OPINION OF ADVOCATE GENERAL KOKOTT

delivered on 18 July 2007 [1]

I — Introduction

1. This case illustrates that the storage of data for specified purposes creates the desire to use those data more extensively. In Spain, providers of access to the Internet are required to store certain data of individual users so that those data can be used, where appropriate, in criminal investigations or for the protection of public security and for national defence. Now an association of holders of copyrights is seeking to identify, with the aid of those data, users who have infringed copyrights by the exchange of files.

2. The referring court would therefore like to know whether Community law allows or even requires the communication of personal traffic data on the use of the Internet to the holders of intellectual property. It assumes that various directives on the protection of intellectual property and the information society grant the holders of corresponding legal positions a claim against the providers of electronic services to the communication of such data if those data can prove an infringement of property rights.

3. However, I shall show below that the provisions of Community law on data protection in the electronic communications sector allow the communication of personal traffic data only to the competent State authorities, but not direct communication to holders of copyrights wishing to bring civil-law actions against the infringement of their rights.

II — Legal framework

A — *Community law*

4. In the present case, provisions on the protection of intellectual property and on

1 — Original language: German.

electronic commerce as well as, in particular, the provisions on data protection are of interest.

1. The protection of intellectual property in the information society

5. With regard to the protection of intellectual property in the information society, Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2] must be mentioned first.

6. Article 1(5) of Directive 2000/31 delimits its scope. Under Article 1(5)(b), the Directive does not apply to 'questions relating to information society services covered by Directives 95/46/EC and 97/66/EC'. [3]

2 — OJ 2000 L 178, p. 1.

3 — The directives referred to are 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) and Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (OJ 1998 L 24, p. 1).

7. Article 15(2) of Directive 2000/31 states:

'Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.'

8. Article 18(1) of Directive 2000/31 is worded as follows:

'Member States shall ensure that court actions available under national law concerning information society services' activities allow for the rapid adoption of measures, including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved.'

9. Special provisions on the protection of intellectual property in electronic commerce are contained in Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. [4] Article 8 in particular, headed 'Sanctions and remedies', is of interest:

'1. Member States shall provide appropriate sanctions and remedies in respect of infringements of the rights and obligations set out in this Directive and shall take all the measures necessary to ensure that those sanctions and remedies are applied. The sanctions thus provided for shall be effective, proportionate and dissuasive.

2. Each Member State shall take the measures necessary to ensure that rightholders whose interests are affected by an infringing activity carried out on its territory can bring an action for damages and/or apply for an injunction and, where appropriate, for the seizure of infringing material as well as of devices, products or components referred to in Article 6(2).

3. …'

10. Article 9 of Directive 2001/29 restricts its application as follows:

'This Directive shall be without prejudice to provisions concerning in particular patent rights, trade marks, design rights, utility models, topographies of semi-conductor products, type faces, conditional access, access to cable of broadcasting services, protection of national treasures, legal deposit requirements, laws on restrictive practices and unfair competition, trade secrets, security, confidentiality, data protection and privacy, access to public documents, the law of contract.'

11. Article 8 of Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights [5] provides for a special right of information for holders of intellectual property:

'1. Member States shall ensure that, in the context of proceedings concerning an infringement of an intellectual property right and in response to a justified and proportionate request of the claimant, the

4 — OJ 2001 L 167, p. 10.

5 — OJ 2004 L 157, p. 45; the corrected version published in OJ 2004 L 195, p. 16, has been used.

competent judicial authorities may order that information on the origin and distribution networks of the goods or services which infringe an intellectual property right be provided by the infringer and/or any other person who:

…

(c) was found to be providing on a commercial scale services used in infringing activities;

…

2. The information referred to in paragraph 1 shall, as appropriate, comprise:

(a) the names and addresses of the producers, manufacturers, distributors, suppliers and other previous holders of the goods or services, as well as the intended wholesalers and retailers;

(b) …

3. Paragraphs 1 and 2 shall apply without prejudice to other statutory provisions which:

(a) — (d) …

or

(e) govern the protection of confidentiality of information sources or the processing of personal data.'

12. At the same time, according to Article 2(3), Directive 2004/48 does not affect:

'(a) the Community provisions governing the substantive law on intellectual property, Directive 95/46/EC, Directive 1999/93/EC or Directive 2000/31/EC, in general, and Articles 12 to 15 of Directive 2000/31/EC in particular;

(b) …'

2. The provisions on data protection

13. With regard to data protection, 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 [6] is relevant.

14. It 'harmonises [according to Article 1(1)] the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, 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.'

15. Under Article 1(2), the provisions of that directive particularise and complement 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 [7] for the purposes mentioned in paragraph 1.

16. Article 2(b) of Directive 2002/58 defines the term 'traffic data' as 'any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.'

17. The processing of traffic data is regulated by Article 6:

'1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).

2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing

6 — OJ 2002 L 201, p. 37.
7 — OJ 1995 L 281, p. 31.

is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

3. — 5. …

6. Paragraphs 1, 2, 3 and 5 shall apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.'

18. The reservation in Article 15(1), mentioned in Article 6(1) of Directive 2002/58, reads as follows:

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

19. It is explained in recital 11 in the preamble:

'(11) Like Directive 95/46/EC, this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States

to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.'

20. Article 19 of Directive 2002/58 regulates that directive's relationship to its predecessor, Directive 97/66:

'Directive 97/66/EC is hereby repealed with effect from the date referred to in Article 17(1).

References made to the repealed Directive shall be construed as being made to this Directive.'

21. Article 13(1) of Directive 95/46, referred to in Article 15(1) of Directive 2002/58, is worded as follows:

'1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others.'

22. In addition, it should be pointed out that an independent working party composed of representatives of the data protection supervisory authorities of the Member States ('the Data Protection Working Party) [8] was set up under Article 29 of Directive 95/46. Its task is to give opinions on questions covering data protection legislation. A similar function is assigned to the Data Protection Supervisor established under Article 286 EC and Regulation No 45/2001. [9]

23. Finally, Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [10] is also of interest for the purposes of this case.

24. Directive 2006/24 requires Member States to retain inter alia traffic data relating to Internet traffic. Under Article 15, it must be transposed by 15 September 2007 but allows retention in relation to Internet traffic to be postponed by a further 18 months. Spain has not made use of that possibility.

25. Article 11 of Directive 2006/24 inserts a new paragraph 1a in Article 15 of Directive 2002/58:

'Paragraph 1 shall not apply to data specifically required by Directive 2006/24/EC … to be retained for the purposes referred to in Article 1(1) of that Directive.'

8 — The documents of the Data Protection Working Party are available at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm.

9 — Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ 2001 L 8, p. 1).

10 — OJ 2006 L 105, p. 54.

26. The communication of data retained under Directive 2006/24 is regulated in Article 4:

‘Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of European Union law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights.’

