Reports of Cases

OPINION OF ADVOCATE GENERAL
CAMPOS SÁNCHEZ-BORDONA
delivered on 12 May 2016[1]

Case C-582/14

Patrick Breyer
v
Bundesrepublik Deutschland(Request for a preliminary ruling from the

Bundesgerichtshof (Federal Court of Justice, Germany))

(Processing of personal data — Directive 95/46/EC — Article 2(a) and Article 7(f) — Concept of 'personal data' — IP addresses — Retention by a provider of electronic media services — National legislation which does not allow account to be taken of the legitimate interests pursued by the controller)

1. An Internet Protocol address ('IP address') is a sequence of binary numbers which, when allocated to a device (a computer, a tablet or a smartphone), identifies it and allows it to access that electronic communications network. The device, in order to connect to the Internet, must use the number sequence provided by Internet service providers. The IP address is transmitted to the server on which the accessed web page is stored.

2. In particular, Internet service providers (generally, telephone companies) assign to their clients 'dynamic IP addresses' on a temporary basis, for each Internet connection, and change them when subsequent connections are made. Those same companies keep a record of which IP address has been assigned, at any one time, to a particular device.[2]

3. The owners of web sites that are accessed using dynamic IP addresses also tend to keep records of which pages are accessed, when and from which dynamic IP address. It is technically possible to retain those records indefinitely after each user terminates his Internet connection.

4. A dynamic IP address is not in itself sufficient to allow a service provider to identify a user of its web page. However, it can do so if it combines the dynamic IP address with other additional data held by the Internet service provider.

1 — Original language: Spanish.

2 — Article 5 of 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 (OJ 2006 L 105, p. 54) imposed the obligation, inter alia, to retain, for the purpose of the investigation, detection and prosecution of serious crime, 'the date and time of the log-in and log-off of the Internet access service, … together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user'.

5. The dispute is concerned with whether dynamic IP addresses are personal data, within the meaning of Article 2(a) of Directive 95/46/EC.[3] In order to answer that question, it is first necessary to determine the relevance, to that end, of the fact that the additional data necessary to identify the user are in the possession not of the owner of the web site, but of a third party (specifically, the Internet service provider).

6. It is a novel question for the Court, since, in paragraph 51 of the judgment in *Scarlet Extended*,[4] the Court stated that IP addresses 'are protected personal data because they allow those users to be precisely identified', but did so in a context in which the collection and identification of IP addresses was carried out by the Internet service provider,[5] not by a content provider, as is the case here.

7. If dynamic IP addresses are, for a provider of services on the Internet, personal data, it is then necessary to examine whether their processing falls within the scope of Directive 95/46.

8. It is possible that, even though they are personal data, they do not benefit from the protection resulting from Directive 95/46 if, for example, they are processed for the purpose of criminal proceedings against any persons attacking the website. In that situation, Directive 95/46 is not applicable, pursuant to the first indent of Article 3(2) thereof.

9. It is also necessary to ascertain whether a service provider that records dynamic IP addresses when users access its web pages (in this case, the Federal Republic of Germany) is acting as a public authority or as a private individual.

10. If Directive 95/46 is applicable, it will be necessary to clarify, lastly, the extent to which Article 7(f) is compatible with national legislation which restricts the scope of one of the conditions set out in that article to justify the processing of personal data.

I – Legislative framework

A – *EU law*

11. Recital 26 of Directive 95/46 reads as follows:

'(26) Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible.'

12. Under Article 1 of Directive 95/46:

'1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

3 — Directive of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).

4 — C-70/10, EU:C:2011:771, paragraph 51.

5 — That was also the situation in *Bonnier Audio and Others* (C-461/10, EU:C:2012:219, paragraphs 51 and 52).

2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.'

13. According to Article 2 of Directive 95/46:

'For the purposes of this Directive:

(a) "personal data" shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) "processing of personal data" ("processing") shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

…

(d) "controller" shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

…

(f) "third party" shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data;

…'

14. Under the heading 'Scope', Article 3 of Directive 95/46 provides:

'1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Directive shall not apply to the processing of personal data:

— in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law;

…'

15. Chapter II of Directive 95/46, concerning 'General rules on the lawfulness of the processing of personal data', opens with Article 5, in accordance with which 'Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful'.

16. Under Article 6 of Directive 95/46:

‘1. Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

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

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.’

17. According to Article 7 of Directive 95/46:

‘Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1).’

18. In accordance with Article 13 of Directive 95/46:

‘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.

…'

B – *National law*

19. Paragraph 12 of the Telemediengesetz (Telemedia Law; 'the TMG')[6] provides:

'(1) A service provider may collect and use personal data to make telemedia available only in so far as this law or another legislative provision expressly relating to telemedia so permits or the user has consented to it.

