ECLI:EU:C:2023:631

Provisional text

JUDGMENT OF THE COURT (First Chamber)

7 September 2023 (*)

(Reference for a preliminary ruling – Telecommunications – Processing of personal data in the electronic communications sector – Directive 2002/58/EC – Scope – Article 15(1) – Data retained by providers of electronic communications services and made available to authorities in charge of criminal proceedings – Subsequent use of those data in an investigation into misconduct in office)

In Case C-162/22,

REQUEST for a preliminary ruling under Article 267 TFEU from the Lietuvos vyriausiasis administracinis teismas (Supreme Administrative Court of Lithuania), made by decision of 24 February 2022, received at the Court on 3 March 2022, in the proceedings brought by

A.G.

other party:

Lietuvos Respublikos generalinė prokuratūra,

THE COURT (First Chamber),

composed of A. Arabadjiev, President of the Chamber, P.G. Xuereb (Rapporteur), T. von Danwitz, A. Kumin and I. Ziemele, Judges,

Advocate General: M. Campos Sánchez-Bordona,

Registrar: A. Lamote, Administrator,

having regard to the written procedure and further to the hearing on 2 February 2023,

after considering the observations submitted on behalf of:

– A.G., by G. Danėlius, advokatas,

– the Lithuanian Government, by S. Grigonis, V. Kazlauskaitė-Švenčionienė and V. Vasiliauskienė, acting as Agents,

– the Czech Government, by O. Serdula, M. Smolek and J. Vláčil, acting as Agents,

– the Estonian Government, by M. Kriisa, acting as Agent,

– Ireland, by M. Browne, A. Joyce and M. Tierney, acting as Agents, and by D. Fennelly, Barrister-at-Law,

– the French Government, by R. Bénard, acting as Agent,

– the Italian Government, by G. Palmieri, acting as Agent, and by A. Grumetto, avvocato dello Stato,

– the Hungarian Government, by Zs. Biró-Tóth and M.Z. Fehér, acting as Agents,

– the European Commission, by S.L. Kalėda, H. Kranenborg, P.-J. Loewenthal and F. Wilman, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 30 March 2023,

gives the following

Judgment

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) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11) (‘Directive 2002/58’).

2 The request has been made in proceedings brought by A.G. concerning the legality of decisions of the Lietuvos Respublikos generalinė prokuratūra (Prosecutor General’s Office of the Republic of Lithuania; ‘the Prosecutor General’s Office’) dismissing him from service as a public prosecutor.

Legal context

European Union law

3 Article 1 of Directive 2002/58, entitled ‘Scope and aim’, provides:

‘1. This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic

communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

…

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

4 Article 5 of that directive, entitled '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.'

5 Article 15 of that directive, entitled 'Application of certain provisions of Directive 95/46/EC', states, in paragraph 1 thereof:

'Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC [of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31)]. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) [TEU].'

Lithuanian law

The Law on electronic communications

6 Article 65(2) of the Lietuvos Respublikos elektroninių ryšių įstatymas (Law of the Republic of Lithuania on electronic communications) of 15 April 2004 (Žin., 2004, No 69-2382), in the version applicable to the facts in the main proceedings ('the Law on electronic communications'), 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 so that those authorities may use them for the purpose of combating serious crime.

7 In accordance with Annex 1 to the Law on electronic communications, the categories of data to be retained are as follows:

‘1. Data necessary to trace and identify the source of a communication: … 2. Data necessary to identify the destination of a communication: … 3. Data necessary to identify the date, time and duration of a communication: … 4. Data necessary to identify the type of communication: … 5. Data necessary to identify users’ communication equipment or what purports to be their equipment: … 6. Data necessary to identify the location of mobile communication equipment: …’

8 Under Article 77(4) of that law, 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 intelligence bodies and pre-trial investigation bodies, in accordance with the detailed rules laid down by the Lietuvos Respublikos baudžiamojo proceso kodeksas (Code of Criminal Procedure of the Republic of Lithuania; ‘the Code of Criminal Procedure’), to monitor the content of information transmitted over electronic communications networks.

The Law on criminal intelligence

9 Point 1 of Article 6(3) of the Lietuvos Respublikos kriminalinės žvalgybos įstatymas (Law of the Republic of Lithuania on criminal intelligence) of 2 October 2012 (Žin., 2012, No 122-6093), in the version applicable to the facts in the main proceedings (‘the Law on criminal intelligence’), provides that, if the conditions laid down by that law to justify a criminal intelligence operation are satisfied and subject to prior authorisation from the public prosecutor’s office or a court, criminal intelligence bodies are to have the power, in addition to those listed in paragraphs 1 and 2 of that article, to obtain information from providers of electronic communications services.