B — *Spanish law*

27. The referring court confines itself essentially, in setting out the legal framework under national law, to Article 12(1) to (3) of Ley 34/2002, de 11 de Julio 2002, de Servicios de la Sociedad de la Información y de Comercio Electrónico (Law 34/2002 of 11 July 2002 on information society services and electronic commerce):

‘Article 12. Duty to retain traffic data relating to electronic communications

1. Operators of electronic communications networks and services, providers of access to telecommunications networks and providers of data storage services must retain for a maximum of 12 months the connection and traffic data generated by the communications established during the supply of an information society service, under the conditions established in this article and the regulations implementing it.

2. … The operators of electronic communications networks and services and the service providers to which this article refers may not use the data retained for purposes other than those indicated in the paragraph below or other purposes permitted by the Law and must adopt appropriate security measures to avoid the loss or alteration of the data and unauthorised access to the data.

3. The data shall be retained for use in the context of a criminal investigation or to safeguard public security and national defence, and shall be made available to the courts or the public prosecutor at their request. Communication of the data to the forces of order shall be effected in accordance with the provisions of the rules on personal data protection.'

28. The referring court also states that the infringement of copyright is a criminal offence in Spain only if the act is committed with the intention to make a profit. [11]

III — Technical background, facts and main proceedings

29. The applicant in the main proceedings (Productores de Música de España, 'Promusicae') is a non-profit-making association of producers and publishers of musical recordings and audiovisual presentations which are essentially musical. It lodged an application against a Spanish provider of Internet access, Telefónica de España SAU, requesting that the company be ordered to disclose the names and addresses of certain Internet users. Promusicae identified those persons by IP addresses and by the date and time of their use.

30. The IP address is a numerical address format, comparable to a telephone number, which enables networked devices such as webservers, e-mail servers or private computers to communicate with one another on the Internet. Thus, the server via which Court of Justice pages are retrieved has the IP address 147.67.243.28. [12] When a page is retrieved, the address of the retrieving computer is communicated to the computer on which the page is stored, so that the data can be routed from one computer to the other via the Internet.

31. Static IP addresses may be assigned in order to connect private users to the Internet, in similar fashion to connection to the telephone network. However, that is rather rare, since the Internet is at present still organised in such a way that each access provider has only a limited number of addresses avail-

11 — It refers in this connection to Circular 1/2006, 5 de mayo de 2006, sobre los delitos contra la propiedad intelectual e industrial tras la reforma de la Ley Orgánica 15/2003, http://www.fiscal.es/csblob/CIRCULAR%201-2006.doc?blobcol=urldata&blobheader=application%2Fmsword&blobkey=id&blobtable=MungoBlobs&blobwhere=1109248064092&ssbinary=true, p. 37 et seq., issued by the Fiscalía General del Estado.

12 — According to www.dnsstuff.com.

able to it.[13] Consequently, in most cases, including this one, dynamic IP addresses are used, which means that the access provider assigns its customers an address, on an ad hoc basis, from its quota of addresses every time they access the Internet. That address may naturally change each time a customer dials up.

32. Promusicae claims that it identified a number of IP addresses which were used at certain times for the purpose of 'file sharing' in respect of music files to which the its members hold the exploitation rights.

33. File sharing is a form of exchange of files containing, for example, pieces of music or films. Users first copy the files onto their computers and then offer them to anyone who is in contact with them via the Internet and a particular program, in this case Kazaa. Normally, in such cases,[14] the IP address of the person offering the file to others for retrieval is used, and can thus be detected.

34. In order to take action against such users, Promusicae claims that the access provider concerned, Telefónica, should inform it which users were assigned the IP addresses identified by it at the times specified by it. Telefónica is able to find out which connection was used in each case, since it retains, after the connection has ended, the details concerning to whom and when it assigned a particular IP address.

35. The referring court first gave a ruling requiring Telefónica to provide the desired information. However, Telefónica objected that, pursuant to Article 12 of the Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, it could in no circumstances provide the court with the information. The electronic communications operator or service provider is allowed to supply the information which he is required by law to retain only in connection with a criminal investigation, or if it is necessary in order to protect public safety, or if national security is involved.

36. The referring court considers it possible that that view is correct under Spanish law, but takes the view that the provision in ques-

13 — See, in that regard, Communication from the Commission to the Council and the European Parliament — Next Generation Internet — priorities for action in migrating to the new Internet protocol IPv6, COM(2002) 96.

14 — Technically it also appears to be possible to conceal one's own IP address. However, such services involve a cost and/or are slow. See the Wikipedia entry Anonymous P2P, http://en.wikipedia.org/wiki/Anonymous_p2p, and Working Document WP 37 of the Data Protection Working Party of 21 November 2000, Privacy on the Internet, p. 86 et seq., which does not yet take file sharing into account.

tion is then incompatible with Community law. It therefore refers the following question to the Court of Justice for a preliminary ruling:

'Does Community law, specifically Articles 15(2) and 18 of Directive 2000/31, Article 8(1) and (2) of Directive 2001/29, Article 8 of Directive 2004/48, and Articles 17(2) and 47 of the Charter, permit Member States to limit to the context of a criminal investigation or to safeguard public security and national defence, thus excluding civil proceedings, the duty of operators of electronic communications networks and services, providers of access to telecommunications networks and providers of data storage services to retain and make available connection and traffic data generated by the communications established during the supply of an information society service?'

37. Promusicae, Telefónica, Finland, Italy, Slovenia, the United Kingdom und the Commission took part in the proceedings. The Data Protection Working Party [15] and the European Data Protection Supervisor were not involved, in particular because Article 23 of the Statute of the Court of Justice does not provide for their participation. However, since they are able to make an important contribution to the discussion of legal issues concerning data protection, I have devoted particular attention at least to their published opinions on the questions raised here.

IV — Legal assessment

38. The Court is required to clarify whether it is compatible with the directives mentioned by the referring court to restrict the obligation to communicate connection data to criminal prosecutions and similar proceedings, but to exclude from it civil proceedings.

39. The referring court thus takes the view that there is a contradiction between Spanish law and Community law. However, in so doing, it fails to take into account the fact

15 — See point 22 above.

that the provision of Spanish law referred to is based on Article 15 of Directive 2002/58 and largely incorporates its wording. That directive contains provisions on data protection in the electronic communications sector and in that respect supplements Directive 95/46 containing general provisions on data protection.

40. It must therefore be examined whether it is compatible with the provisions mentioned by the referring court, having regard to the provisions on data protection, to prohibit providers of Internet access from identifying the holders of subscriber lines in order to enable civil proceedings for copyright infringements.