(2) Where personal data have been supplied in order for telemedia to be made available, a service provider may use them for other purposes only in so far as this law or another legislative provision expressly relating to telemedia so permits or the user has consented to it.

(3) Except as otherwise provided for, the relevant provisions concerning the protection of personal data shall apply even if the data are not processed automatically.'

20. In accordance with paragraph 15 of the TMG:

'(1) A service provider may collect and use the personal data of a user only to the extent necessary in order to facilitate, and charge for, the use of telemedia (data concerning use). Data concerning use include, in particular:

1. particulars for the identification of the user,

2. information concerning the beginning, end and extent of the particular use, and

3. information concerning the telemedia used by the user.

(2) A service provider may combine the data concerning use of a user relating to the use of different telemedia to the extent that this is necessary for the purposes of charging the user.

…

6 — Law of 26 February 2007 (BGBl 2007 I, p. 179).

(4) A service provider may use data concerning use after the end of the use to the extent that they are required for the purposes of charging the user (invoicing data). The service provider may block the data in order to comply with existing limits on storage periods laid down by law, statutes or contract. …'

21. In accordance with paragraph 3(1) of the Bundesdatenschutzgesetz (Federal Data Protection Law; 'the BDSG'),[7] 'Personal data are individual indications concerning the personal or factual circumstances of an identified or identifiable natural person (data subject) …'.

II – Facts

22. Mr Breyer brought an action seeking a prohibitory injunction against the Federal Republic of Germany for storing IP addresses.

23. Many German public institutions operate publicly accessible websites on which they supply topical information. With the aim of preventing attacks and making it possible to prosecute attackers, most of those websites store information on all access operations in logfiles. Even after access has been terminated, information is retained in the logfiles concerning the name of the file or web page to which access was sought, the terms entered in the search fields, the time of access, the quantity of data transferred, an indication of whether access was successful and the IP address of the computer from which access was sought.

24. Mr Breyer, who consulted several such web pages, sought an injunction requiring the Federal Republic to refrain from storing, or arranging for third parties to store, the IP address of the host system from which he sought access, except in so far as the storage is required in order to restore the availability of the telemedium in the event of a fault occurring.

25. Mr Breyer's application was dismissed at first instance. His appeal was upheld in part, however, and the Federal Republic ordered to refrain from storing IP addresses after the end of each period of access. The prohibition order was made conditional on the applicant revealing, during the access operation, his personal data, including in the form of an email address, and except in so far as the storage is required in order to restore the availability of the telemedium.

III – Question referred

26. Both parties having appealed on points of law, on 17 December 2014 the Sixth Chamber of the Bundesgerichtshof (Federal Court of Justice, Germany) referred the following questions for a preliminary ruling:

'(1) Must Article 2(a) of Directive 95/46/EC … be interpreted as meaning that an Internet Protocol address (IP address) which a service provider stores when his website is accessed already constitutes personal data for the service provider if a third party (an access provider) has the additional knowledge required in order to identify the data subject?

(2) Does Article 7(f) of the Data Protection Directive preclude a provision in national law under which a service provider may collect and use a user's personal data without his consent only to the extent necessary in order to facilitate, and charge for, the specific use of the telemedium by the user concerned, and under which the purpose of ensuring the general operability of the telemedium cannot justify use of the data beyond the end of the particular use of the telemedium?'

7 — Law of 20 December 1990 (BGBl 1990 I, p. 2954).

27. As the referring court explains, according to German law the applicant was entitled to demand that the storage of IP addresses cease, if their storage constitutes under data protection law an unlawful interference with his general personality right, more particularly his right of 'informational self-determination' [paragraph 1004(1) and paragraph 823(1) of the Bürgerliches Gesetzbuch (German Civil Code), in conjunction with Articles 1 and 2 of the Grundgesetz (Basic law)].

28. That would be the case if: (a) the IP address (in any event together with the time when a website was accessed) constituted 'personal data' within the meaning of Article 2(a) read in conjunction with the second sentence of recital 26 of Directive 95/46, or within the meaning of paragraph 12(1) and (3) of the TMG in conjunction with paragraph 3(1) of the BDSG; and (b) there were no grounds for authorisation for the purposes of Article 7(f) of Directive 95/46 and paragraph 12(1) and (3) and 15(1) and (4) of the TMG.

29. According to the Bundesgerichtshof (Federal Court of Justice), it is essential, in order to interpret the national law (paragraph 12(1) of the TMG), to determine how the personal nature of the data referred to in Article 2(a) of Directive 95/46 must be understood.