10 Article 8(1) of that law provides that an investigation is to be carried out by criminal intelligence bodies where, inter alia, information comes to light concerning the preparation or commission of a very serious, serious or less serious criminal offence or concerning persons who are preparing, committing or have committed such an offence. Article 8(3) of that law states that, if such an investigation reveals the existence of a criminal offence, a pre-trial investigation is to be initiated immediately.

11 Under point 5 of Article 19(1) of the Law on criminal intelligence, information from criminal intelligence 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. In accordance with paragraph 3 of that article, information from criminal intelligence operations relating to an act 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.

The Code of Criminal Procedure

12 Article 154 of the Code of Criminal Procedure provides that an investigator may, by decision of an investigating judge taken at the request of the public prosecutor’s office, listen to and transcribe conversations transmitted over electronic communications networks and monitor, record and store other information transmitted over electronic communications networks if, inter alia, 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.

13 Article 177(1) of that code provides 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 only in so far as such disclosure is justified.

14 For the purpose of implementing Article 177 of that code, the Ikiteisminio tyrimo duomenų teikimo ir panaudojimo ne baudžiamojo persekiojimo tikslais ir ikiteisminio tyrimo duomenų apsaugos rekomendacijos (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 I-279 of the Prosecutor General of 17 August 2017 (TAR, 2017, No 2017-13413), as last amended by Decree No I-211 of 25 June 2018, are applicable.

15 Paragraph 23 of those recommendations provides that, upon receiving a request for access to investigation data, the public prosecutor is to decide whether such data should be provided. If the decision is taken to provide them, the public prosecutor must specify to what extent the data covered by the request may be provided.

The dispute in the main proceedings and the question referred for a preliminary ruling

16 The Prosecutor General's Office opened an internal investigation into the appellant in the main proceedings, who at the time was a public prosecutor in a Lithuanian public prosecutor's office, on the ground that there was reason to believe that he had, when leading a pre-trial investigation, unlawfully provided information pertaining to that pre-trial investigation to the suspect and his lawyer.

17 In its report on that investigation, the Prosecutor General's Office found that the appellant in the main proceedings had in fact engaged in misconduct in office.

18 According to that report, that misconduct in office was demonstrated by the evidence obtained during the internal investigation. In particular, information obtained during criminal intelligence operations and data collected during two pre-trial investigations confirmed telephone communications between the appellant in the main proceedings and the suspect's lawyer in the pre-trial investigation led by the appellant in the main proceedings concerning the suspect. The report also noted that a court order had authorised the interception and recording of the content of information transmitted over electronic communications networks concerning the lawyer in question and that another court order had authorised the same measure concerning the appellant in the main proceedings.

19 On the basis of that report, the Prosecutor General's Office adopted two orders by which it, first, imposed the penalty of dismissal from service on the appellant in the main proceedings and, second, dismissed him from service.

20 The appellant in the main proceedings brought an action before the Vilniaus apygardos administracinis teismas (Regional Administrative Court, Vilnius, Lithuania), requesting, inter alia, that those two orders be set aside.

21 By judgment of 16 July 2021, that court dismissed the action brought by the appellant in the main proceedings, on the ground, inter alia, that the criminal intelligence operations carried out in the present case were lawful and that the information gathered in accordance with the provisions of the Law on criminal intelligence had been used lawfully to assess whether the appellant in the main proceedings had engaged in misconduct in office.

22 The appellant in the main proceedings brought an appeal before the Lietuvos vyriausiasis administracinis teismas (Supreme Administrative Court of Lithuania), the referring court, claiming that access by the intelligence bodies, in connection with a criminal intelligence operation, to traffic data and the actual content of electronic communications constituted such a serious interference with fundamental rights that, having regard to the provisions of Directive 2002/58 and the Charter of Fundamental Rights of the European Union ('the Charter'), such access could be granted only for the purpose of combating serious crime. However, Article 19(3) of the Law on criminal intelligence provides that such data may be used to investigate not only serious criminal offences, but also disciplinary misconduct or misconduct in office related to acts of corruption.

23 According to the referring court, the issues raised by the appellant in the main proceedings involve two elements: (i) access to data retained by providers of electronic communications services for purposes other than combating serious crime and preventing serious threats to public security; and (ii) once such access has been obtained, the use of those data in investigating corruption-related misconduct in office.