B — *The relationship of the various directives to each other*

A — *Admissibility of the request*

41. There could be doubts as to the admissibility of the request for a preliminary ruling in terms of its relevance to a decision. [16] A directive cannot of itself impose obligations on an individual. [17] If Spanish law unquestionably precluded communication of the data at issue, even the interpretation of directives requested by the referring court could not lead to Telefónica's being obliged to communicate them. On the basis of the available information, however, it is conceivable that Spanish law could be interpreted in conformity with the directives. As long as that possibility exists, a request for a preliminary ruling such as this one cannot be regarded as irrelevant. [18]

42. Certain parties concentrate — almost exclusively — on the interpretation of the directives mentioned by the referring court. In so doing, they invariably emphasise the necessity of effective legal protection against infringements of copyright. The Commission, on the other hand, rightly points out that none of the three directives affects the law on data protection.

16 — See Case C-3/04 *Poseidon Chartering* [2006] ECR I-2505, paragraph 14, and Case C-217/05 *Confederación Española de Empresarios de Estaciones de Servicio* [2006] ECR I-11987, paragraph 17, both with further references.

17 — Joined Cases C-397/01 to C-403/01 *Pfeiffer and Others* [2004] ECR I-8835, paragraph 108, and Joined Cases C-387/02, C-391/02 and C-403/02 *Berlusconi and Others* [2005] ECR I-3565, paragraph 73.

18 — See Case C-105/03 *Pupino* [2005] ECR I-5285, paragraph 31 et seq., in particular paragraph 48.

43. Under Article 1(5)(b) of Directive 2000/31 on electronic commerce, the Directive does not apply to questions relating to information society services covered by Directive 95/46 on data protection and Directive 97/66 concerning the processing of personal data and the protection of privacy in the telecommunications sector. The last-mentioned directive has since been replaced by Directive 2002/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

44. In the same way, Article 9 of Directive 2001/29 on the harmonisation of certain aspects of copyright and related rights in the information society expressly states that the directive is without prejudice to, inter alia, provisions concerning data protection and privacy.

45. The relationship of Directive 2004/48 on the enforcement of intellectual property rights to data protection is somewhat less clear. Article 2(3)(a) provides that that directive does not affect Directive 95/46. Promusicae infers from this that Directive 2002/58, which is not mentioned in that provision, is not applicable within the field of application of Directive 2004/48.

46. That argument could be intended to mean that, under the principle *lex posterior derogat legi priori*, Directive 2004/48 takes precedence over Directive 2002/58, but not over Directive 95/46 which is expressly made an exception. However, that argument must be answered by pointing out that, according to Article 1(2), Directive 2002/58 is intended to particularise and complement Directive 95/46. Directive 2004/48 does not lay claim to that function. Rather, according to the second recital in the preamble, the protection of intellectual property which it brings about should not hamper the protection of personal data, including on the Internet. However, it would be inconsistent to allow particularising and complementing provisions which relate, in particular, to the protection of data on the Internet, which expressly must not be impaired, to be overridden without being replaced, but to continue to accord respect to the general provisions. Instead, it is more logical to extend the reservation in favour of Directive 95/46 to Directive 2002/58.

47. A further point in favour of that conclusion, as regards the right of information under Article 8(1) and (2) to be considered here, is that, according to Article 8(3)(e), those paragraphs apply without prejudice to other statutory provisions which govern the processing of personal data. That additional express emphasis on data protection was not

yet reflected in the Commission's Proposal, but was incorporated in the Directive during the discussions in the Council and in the Parliament.[19] Directive 2002/58 contains precisely such provisions and is therefore not infringed, at least not by the right of information under Article 8 of Directive 2004/48 at issue here.

48. It should additionally be pointed out that even the TRIPS Agreement[20] does not require data protection to be overridden by Directive 2004/48. Promusicae rightly submits that Articles 41 and 42 of TRIPS require effective protection for intellectual property and in particular that access to the courts for legal protection must be possible. However, a right of information is only provided for directly vis-à-vis infringers in Article 47 of TRIPS.[21] The Contracting States may introduce such a right, but according to the wording of Article 47 of TRIPS, are not required to do so.[22] The extension by Article 8 of Directive 2004/48 of the duty to provide information to include third parties goes even beyond that option. It can therefore be restricted by data protection without any conflict with the TRIPS Agreement.

49. All three directives mentioned by the referring court thus cede precedence to the Data Protection Directives, 95/46 and 2002/58. Contrary to what has been submitted by some parties, that does not mean that data protection enjoys priority over the aims of those directives. Rather, a reasonable balance between data protection and those aims must be struck in the context of the Data Protection Directives.

C — *Data protection*

50. The secondary legislation relevant to the present case is Directive 2002/58 containing provisions on data protection in the elec-

19 — Compare Article 9(3)(e) of the Commission's Proposal (COM/2003/46) with the same provision of the Council's consolidated draft of 19 December 2003 (Council document 16289/03) and with Article 8(3)(e) of the draft revised by the Parliament (OJ 2004 C 102 E, p. 242 et seq.), which was adopted unchanged by the Council.

20 — Agreement on Trade-Related Aspects of Intellectual Property Rights, which is to be found in Annex 1 C to the Agreement establishing the World Trade Organisation, which was approved on behalf of the Community, as regards matters within its competence, by Council Decision 94/800/EC of 22 December 1994 (OJ 1994 L 336, p. 1).

21 — The fourth sentence of Article 42 of TRIPS could, admittedly, in its German version, be (mis)construed as meaning that effective legal protection must provide for the discovery of confidential information, yet, on the contrary, that provision is intended to protect confidential information in judicial proceedings, if that is permissible. This is more clearly apparent in the authentic language versions (English, French and Spanish). As here, also Daniel Gervais, *The TRIPS Agreement, Drafting History and Analysis*, London 2003, p. 291.

22 — That is also the view of the Council and the Commission in the context of the procedure for the adoption of Directive 2004/48 (Council document 6052/04 of 9 February 2004, p. 6 et seq.).

tronic communications sector, together with Directive 95/46 which regulates data protection in general. The Court, however, derives important criteria for the interpretation of those provisions of secondary legislation from the foundations of data protection, which lie in fundamental rights.

1. The link between data protection and fundamental rights

51. Data protection is based on the fundamental right to private life, as it results in particular from Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms signed at Rome on 4 November 1950 ('the ECHR'). [23] The Charter of fundamental rights of the European Union, proclaimed at Nice on 7 December 2000 [24] ('the Charter'), confirmed that fundamental right in Article 7, and in Article 8 specifically emphasised the fundamental right to the protection of personal data, including important fundamental principles of data protection.

