosecution before the court and is therefore also a party to the court proceedings. Accordingly, it is mainly on account of the status of the public prosecutor's office as a prosecuting party that the referring court has doubts as to whether it may be regarded as an 'independent administrative authority' within the meaning of *Tele2 Sverige and Watson and Others*.

115. Expressed in that way, the doubts raised by the referring court therefore relate, more particularly, to the impartiality of the public prosecutor's office when reviewing the proportionality of the access to data by the investigating authorities which it is expected to do before authorising such access.

116. Before addressing the issue of impartiality, I note that Paragraph $1(1^1)$ of the Law on the Public Prosecutor's Office provides that the latter 'performs its statutory duties independently'. Moreover, in accordance with Paragraph 2(2) of that law, 'the public prosecutor performs his duties independently and acts exclusively according to the law and his convictions'. [65]

117. In that regard, the Estonian Government states that, although the public prosecutor's office is an authority which falls under the jurisdiction of the Ministry of Justice, Estonian law precludes the latter from making an assessment on a specific procedure or from intervening in ongoing criminal proceedings. It explains that disregarding the independence of the public prosecutor's office constitutes a punishable offence.

118. While there is therefore no reason to doubt the independence of the public prosecutor's office in carrying out the duties assigned to it under Estonian legislation, that legislation seems to me, however, to be of such a nature as to raise legitimate doubts as to the ability of the public prosecutor's office to carry out a neutral and objective prior review of the proportionality of the access to data when it may be called upon, in a given case, to perform at the same time duties consisting of directing the pre-trial procedure, the prosecution of criminal offences and representing the public prosecution in judicial proceedings.

119. It is true that several elements included in Estonian law constitute guarantees that the public prosecutor's office acts, when fulfilling the duties assigned to it, in accordance with the requirement of impartiality.

120. Thus, pursuant to Paragraph 211(2) of the Code of Criminal Procedure, the public prosecutor's office is required to ascertain the circumstances exonerating and incriminating the suspect or accused.

121. Furthermore, as is apparent from Paragraph 1(1) of the Law on the Public Prosecutor's Office, the public prosecutor's office is required to guarantee the lawfulness of the pre-trial procedure which it is responsible for directing. Moreover, in accordance with Paragraph $1(1^1)$ and Paragraph 2(2) of that law, the public prosecutor's office must perform its duties in accordance with the law. This means that, in

64 For example, the public prosecutor's office grants authorisation for the undercover surveillance of a person, an object or a location and, in many cases, for a search.

65 See, also, to the same effect, Paragraph 30(2) of the Code of Criminal Procedure.

directing the pre-trial procedure, the public prosecutor's office must ensure not only its effectiveness and but also that it does not constitute a disproportionate interference with the private life of the persons concerned. It may be considered that authorising access to retained data is an integral part of the broader role of the public prosecutor's office which consists of monitoring the lawfulness of the means employed by the investigating authorities, in particular the proportionality of investigative acts in the light of the type and seriousness of the offence.

122. The argument could therefore be raised that it is precisely because it directs the pre-trial procedure that the public prosecutor's office is able to assess whether, having regard to the specific circumstances of each case, access to data retained by telecommunications operators is strictly necessary, in the absence of alternative evidence, in order to advance the investigation of an alleged offence.

123. The fact remains that, from the point of view of persons affected by the request for access to data, the fact that the administrative authority responsible for assessing whether that access is strictly necessary within the framework of the investigation may, at the same time, prosecute them and later represent the public prosecution in judicial proceedings is, in my opinion, such as to weaken the guarantees of impartiality provided by Estonian law. From that point of view, there may be a potential for conflict between the duties assigned to the public prosecutor's office, on the one hand, and the requirement that the prior review of the proportionality of the access to data be carried out with neutrality and objectivity, on the other.

124. Within the framework of its duties, the public prosecutor's office is required to gather evidence, assess its relevance and to draw conclusions as to whether the person in question is guilty. It is for that State authority to put forward and prove the prosecution's case in the context of the public prosecution which it represents before the court, being, therefore, a party to the proceedings. On account of those duties, the public prosecutor's office is under an evidential burden which may appear, in the eyes of persons suspected of having committed a criminal offence, as being inconsistent with the ability of that authority to carry out, with neutrality and objectivity, a prior review of whether the access to data is proportionate.