24 The referring court recalls that it is apparent from the Court's case-law, in particular the judgment of 6 October 2020, *Privacy International* (C-623/17, EU:C:2020:790, paragraph 39), that Article 15(1) of Directive 2002/58, read in conjunction with Article 3 thereof, must be interpreted as meaning that the scope of that directive extends not only to a legislative measure that requires providers of electronic communications services to retain traffic data and location data, but also to a legislative measure requiring them to grant the competent national authorities access to those data. Moreover, it follows from that case-law, in particular from the judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)* (C-746/18, EU:C:2021:152, paragraphs 33 and 35), that, so far as concerns the objective of preventing, investigating, detecting and prosecuting criminal offences, in accordance with the principle of proportionality, only action to combat serious crime and measures to prevent serious threats to public security are capable of justifying serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, such as the interference entailed by the retention of traffic and location data, whether the retention be general and indiscriminate or targeted.

25 However, the Court has not yet ruled on the impact of the subsequent use of the data concerned on the interference with fundamental rights. In those circumstances, the referring court harbours doubts as to whether such subsequent use must also be regarded as constituting such a serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter that it can be justified only for the purposes of combating serious crime and preventing serious threats to public security, thus denying the possibility of using the data concerned for the investigation of corruption-related misconduct in office.

26 In those circumstances, the Lietuvos vyriausiasis administracinis teismas (Supreme Administrative Court of Lithuania) decided to stay the proceedings and to refer 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], 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?'

Consideration of the question referred

27 By its question, the referring court asks, in essence, whether Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding the use, in connection with investigations into corruption-related misconduct in office, of personal data relating to electronic communications which have been retained, pursuant to a legislative measure adopted under that provision, by providers of electronic communications services and which have subsequently been made available, pursuant to that measure, to the competent authorities for the purpose of combating serious crime.

28 As a preliminary point, it is apparent from the order for reference that, although the administrative file relating to the proceedings that gave rise to the orders at issue in the main proceedings, referred to in paragraph 19 above, also included information that had been gathered by the competent authorities through the interception and registration of electronic communications that had been authorised, for the purposes of criminal prosecutions, by two court orders, the fact remains that the referring court does not harbour doubts as to the use of personal data that were obtained without the involvement of providers of electronic communications services, but harbours doubts as to the subsequent use of personal data that have been retained by such providers on the basis of a legislative measure of the Member State imposing such a retention obligation on them, on the basis of Article 15(1) of Directive 2002/58.

29 In that regard, it follows from the information in the request for a preliminary ruling that the data to which the question referred relates are the data retained pursuant to Article 65(2) of the Law on electronic communications, read in conjunction with Annex 1 to that law, which imposes on providers of electronic communications services an obligation to retain, generally and indiscriminately, traffic and location data relating to such communications for the purpose of combating serious crime.

30 As regards the conditions under which those data may be used during an internal procedure concerning corruption-related misconduct in office, it must first of all be recalled that access to those data may be granted, pursuant to a measure adopted under Article 15(1) of Directive 2002/58, only in so far as those data have been retained by those providers in a manner that is consistent with that provision (see, to that effect, judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C-746/18, EU:C:2021:152, paragraph 29 and the case-law cited). Next, subsequent use of traffic and location data relating to such communications for the purpose of combating serious crime is possible only on condition, first, that the retention of those data by providers of electronic communications services was consistent with Article 15(1) of Directive 2002/58, as interpreted by the case-law of the Court, and, second, that the access to those data granted to the competent authorities was itself consistent with that provision.

31 In that regard, the Court has already held that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, precludes legislative measures which provide, on a preventative basis, for the purposes of combating serious crime and preventing serious threats to public security, for the general and indiscriminate retention of traffic and location data (judgment of 20 September 2022, *SpaceNet and Telekom Deutschland*, C-793/19 and C-794/19, EU:C:2022:702, paragraphs 74 and 131 and the case-law cited). However, the Court specified that Article 15(1), read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not preclude legislative measures that, for the purposes of combating serous crime and preventing serious threats to public security, provide for:

– the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary, but which may be extended;

– the general and indiscriminate retention of IP addresses assigned to the source of an internet connection for a period that is limited in time to what is strictly necessary;

– the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems; and

– recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the expedited retention of traffic and location data in the possession of those service providers,

provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse (judgment of 20 September 2022, *SpaceNet and Telekom Deutschland*, C-793/19 and C-794/19, EU:C:2022:702, paragraph 75 and the case-law cited).

32 As regards the objectives capable of justifying the use, by public authorities, of data retained by providers of electronic communications services pursuant to a measure in accordance with those provisions, it must be recalled that Article 15(1) of Directive 2002/58 enables the Member States to introduce exceptions to the obligation of principle, laid down in Article 5(1) of that directive, to ensure the confidentiality of personal data, and to the corresponding obligations, referred to, inter alia, in Articles 6 and 9 of that directive, where such a restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence and public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system. To that end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on one of those grounds (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 110).