52. The communication of personal data to a third party, whatever the subsequent use of the information thus communicated, therefore constitutes an infringement of the right of the person concerned to respect for private life and consequently an interference within the meaning of Article 8 of the ECHR. [25]

53. Such an interference violates Article 8 of the ECHR unless it is 'in accordance with the law'. [26] It must therefore, in accordance with the requirement of foreseeability, be formulated with sufficient precision to enable the citizen to adjust his conduct accordingly. [27] The requirement of foreseeability has found particular expression in data protection law in the criterion — expressly mentioned in Article 8(2) of the Charter — of purpose limitation. Pursuant to the specific embodiment of the purpose limitation criterion in Article 6(1)(b) of Directive 95/46, personal data may be collected only for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

54. In addition, any interference with private life — the processing of personal data —

23 — Joined Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others* [2003] ECR I-4989, paragraph 73 et seq.

24 — OJ 2000 C 364, p. 1.

25 — *Österreichischer Rundfunk and Others*, cited in footnote 23, paragraph 74.

26 — *Österreichischer Rundfunk and Others*, cited in footnote 23, paragraph 76.

27 — *Österreichischer Rundfunk and Others*, cited in footnote 23, paragraph 77, invoking the case-law of the European Court of Human Rights.

must be proportionate to the aims pursued. [28] There must therefore be a pressing social need and the measure must be in reasonable proportion to the legitimate aim pursued. [29]

55. In the context of legitimate aims, the relevant fundamental rights of the holders of copyrights, in particular the protection of property and the right to effective judicial protection, will have to be taken into account in the present case. According to settled case-law, both those rights form part of the general principles of Community law, [30] as confirmed by Article 17 and Article 47 of the Charter. Article 17(2) of the Charter emphasises in this connection that intellectual property also falls within the protective scope of the fundamental right to property. [31]

56. The balance between the relevant fundamental rights must first be struck by the Community legislature and, in the interpretation of Community law, by the Court. However, the Member States are also obliged to observe it when using up any remaining margin for regulation in the implementation of directives. Moreover, the authorities and courts of the Member States are not only required to interpret their national law in conformity with the Data Protection Directives, but also to ensure that they do not act on the basis of an interpretation of those directives which conflicts with the fundamental rights protected by the Community legal order or the other general principles of Community law. [32]

2. Applicability of the Data Protection Directives

57. The secondary legislation gives concrete expression to the requirements as regards fundamental rights for data protection and extends them in a respect which is one of the decisive factors in this case. The directives not only provide for a binding obliga-

28 — *Österreichischer Rundfunk and Others*, cited in footnote 23, paragraph 80.

29 — *Österreichischer Rundfunk and Others*, cited in footnote 23, paragraph 83, invoking the case-law of the European Court of Human Rights.

30 — See, with regard to property, for instance, Case 265/87 *Schräder* [1989] ECR 2237, paragraph 15; Case C-200/96 *Metronome Musik* [1998] ECR I-1953, paragraph 21; and Joined Cases C-453/03, C-11/04, C-12/04 and C-194/04 *ABNA and Others* [2005] ECR I-10423, paragraph 87, and, with regard to effective judicial protection, Case 222/84 *Johnston* [1986] ECR 1651, paragraphs 18 and 19; Case 222/86 *Heylens and Others* [1987] ECR 4097, paragraph 14; Case C-50/00 P *Unión de Pequeños Agricultores* v *Council* [2002] ECR I-6677, paragraph 39; and Case C-432/05 *Unibet* [2007] ECR I-2271, paragraph 37.

31 — See *Metronome Musik*, cited in footnote 30, paragraphs 21 and 26, and, most recently, Eur. Court HR, *Anheuser-Busch Inc.* v. *Portugal* judgment of 11 January 2007 (Application No 73049/01, § 72).

32 — See Case C-101/01 *Lindqvist* [2003] ECR I-12971, paragraph 87.

tion for governmental authorities to protect data, but also extend it to individuals except in so far as, pursuant to the second indent of Article 3(2) of Directive 95/46, the activity concerned is carried out by a natural person in the course of a purely personal or household activity. [33] The Community thereby fulfils and gives concrete expression to an objective of protection resulting from the fundamental right to data protection. [34]

58. The bringing of civil proceedings against copyright infringements by Promusicae and the processing of connection data by Telefónica are not to be categorised as personal or household activities. That is also apparent, with regard to the processing of connection data, from the existence of Directive 2002/58, which does not include the exemption for personal and household activities, but assumes that the processing of personal data by providers of electronic communications services is in principle subject to data protection. Transmission of such data between private undertakings is therefore not excluded from the scope of data protection. Consequently, it must be examined whether the other conditions for the application of data protection law are fulfilled in this case.

59. Directive 2002/58, as provided in Article 3(1), applies to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community. Under Article 2 of Directive 2002/58, those concepts are defined in Directive 95/46 and Directive 2002/21. [35]

60. The provision of access to the Internet is a publicly available electronic communications service within the meaning of Article 2(c) of Directive 2002/21, that is, a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks.

61. The indication of which users were assigned particular IP addresses at particular times consists of personal data under Article 2(a) of Directive 95/46, namely infor-

33 — See *Lindqvist*, cited in footnote 32, paragraph 46 et seq.

34 — With regard to the secrecy of telecommunications, the German Bundesverfassungsgericht (Federal Constitutional Court), in its orders of 9 October 2002 (1 BvR 1611/96 and 1 BvR 805/98, BVerfGE 106, 28 [37], paragraph 21 of the version on www.bundesverfassungsgericht.de) and 27 October 2006 (1 BvR 1811/99, *Multimedia und Recht* 2007, 308, paragraph 13 of the version on www.bundesverfassungsgericht.de), even assumes a corresponding State duty of protection. However, the question whether private individuals' duties as regards data protection under Community law are also based on a mandatory Community duty of protection does not need to be determined in this case.

35 — Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (OJ 2002 L 108, p. 33).

mation relating to identified or identifiable [36] natural persons. With the aid of those data, the actions performed using the IP address concerned are linked to the subscriber.

62. In Article 2(b) of Directive 95/46, the disclosure of such data is expressly listed as an example of processing, that is, an operation performed by or without automatic means.

63. At the same time, at least the temporarily assigned IP addresses of users are traffic data according to the definition in Article 2(b) of Directive 2002/58, namely data which are processed for the purpose of the conveyance of a communication on an electronic communications network.

3. The applicable prohibitions on processing

64. Under Article 5(1) of Directive 2002/58, the confidentiality of communications also applies to the traffic data arising during the communications. In particular, the Member States must prohibit the storage and other kinds of interception or surveillance of traffic data by persons other than the users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1).

65. Article 6(1) of Directive 2002/58 makes it clear, with regard to any storage of traffic data during the operation of communications networks, that such data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of that article and Article 15(1).