30. The referring court also points out that since, according to paragraph 15(1) of the TMG, a service provider may collect and use the personal data of a user only to the extent necessary in order to facilitate, and charge for, the use of telemedia (data concerning use),[8] the interpretation of that national provision is linked to any interpretation of Article 7(f) of Directive 95/46.

IV – The procedure before the Court and arguments of the parties

31. Written submissions were presented by the German, Austrian, and Portuguese Governments and by the Commission. Only the Commission and Mr Breyer attended the public hearing held on 25 February 2016, at which the German Government declined to participate.

A – *Arguments of the parties in relation to the first question*

32. According to Mr Breyer, personal data include those which it is possible to combine only from a theoretical point of view, that is to say, where there exists an abstract potential risk of combination, it being of little importance whether that combination occurs in practice. In his view, the fact that a body may be subjectively incapable of identifying a person using the IP address does not mean that there is no risk for that person. Moreover, in his view, it is relevant that Germany retains his IP data for the purposes of, where appropriate, identifying possible attacks or bringing criminal proceedings, as permitted by paragraph 113 of the Telekommunikationsgesetz (Law on telecommunications) and as has occurred on numerous occasions.

33. The German Government takes the view that the first question should be answered in the negative. In its view, dynamic IP addresses do not reveal an 'identified' person, within the meaning of Article 2(a) of Directive 95/46. In order to determine whether dynamic IP addresses relate to an 'identifiable' person, within the meaning of that provision, examination of *identifiability* should be carried out using a 'subjective' criterion. This follows, in its view, from recital 26 of Directive 95/46, according to which it is necessary to take into account only the means likely 'reasonably' to be used by the controller, or by a third party, to identify a person. It claims that that point indicates that the EU legislature did not want to include within the scope of Directive 95/46 those situations where identification is objectively possible by any third party.

8 — According to the Bundesgerichtshof (Federal Court of Justice), data concerning use are those identifying the user, those concerning the beginning, end and extent of the particular use and those relating to the telemedia which the user has used.

34. The German Government also understands that the concept of 'personal data', within the meaning of Article 2(a) of Directive 95/46, must be interpreted in the light of the purpose of that directive, namely, to ensure respect for fundamental rights. The need to protect natural persons might be seen differently depending on who possesses the data and whether or not the latter has the means to use those data for the purpose of identifying those natural persons.

35. The German Government maintains that Mr Breyer is not identifiable from the IP addresses combined with the other data which content providers retain. To identify him it would be necessary to handle information held by Internet access service providers, which, without a legal basis, cannot provide it to content providers.

36. The Austrian Government, however, considers that the answer should be in the affirmative. According to recital 26 of Directive 95/46, in order for a person to be considered identifiable it is not necessary for all his identification data to be held by a single entity. Accordingly, an IP address could be personal data if a third party (such as, for example, the Internet access service provider) has the means to identify the holder of the IP address without making a disproportionate effort.

37. The Portuguese Government also supports an affirmative response, considering that an IP address, together with the date of the access operation, constitutes personal data, insofar as it may lead to a user being identified by an entity other than that which retained the IP address.

38. The Commission also proposes an affirmative answer, relying on the solution adopted by the Court in the judgment in *Scarlet Extended*.[9] According to the Commission, since storing IP addresses serves specifically to identify users in the event of cyber attacks, the use of supplementary data which Internet access service providers record is a means which might 'reasonably' be used, within the meaning of recital 26 of Directive 95/46. In short, in the Commission's view, both the objective pursued by that directive and Articles 7 and 8 of the Charter of fundamental rights of the European Union ('the Charter') support a broad interpretation of Article 2(a) of Directive 95/46.

B – *Arguments of the parties in relation to the second question*

39. Mr Breyer understands that Article 7(f) of Directive 95/46 is a general clause whose implementation requires specific expression. According to the case-law of the Court, it would be necessary, therefore, to assess the circumstances of the particular case and to determine whether there are groups having a legitimate interest, within the meaning of that provision, where the provision of specific rules for such groups is not only permitted, but essential for the purposes of applying that article. In that situation, and according to Mr Breyer, the national legislation is compatible with Article 7(f) of Directive 95/46 insofar as the public website has no interest in retaining the personal data or because the interest in protecting anonymity carries greater weight. In his view, however, the systematic retention of personal data is neither consistent with a democratic society nor necessary or proportionate to ensure the functioning of electronic media, which is perfectly possible without the storage of those personal data, as the websites of some federal ministries demonstrate.

40. The German Government argues that it is not necessary to address the second question, raised only in the event that the first question should be answered in the affirmative, which is not the case in its view, for the above reasons.