33 Article 15(1) of Directive 2002/58 cannot permit the exception to the obligation of principle to ensure the confidentiality of electronic communications and data relating thereto and, in particular, to the prohibition on storage of those data, laid down in Article 5 of that directive, to become the rule, if the latter provision is not to be rendered largely meaningless (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 40).

34 As regards the objectives that are capable of justifying a limitation of the rights and obligations laid down, in particular, in Articles 5, 6 and 9 of Directive 2002/58, the Court has previously held that the list of objectives set out in the first sentence of Article 15(1) of that directive is exhaustive, as a result of which a legislative measure adopted under that provision must correspond, genuinely and strictly, to one of those objectives (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 41).

35 As regards the public interest objectives that may justify a measure taken pursuant to Article 15(1) of Directive 2002/58, it is clear from the Court’s case-law that, in accordance with the

principle of proportionality, there is a hierarchy amongst those objectives according to their respective importance and that the importance of the objective pursued by such a measure must be proportionate to the seriousness of the interference that it entails (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 56).

36 In that regard, the importance of the objective of safeguarding national security, read in the light of Article 4(2) TEU, according to which national security remains the sole responsibility of each Member State, exceeds that of the other objectives referred to in Article 15(1) of Directive 2002/58, inter alia the objectives of combating crime in general, even serious crime, and of safeguarding public security. Subject to meeting the other requirements laid down in Article 52(1) of the Charter, the objective of safeguarding national security is therefore capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by those other objectives (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 57 and the case-law cited).

37 As regards the objective of preventing, investigating, detecting and prosecuting criminal offences, the Court held that, in accordance with the principle of proportionality, only action to combat serious crime and measures to prevent serious threats to public security are capable of justifying serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, such as the interference entailed by the retention of traffic and location data. Accordingly, only non-serious interference with those fundamental rights may be justified by the objective of preventing, investigating, detecting and prosecuting criminal offences in general (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 59 and the case-law cited).

38 It follows from that case-law that, although the fight against serious crime and the prevention of serious threats to public security are of lesser importance in the hierarchy of objectives of public interest than the safeguarding of national security (see, to that effect, judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 99), their importance is however greater than that of fighting crime generally and of preventing non-serious threats to public security.

39 In that context, it must nevertheless be recalled that, as is also apparent from paragraph 31 above, the question whether the Member States may justify a limitation on the rights and obligations laid down, inter alia, in Articles 5, 6 and 9 of Directive 2002/58 must be assessed by measuring 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 (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 131).

40 Moreover, the Court has already held that 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 that directive, 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 (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 98 and the case-law cited).

41 Those considerations apply *mutatis mutandis* to the subsequent use of traffic and location data retained by providers of electronic communications services pursuant to a measure adopted

under Article 15(1) of Directive 2002/58 for the purpose of combating serious crime. Once they have been retained and made available to the competent authorities for the purpose of combating serious crime, such data cannot be transmitted to other authorities and used in order to achieve objectives, such as, in the present case, combating corruption-related misconduct in office, which are of lesser importance in the hierarchy of objectives of public interest than the objective of combating serious crime and preventing serious threats to public security. To authorise, in that situation, access to retained data and the use thereof would be contrary to that hierarchy of public interest objectives recalled in paragraphs 33, 35 to 37 and 40 above (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 99).

42 As regards the argument raised by the Czech Government and by Ireland in their written observations that disciplinary proceedings concerning corruption-related misconduct in office could be connected with the safeguarding of public security, it is sufficient to note that, in its order for reference, the referring court has not indicated any serious threat to public security.

43 Furthermore, while it is true that internal investigations into disciplinary misconduct or misconduct in office related to acts of corruption may play an important role in the fight against such acts, a legislative measure providing for such investigations does not correspond, genuinely and strictly, to the objective of the prosecution and punishment of criminal offences, referred to in the first sentence of Article 15(1) of Directive 2002/58, which covers only criminal prosecutions.

44 In the light of the foregoing, the answer to the question referred is that 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 the use, in connection with investigations into corruption-related misconduct in office, of personal data relating to electronic communications which have been retained, pursuant to a legislative measure adopted under that provision, by providers of electronic communications services and which have subsequently been made available, pursuant to that measure, to the competent authorities for the purpose of combating serious crime.

Costs

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

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

Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union,

must be interpreted as precluding the use, in connection with investigations into corruption-related misconduct in office, of personal data relating to electronic communications which have been retained, pursuant to a legislative measure adopted under that provision, by providers of electronic communications services and which have subsequently been made available, pursuant to that measure, to the competent authorities for the purpose of combating serious crime.

[Signatures]

---

* Language of the case: Lithuanian.