36 — In so far as the respective holders of the IP addresses are identifiable due to the storage of the assignments by the provider of Internet access, this involves, as soon as the IP addresses are intercepted by Promusicae, the processing of personal data, which must comply with the requirements of data protection; see the judgment of the Rechtbank Utrecht of 12 July 2005, *Brein* (194741/KGZA 05-462, Annex 5 to the written observations submitted by Promusicae, point 4.24 et seq.), Working Document WP 104 of the Data Protection Working Party of 18 January 2005 on data protection issues related to intellectual property rights, p. 4, and, under French law, the decisions (Délibérations) of the Commission nationale de l'informatique et des libertés (CNIL) 2005-235 of 18 October 2005 and 2006-294 of 21 December 2006 (available at http://www.legifrance.gouv.fr/WAspad/RechercheExperteCnil.jsp). The register of processing operations of the Agencia Española de Protección de Datos, https://www.agpd.es/index.php?idSeccion=100, contains a corresponding registration for Promusicae.

66. Both the storage and the communication of personal traffic data on Internet use must therefore be prohibited in principle.

4. The exceptions to the prohibitions on processing

67. However, there are also exceptions to those prohibitions on processing. They are set out in Article 6 and Article 15 of Directive 2002/58.

(a) The exceptions under Article 2002/58

68. Article 6(2), (3) and (5) of Directive 2002/58, expressly mentioned as exceptions in Article 6(1), are not an appropriate basis for overriding the prohibition on processing under Article 6(1) by communication to Promusicae.

69. Article 6(2) of Directive 2002/58 allows as an exception the processing of such traffic data where and in so far as they are necessary for the purposes of subscriber billing and interconnection payments. It is already doubtful whether that exception allows any storage at all of particulars concerning the persons to whom and times when a dynamic IP address was assigned. That information is not normally needed for the purpose of billing the access provider's charges. The standard billing methods are based on the duration of the dial-up connection to the access provider or on the volume of the data traffic generated by the user, if, that is, unrestricted use of access in return for a flat-rate amount has not been agreed. However, if processing of the IP address is not necessary for billing, it must not be stored for that purpose either. [37]

70. Irrespective of that, Article 6(2) is in any event not an appropriate basis for the communication of traffic data to third parties wishing to take action against the user for acts committed using that IP address. Such proceedings have no connection with subscriber billing or interconnection payments.

37 — See, to that effect, point 2.8. of Opinion 1/2003 of the Data Protection Working Party on the storage of traffic data for billing purposes (WP 69 of 29 January 2003).

71. The exemption under Article 6(3) of Directive of 2002/58 is equally irrelevant. It allows processing by the access provider for the purpose of marketing electronic communications services or for the provision of value added services only after users have given their consent.

72. Finally, Promusicae may not rely on Article 6(5) of Directive 2002/58 either. Under that provision, third parties may process traffic data under the authority of the access provider for specific purposes, in particular that of combating fraud. The 29th recital in the preamble makes it clear in this respect that fraud means unpaid use of the electronic communications service. Promusicae does not act under the authority of Telefónica and the infringement of copyrights cannot be regarded as fraud in that sense.

(b) Article 6(6) of Directive 2002/58

73. In the view of Promusicae, the communication and use of traffic data for the enforcement of copyright claims in the civil courts is however permissible under Article 6(6) of Directive 2002/58. Under that provision, it is possible for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.

74. However, that provision cannot justify the communication of traffic data to Promusicae, simply because Promusicae is not a competent body for the settlement of disputes. Nor is there, in the main proceedings between Promusicae and Telefónica, any apparent necessity for communication of the connection data at issue to the court. Determination of the dispute as to whether Telefónica is entitled and obliged to disclose those data to Promusicae does not require the court to be acquainted with them.

75. The fact that Promusicae demands the traffic data in order to be able to start contentious proceedings against the individual users concerned likewise does not result in communication under Article 6(6) of Directive 2002/58.

76. To interpret Article 6(6) of Directive 2002/58 to the effect that the mere purpose of using traffic data in contentious proceedings allows their communication to the potential opponent would, in the absence of adequate indications in the wording, be incompatible with the foreseeability which must be observed in the statutory justification of interferences with private life and data protection. In addition to the exceptions under Article 6(2), (3) and (5) and under Article 15(1), which are expressly mentioned in Article 6(1) and relatively clearly defined, a new, almost limitless exception would be introduced. [38] According to the wording of Article 6, the user of electronic communications services does not have to reckon with that exception.

77. At the same time, such an exception would be very extensive and could therefore not be accepted as proportionate to the aims pursued. The user would in principle have to reckon continually — not only in the case of copyright infringements — with the fact that his traffic data were being disclosed to third parties who, for some reason, wanted to start contentious proceedings against him. It is inconceivable that such disputes could in any event be based on a pressing social need as referred to in the case-law on Article 8 of the ECHR. [39]

78. A look at the purposes of storage of traffic data under Article 6 of Directive 2002/58 points even more in favour of the restriction of communication. Only the purposes of the storage can justify the communication of the data, as provided for in Article 6(1)(b) of Directive 95/46. Those purposes are, in the case of traffic data under Article 6 of Directive 2002/58, the operation of the communications network, subscriber billing, marketing and value added services with the consent of the user and — over and above those — processing under authority for customer enquiries and fraud detection in the abovementioned [40] sense. Dispute settlement is not an intrinsic purpose of storing traffic data, but only allows the competent authorities to be informed. It can therefore refer only to disputes which are connected with the purposes of the storage. [41] However, the provision of evidence for contentious proceedings with third parties is not an identifiable purpose of storage.

79. Communication of the desired traffic data to Promusicae can therefore not be based on Article 6(6) of Directive 2002/58.

38 — See my Opinion in Case C-350/02 *Commission* v *Netherlands* [2004] ECR I-6213, point 71, on the interpretation of Article 6(4) of Directive 97/66.

39 — See point 54 above.

40 — See point 72 above.

41 — In that respect, my view on 'the diversity of disputes', stated in a different context in the Opinion in *Commission* v *Netherlands*, cited in footnote 38, point 81, should not be over-interpreted.

(c) Article 15(1) of Directive 2002/58

80. Furthermore, Article 15(1) of Directive 2002/58 allows the restriction of the rights under Article 6(1). Such a restriction must be necessary, appropriate and proportionate within a democratic society to safeguard national security (that is, 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.

81. Spain has made use of that derogation and in Article 12(1) of Ley 34/2002 has imposed on access providers the duty to retain traffic and connection data. Communication is however expressly restricted to criminal investigations, safeguarding public security and defence. The stored data must expressly not be communicated for other purposes.

82. It may be doubted whether the storage of traffic data of all users without any concrete suspicions [42] — laying in a stock, as it were — is compatible with fundamental rights, [43] but the Spanish rules are in any case compatible with the wording of Article 15(1) of Directive 2002/58. Such an interference with fundamental rights would be beyond the scope of these proceedings, since they do not concern the validity of Article 15(1). [44] This question may have to be examined one day in connection with Directive 2006/24, which intro-

42 — The German Bundesverfassungsgericht attributes a high intensity of interference to such interferences since the individual gives no cause for the interference but may be intimidated in his lawful conduct because of the risks of abuse and the feeling of being under surveillance; see the order of 4 April 2006 on the pinpointing of criminal suspects by the computerised analysis of data on many people (1 BvR 518/02, *Neue Juristische Wochenschrift 2006*, 1939 [1944], paragraph 117 of the version on www.bundesverfassungsgericht.de).