125. As the Commission observes, the risk could be that, in view of the overlap in the duties assigned to it, the public prosecutor's office may be perceived by the persons concerned as having an interest in giving broad access to their data, whether of an incriminating or exculpatory nature. Furthermore, the persons suspected of having committed a criminal offence may have legitimate doubts as to the impartiality of the public prosecutor's office when it authorises access to their data, since it may be the prosecuting party in the proceedings which follow. I consider that the requirement of impartiality on the part of the administrative authority responsible for carrying out the prior review pursuant to *Tele2 Sverige and Watson and Others* presupposes a certain distance and neutrality with regard to the conflicting interests likely to come into play in the pre-trial procedure, namely, on the one hand, the effectiveness of that procedure and, on the other, the protection of the personal data of the persons concerned. According to the Commission, the situation could be different if the internal administrative organisation of the public prosecutor's office was such that the public prosecutor responsible for ruling on a request for access to data played no role in the pre-trial procedure or any subsequent stages of the proceedings, including the public prosecution.

126. Since, as was confirmed at the hearing, the public prosecutor's office is organised hierarchically within Estonia, I am not convinced that the Commission's suggestion would overcome the shortcomings caused by the overlap in the duties assigned to the public prosecutor's office under Estonian law. In any event, that does not mean that the idea behind that suggestion, namely that the prior review of the proportionality of the access to data should be carried out by an administrative authority which is not directly involved in the criminal investigation in question and adopts a neutral stance vis-à-vis the parties to the criminal proceedings, is of no consequence. Such an authority, independent of any interests related to the investigation and public prosecution in the case in the main

proceedings, could not be criticised for wanting to put the interests of the investigation first at the expense of those linked to the protection of the data of the persons concerned. That authority would then be able to adopt, in an impartial way, a decision restricting the access to retained data to what is strictly necessary to achieve the objective pursued, in accordance with the requirement set out in Article 15(1) of Directive 2002/58, as interpreted by the Court in the judgments of 8 April 2014, *Digital Rights Ireland and Others*[66] and *Tele2 Sverige and Watson and Others*. At the same time, I am very aware that having an institution with an outside view on the interests relating to the proceedings in question must not be at the expense of weakening the effectiveness of the investigation, detection and prosecution of criminal offences.

127. In order to respect the procedural autonomy of the Member States, the Court should not interfere further with the general organisation of the administration of justice in the Member States, any more than in the internal organisation of the public prosecutor's office. It is for the Member States to implement their own measures to ensure that the prior review of the access to retained data strikes a balance between the interests relating to the effectiveness of the criminal investigation and the right to data protection of the persons affected by that access.

128. I will close by stating that, in my opinion, the fact that no prior review is carried out by an 'independent' administrative authority within the meaning of *Tele2 Sverige and Watson and Others* cannot be offset by carrying out a judicial review after access has been granted.[67] Otherwise the prior nature of the review would lose its purpose, which is to prevent access to retained data that would be disproportionate to the objective of investigating, prosecuting and sanctioning criminal offences.

129. In view of the foregoing, I propose that the Court's answer to the third question should be that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8, 11 and Article 52(1) of the Charter, must be interpreted as meaning that the requirement that the access of the competent national authorities to retained data be subject to prior review by a court or an independent administrative authority is not met where national legislation provides that such review is to be carried out by the public prosecutor's office which is responsible for directing the pre-trial procedure, whilst also being likely to represent the public prosecution in judicial proceedings.

V. Conclusion

130. In the light of the foregoing, I propose that the Court should answer the questions referred by the Riigikohus (Supreme Court, Estonia) as follows:

1. Article 15(1) of Directive 2002/58/EC the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8, 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as meaning that the categories of data concerned and the duration of the period in respect of which access is sought should be included amongst the criteria for assessing the seriousness of the interference with fundamental rights that is associated with the access by competent national authorities to the personal data that providers of electronic communications services are obliged to retain under national legislation. It is for the referring court to assess, depending on the seriousness of the interference, whether that access was strictly necessary to achieve the objective of preventing, investigating, detecting and prosecuting criminal offences.

66 C-293/12 and C-594/12, EU:C:2014:238.

67 According to the evidence submitted to the Court at the hearing, under Estonian law, that judicial review may be carried out at the end of the pre-trial procedure when a suspect, having been informed of the criminal file, decides to challenge a procedural document, or at the hearing.

2. Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8, 11 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as meaning that the requirement that the access of the competent national authorities to retained data be subject to prior review by a court or an independent administrative authority is not met where national legislation provides that such review is to be carried out by the public prosecutor's office which is responsible for directing the pre-trial procedure, whilst also being likely to represent the public prosecution in judicial proceedings.