43 — See the Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM(2005) 438 final), OJ 2005 C 298, p. 1, and the Opinions of the Data Protection Working Party of 21 October 2005, 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM(2005) 438 final of 21 September 2005) and of 25 March 2006, 3/2006 on Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

44 — See Case C-408/95 *Eurotunnel and Others* [1997] ECR I-6315, paragraph 33 et seq.

duces a duty of retention under Community law. [45] However, if the Court wished to examine the permissibility of retention in the present case as a preliminary question, it would certainly be necessary to re-open the oral procedure in order to give the parties entitled under Article 23 of the Statute to make submissions the opportunity to do so.

84. Under Article 15(1) of Directive 2002/58, two types of bases for exceptions are expressly mentioned, namely, on the one hand, in the first four alternatives, national security (that is, State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences and, on the other, in the fifth alternative, unauthorised use of the electronic communication system. In addition, Article 15(1) of Directive 2002/58 refers to Article 13(1) of Directive 95/46, which contains further grounds of exception.

Article 15(1) of Directive 2002/58 in conjunction with Article 13(1)(g) of Directive 95/46

83. In essence, the question which arises here, however, is whether Article 15(1) of Directive 2002/58 permits the communication of the desired — retained — data to Promusicae. If communication were permissible under data protection law, it would need to be examined whether the directives mentioned by the referring court — and the property of the holders of copyrights protected under them — require that that possibility also be used. In that case, the Spanish courts would be obliged to use any available margin of interpretation in order to facilitate such communication. [46]

85. A first basis for communication could result from Article 15(1) of Directive 2002/58 in conjunction with Article 13(1)(g) of Directive 95/46. Article 13(1)(g) of Directive 95/46 allows the communication of personal data for the protection of the rights and freedoms of others. Unlike the grounds of exception in Article 13(1) of Directive 95/46, this ground is admittedly not expressly listed in Article 15(1) of

45 — The action in Case C-301/06 *Ireland* v *Council and Parliament* (Notice in OJ 2006 C 237, p. 5) is currently pending. Ireland claims that Directive 2006/24 should be annulled on the ground that the wrong legal basis was chosen. However, the action does not cover the question whether retention is compatible with fundamental rights.

46 — See *Lindqvist*, cited in footnote 32, paragraph 87.

Directive 2002/58, although Article 15(1) of Directive 2002/58, in the German version, does allow restrictions 'in accordance with Article 13(1) of Directive 95/46'.

86. Viewed in isolation, that could be understood as a reference to *all* the grounds of exception under Article 13(1) of Directive 95/46. [47] However, that is contradicted simply by the fact that Article 15(1) of Directive 2002/58 itself mentions grounds of exception which are intended to allow a restriction 'in accordance with Article 13(1) of Directive 95/46'. Those grounds correspond only in part to the grounds in Article 13(1) of Directive 95/46 and do not include the exception for the rights of others, mentioned under (g). Consequently, the grounds mentioned in Article 13(1) of Directive 95/46 are applicable in the electronic communications sector only in so far as they are expressly included in Article 15(1) of Directive 2002/58.

87. That rule is more clearly apparent from other language versions than from the German version. Instead of the ambiguous 'gemäß' ('in accordance with'), the reference is made in the form 'as referred to in Article 13(1) of Directive 95/46'. [48] That is based on a deliberate decision during the legislative procedure. As the Commission points out, when it first adopted that rule in Directive 97/66, the Council refrained from incorporating the grounds of exception in Article 13(1) of Directive 95/46 in their entirety and instead chose the present, differentiated rule. [49]

88. That conclusion is also supported by the speciality of Article 15(1) of Directive 2002/58 as compared with Article 13(1) of Directive 95/46. [50] The latter applies to all personal data irrespective of the context in which they arise. It is thus relatively general since it has to be applied to a large number of very different situations. [51] The former, on the other hand, relates specifically to the personal data which arise in the context of

47 — Thus, for example, Christian Cychowski in 'Auskunftsansprüche gegenüber Internetzugangsprovidern "vor" dem 2. Korb und "nach" der Enforcement-Richtlinie der EU', *Multimedia und Recht 2004*, p. 514 (p. 517 et seq.), takes the view that the German transposition of this exception allows the communication of the traffic data of copyright infringers to the rightholders.

48 — Thus the French version has 'comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE', the English version 'as referred to in Article 13(1) of Directive 95/46/EC' and the Spanish version 'a que se hace referencia en el apartado 1 del artículo 13 de la Directiva 95/46/CE', in each case following a list of the various permissible grounds of justification.

49 — See footnote 6 to the Commission's written observations.

50 — Ulrich Sieber/Frank Michael Höfiger, 'Drittauskunftsansprüche nach § 101a UrhG gegen Internetprovider zur Verfolgung von Urheberrechtsverletzungen', *Multimedia und Recht* 2004, 575 (582), and Gerald Spindler/Joachim Dorschel, 'Auskunftsansprüche gegen Internet-Service-Provider', *Computer und Recht* 2005, 38 (45 et seq.).

51 — See to that effect *Lindqvist*, cited in footnote 32, paragraph 83.

electronic communications and is therefore based on a comparatively precise assessment of the extent to which communication of personal traffic data interferes with the fundamental right to data protection.

89. Consequently, the protection of the rights and freedoms of others under Article 13(1)(g) of Directive 95/46 cannot justify the communication of personal traffic data.

Unauthorised use of the electronic communication system

90. A further possible basis for communication could be unauthorised use of the electronic communication system, which is the fifth alternative in Article 15(1) of Directive 2002/58.

91. The concept of unauthorised use of the electronic communication system essentially allows two interpretations with regard to the conduct in question, namely use for unauthorised purposes and use contrary to the system. Infringement of copyright would certainly be an unauthorised purpose. When such an infringement is committed, the communication system may nevertheless be used as intended, namely for loading data from other computers which are connected to the Internet. The communication system does not need to be manipulated — in ways contrary to the system — by, for example, obtaining passwords for other persons' computers or simulating a false identity to the external computer. [52]

92. In the Commission's view, the meaning intended in Article 15(1) of Directive 2002/58 is use contrary to the system, jeopardising the integrity or security of the communication system. That, it says, also follows from the drafting history, since the concept was introduced in Directive 97/66 for ensuring correct frequency use.

93. That narrow interpretation of the concept of unauthorised use accords with the secrecy of communications, protected under Article 5 of Directive 2002/58. Use

52 — Use contrary to the system would normally also cover acts punishable under Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems (OJ 2005 L 69, p. 67).

for unauthorised purposes can normally be established only by monitoring the content of the communication.

94. While Article 15(1) does also justify exceptions to the confidentiality of communications, the other grounds of exception expressly mentioned would, on a wide interpretation of the concept of unauthorised use, be superfluous and largely deprived of their practical effectiveness, since acts endangering national security, public security or defence and criminal offences committed by the use of electronic communications systems are normally accompanied by an unauthorised purpose.

95. At the same time, a broadly worded exception for communications for unauthorised purposes would hardly be foreseeable in its application and would largely render meaningless the right to protection of personal traffic data.

96. The range of unauthorised communication operations under criminal law is already relatively wide. Moreover, communication may also come into conflict with duties not subject to criminal sanctions, arising from specific legal relationships, such as, for example, with employment relationships or duties towards the family. There would even be the possibility that the provider of the electronic communication service could object to access to certain content or its dissemination. It would therefore be virtually impossible to define which of those legal relationships could allow storage and communication of traffic data or perhaps even of communication content. As a result, this ground of restriction would not, on a wide interpretation, be reconcilable with the requirement of foreseeability.

97. In addition, a wide interpretation would render largely meaningless not only the protection of personal traffic data, but also the protection of confidentiality of communications. In order to be able effectively to verify whether electronic communication systems were being used for unauthorised purposes, it would be necessary to store the entire communication and process it intensively with regard to the content. The citizen 'under the eye of Big Brother' would thus be a reality.

98. The Commission's interpretation must therefore be favoured. Consequently, unauthorised use of the electronic communication

system covers only use contrary to the system, but not use for unauthorised purposes.

The grounds of exception in the first four alternatives in Article 15(1) of Directive 2002/58

99. Consequently, only the first four alternatives in Article 15(1) of Directive 2002/58, in particular the prevention, investigation, detection and prosecution of criminal offences, and public security now remain as a basis for communication of the connection data.

100. Recital 11 in the preamble to Directive 2002/58 explains the first four alternatives in Article 15(1). According to that recital, the Directive does not apply to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1), necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law.

101. As the Court has already held, those are activities of the State or of State authorities. [53] It is true that State authorities may oblige private individuals to assist them, [54] but autonomous action by private individuals against infringements of rights no longer falls under those exceptions. For that reason alone, the first four alternatives of Article 15(1) of Directive 2002/58 can permit only communication to State authorities, but not the direct communication of traffic data to Promusicae. [55]

102. Whether communication to State authorities would be possible in the present case under the fourth alternative in Article 15(1) of Directive 2002/58, that is to

53 — *Lindqvist*, cited in footnote 32, paragraph 43.

54 — Joined Cases C-317/04 and C-318/04 *Parliament* v *Council and Commission* [2006] ECR I-4721, paragraph 58.

55 — According to Promusicae, the conclusion thus reached on the third and fourth alternatives in Article 15(1) of Directive 2002/58 corresponds to the legal position in France, Italy and Belgium, where, it claims, the legislation provides that the competent State authorities may require the surrender of personal traffic data. The Data Protection Working Party, in Working Document WP 104 (cited in footnote 36, p. 8), even goes a step further and restricts communication to the prosecuting authorities: 'On the basis of the compatibility principle as well as in compliance with the confidentiality principle included in Directives 2002/58 and 95/46, data detained by ISPs processed for specific purposes including mainly the performance of a telecommunication service cannot be transferred to third parties such as right holders, except, in defined circumstances provided by law, to public law enforcement authorities.'

say, for the prevention, investigation, detection and prosecution of criminal offences, is also doubtful. As the Commission rightly submits, that presupposes that the copyright infringements alleged by Promusicae must also be regarded as criminal offences.

103. Under Community law, criminal liability is not excluded since — as is also apparent in Article 8(1) of Directive 2001/29 and Article 16 of Directive 2004/48 — the national legislature must decide whether and in what form infringements of copyright are penalised. The legislature can therefore make infringement of copyright by file sharing a criminal offence. According to the referring court, however, criminal liability for such acts in Spain presupposes the intention to make a profit. [56] No indications of that have been put forward up to now.

104. In addition, among the exceptions in Article 15(1) of Directive 2002/58, the third alternative, namely public security, is a further possible legal basis. According to the case-law in the sphere of the fundamental freedoms, public policy and security may only be invoked if a genuine and sufficiently serious threat exists, affecting one of the fundamental interests of society. [57]

105. The protection of copyright is an interest of society, the importance of which has been repeatedly emphasised by the Community. Consequently, even though the interest of rightholders is primarily not of a public, but of a private nature, this aim can be recognised as a fundamental interest of society. Illegal file sharing also genuinely threatens the protection of copyright.

106. It is however not certain that private file sharing, in particular when it takes place without any intention to make a profit, threatens the protection of copyright sufficiently seriously to justify recourse to this

56 — See point 28 above.

57 — See, for example, Joined Cases C-482/01 and C-493/01 *Orfanopoulos and Oliveri* [2004] ECR I-5257, paragraph 66, on freedom of movement and Case C-54/99 *Église de scientologie* [2000] ECR I-1335, paragraph 17, on the free movement of capital.

exception. To what extent private file sharing causes genuine damage is in fact disputed. [58]

107. That assessment should — subject to review by the Court — be left to the legislature. In particular when Member States make the infringement of copyright by file sharing a criminal offence, they undertake a corresponding assessment, but in that case the fourth alternative in Article 15(1) of Directive 2002/58 already applies, so that there is no need for recourse to public security.

108. Criminal liability would admittedly be weighty evidence of a sufficiently serious threat to the protection of copyright, but criminal law is not necessarily the only form in which the legislature can give expression to an appropriate condemnation. Rather, the legislature can also enforce that assessment by first providing only for communication of personal traffic data in order to enable civil proceedings to be brought. However, the condition for such legislation remains that data protection should not be restricted on account of the possible infringement of copyrights in trivial cases.

109. Such provisions must, under the principle of foreseeability and purpose limitation in data protection law, state sufficiently clearly that the storage and communication of personal data by the providers of Internet access will also take place for the protection of copyright. Since such provisions are based on the third alternative in Article 15(1) of Directive 2002/58, account would also have be taken of the fact that the protection of public security is a task of State authorities and therefore traffic data may not be surrendered to private rightholders without the involvement of such authorities (for example, the courts or the data protection supervisory authorities).

110. The *Community legislature* has in any case not as yet taken any such decision on breaching data protection for the purpose of acting against copyright infringements. In particular, the directives mentioned by the referring court are not relevant since they, as already stated, [59] do not affect data

58 — See the report DSTI/ICCP/IE(2004)12/FINAL of 13 December 2005 (http://www.oecd.org/dataoecd/13/2/34995041.pdf, S. 76 ff.) to the Working Party on the Information Economy of the Organisation for Economic Cooperation and Development (OECD).

59 — See point 42 et seq. above.

protection. That applies in particular to the right of information under Article 8 of Directive 2004/48, the wording of which could also be construed as covering disclosure of the identity of Internet users. According to paragraph 3(e), that provision is to apply without prejudice to other statutory provisions which govern the processing of personal data.

111. It would therefore not be foreseeable to infer from those directives a purpose of traffic data storage which is not expressly laid down in them, as is necessary under the requirement of foreseeability and Article 6(1)(b) of Directive 95/46.[60] Nor is there any reference in them to involvement of State authorities in the communication of personal traffic data to private rightholders.

112. However, as Community law stands at present, under the third and fourth alternatives in Article 15(1) of Directive 2002/58, *Member States* may provide for personal traffic data to be communicated to State authorities in order to facilitate both criminal and civil proceedings against copyright infringements by file sharing. However, they are not obliged to do so.

113. Compared with the direct communication of personal traffic data to the holders of infringed rights, that is a more lenient method in the present situation, and at the same time ensures that communication remains appropriate in relation to the protected legal positions.

114. Involving State authorities is more lenient because, unlike private individuals, they are directly bound by fundamental rights. In particular, they must respect procedural safeguards. Moreover, they invariably also take into consideration circumstances which exonerate the user accused of an infringement of copyright.

115. Accordingly, it does not follow conclusively from the fact that copyrights

60 — See point 53 above.

were infringed under an IP address at a particular time that those acts were also carried out by the subscriber to whom that address was assigned at that time. Rather, it is also possible that other people used his connection or computer. This may even have occurred without his knowledge if, for example, he operates an inadequately protected local wireless network in order to avoid cable connections, [61] or if his computer was 'taken over' by third parties via the Internet.

116. The holders of copyrights will — unlike State authorities — have no interest in allowing for or clarifying such circumstances.

117. The appropriateness of communication of personal traffic data will also be more effectively ensured if State authorities are involved.

118. The legislature will provide for their intervention only where there is adequate suspicion of an infringement of rights. A wide discretion exists in that regard. It is true that the sanctions under Article 8(1) of Directive 2001/29 and Article 16 of Directive 2004/48 must be appropriate, effective, proportionate and dissuasive, but the seriousness of the particular infringement of copyrights must also be taken into account in that regard.

119. Consequently, the possibility of communication of personal traffic data may be restricted to particularly serious cases such as, for example, offences committed with a view to making a profit, that is, an illegal use of protected works which substantially impairs their economic exploitation by the holder of the right. The intention that the enforcement of copyrights in the face of infringements on the Internet should be geared specifically to serious impairments is also apparent from the ninth recital in the preamble to Directive 2004/48. The United Kingdom rightly points out that the recital refers to the distribution of pirated copies

61 — See the Working Paper of the International Working Group on Data Protection in Telecommunications of 15 April 2004 on potential privacy risks associated with wireless networks, available in English and German at http://www.datenschutz-berlin.de/doc/int/iwgdpt/index.htm. According to Stefan Dörhöfer, *Empirische Untersuchungen zur WLAN-Sicherheit mittels Wardriving*, https://pi1-old.informatik.uni-mannheim.de:8443/pub/research/theses/diplomarbeit-2006-doerhoefer.pdf, p. 98, on the survey date in Germany, approximately 23% of all wireless networks were not protected at all and approximately 60% were inadequately protected. With regard to the methods of attack, see Erik Tews, Ralf-Philipp Weinmann and Andrei Pyshkin, *Breaking 104 bit WEP in less than 60 seconds*, http://eprint.iacr.org/2007/120.pdf.

on the Internet, but such distribution is mentioned in connection with organised crime.

120. The fundamental rights to property and to effective judicial protection do not call that assessment of appropriateness into question. It is certainly necessary, in terms of fundamental rights, to establish the possibility for the holders of copyrights to defend themselves against infringements of those rights. The present case, however, unlike the case of *Moldovan and Others* v *Romania* [62] cited by Promusicae, is not concerned with whether access to the courts is actually available, but with the means made available to rightholders in order to establish the infringement.

121. In that respect, the State's duties of protection are not so far-reaching that unlimited means should be made available to the rightholder for the purpose of detecting infringements of rights. Rather, it is not objectionable for certain rights of detection to remain reserved for State authorities or not to be available at all.

62 — Eur Court HR judgment of 12 July 2005 (Applications Nos. 41138/98 and 64320/01, § 118 et seq.).

5. Directive 2006/24

122. Directive 2006/24 does not lead to a different conclusion so far as the present case is concerned. Although, under that directive, Article 15(1) of Directive 2002/58 does not apply to data retained in accordance with Directive 2006/24, the data at issue here were not stored pursuant to the new directive. As Promusicae also submits, the Directive is therefore, *ratione temporis*, not applicable.

123. Even if Directive 2006/24 were applicable, it would not allow direct communication of personal traffic data to Promusicae. Under Article 1, retention is solely for the purpose of the investigation, detection and prosecution of serious crime. Accordingly, pursuant to Article 4, those data may be provided only to the competent authorities.

124. If anything at all can be inferred from Directive 2006/24 with respect to the present case, it is the value judgment of the Community legislature that up to now only serious crime has necessitated Community-wide retention of traffic data and their use.

6. Conclusion with regard to data protection

125. Consequently, in the light of Directive 2002/58, it is compatible with Community law, in particular Directive 2000/31, Directive 2001/29 and Directive 2004/48, for Member States to exclude the communication of personal traffic data for the purpose of bringing civil proceedings against copyright infringements.

126. Should the Community consider that more far-reaching protection of the holders of copyrights is necessary, that would require an amendment of the provisions on data protection. Up to now, however, the legislature has not yet taken that step. On the contrary, in adopting Directives 2000/31, 2001/29 and 2004/48, it provided for the unaltered continued applicability of data protection and saw no reason, when adopting the sector-specific Directives 2002/58 and 2006/24, to introduce restrictions of data protection in favour of the protection of intellectual property.

127. Directive 2006/24 could, on the contrary, lead to a strengthening of data protection under Community law with regard to disputes concerning infringements of copyright. The question then arises, even in criminal investigations, as to the extent to which it is compatible with the fundamental right to data protection under Community law to grant aggrieved rightholders access to the results of the investigation if the latter are based on the evaluation of retained traffic data within the meaning of Directive 2006/24. Up to now that question is not affected by Community law since the Data Protection Directives do not apply to the prosecution of criminal offences. [63]

63 — See *Parliament* v *Council and Commission*, cited in footnote 54, paragraph 58.

V — Conclusion

128. I therefore propose that the Court should reply to the request for a preliminary ruling as follows:

'It is compatible with Community law for Member States to exclude the communication of personal traffic data for the purpose of bringing civil proceedings against copyright infringements.'