41. The Austrian Government proposes that the response should be that Directive 95/46 does not preclude in general the retention of data such as those at issue in the main proceedings, when it is essential to ensure the proper functioning of electronic media. According to that Government, a limited retention of IP addresses, after the period of accessing a web page, may be lawful, insofar as it

9 — C-70/10, EU:C:2011:771, paragraph 51.

concerns the obligation of the controller of the personal data to apply the measures protecting those data imposed by Article 17(1) of Directive 95/46. In order to combat cyber attacks it may be legitimate to analyse data relating to previous attacks and to deny certain IP addresses access to a website. The proportionality of retaining data such as those at issue in the main proceedings, from the point of view of the objective of ensuring the proper functioning of electronic media, should be assessed on a case-by-case basis, taking into account the principles set out in Article 6(1) of Directive 95/46.

42. The Portuguese Government argues that Article 7(f) of Directive 95/46 does not preclude the national rules at issue in the main proceedings, because the German legislature has already carried out the balancing exercise, laid down in that provision, between the legitimate interests of the controller of the personal data, on the one hand, and the rights and freedoms of data subjects, on the other.

43. In the Commission's view, national legislation which incorporates Article 7(f) of Directive 95/46 must define the objectives of processing personal data in such a way that they are predictable for the individual concerned. In its view, the German legislation does not comply with that requirement, since it establishes, in paragraph 15(1) of the TMG, that the retention of IP addresses is authorised 'to the extent necessary in order to facilitate … the use of telemedia'.

44. The Commission proposes, therefore, that the answer to the second question referred should be that that provision precludes a provision in national law under which a public authority acting as a service provider may collect and use a user's personal data without his consent, even if the objective pursued is to ensure the proper functioning of the electronic medium, where the provision in national law concerned does not establish that objective in a sufficiently clear and precise manner.

V – Assessment

A – *First question*

1. Determining the scope of the question referred

45. According to the terms used by the Bundesgerichtshof (Federal Court of Justice), the first of its questions seeks to ascertain whether an IP address which is used to access a web page constitutes personal data (within the meaning of Article 2(a) of Directive 95/46/EC) for the public authority owner of that page, where the Internet service provider has the additional knowledge required in order to identify the data subject.

46. Thus worded, the question is sufficiently precise to rule out, at the outset, other questions which might be raised *in abstracto* concerning the legal nature of IP addresses in the context of the protection of personal data.

47. In the first place, the Bundesgerichtshof (Federal Court of Justice) refers exclusively to 'dynamic IP addresses', that is those which are allocated on a temporary basis for each connection to the network and are changed when subsequent connections are made. This therefore leaves aside 'fixed or static IP addresses', which are invariable and allow continuous identification of the device connected to the network.

48. In the second place, the referring court presumes that the provider of the web page in the main proceedings is unable to identify, by means of the dynamic IP address, the individuals who visit its pages and does not itself have additional data which, combined with that IP address, facilitate their identification. The Bundesgerichtshof (Federal Court of Justice) seems to consider that, in that context, the dynamic IP address is not personal data, within the meaning of Article 2(a) of Directive 95/46, *for the provider of the web page*.

49. The uncertainty of the referring court concerns whether, as regards the provider of the web page, the dynamic IP address should be classified as personal data *if a third party has additional data* which, combined with the IP address, identify persons who access its pages. However, and this is a further relevant detail, the Bundesgerichtshof (Federal Court of Justice) refers not to any third party which is in possession of additional data, but only to the Internet service provider (excluding, therefore, other possible holders of such data).

50. The following matters, inter alia, are therefore not in dispute: (a) whether static IP addresses are personal data under Directive 95/46;[10] (b) whether dynamic IP addresses are, always and in all circumstances, personal data within the meaning of that directive and, lastly; (c) whether the classification of dynamic IP addresses as personal data is necessary as soon as there is a third party, irrespective of who it may be, capable of using those dynamic IP addresses to identify network users.

51. The issue, then, is solely of determining whether a dynamic IP address is personal data for the provider of a service on the Internet where the communications company which offers network access (the Internet access provider) handles additional data which, when combined with that address, identify who accessed the web page operated by the former.

2. Substance

52. The question raised in this reference for a preliminary ruling is a subject matter of intense debate in German academic writings and case-law, which has polarised into two currents of opinion.[11] According to the first (which opts for an 'objective' or 'absolute' criterion) a user is identifiable — and, therefore, the IP address is personal data capable of protection — when, regardless of the abilities and means of the provider of a service on the Internet, it is feasible to identify him, solely by combining that dynamic IP address with data provided by a third party (for example, the Internet service provider).

53. For the supporters of the other current of opinion (who favour a 'subjective' criterion), the possibility that a user may ultimately be identified with the assistance of a third party is insufficient for a dynamic IP address to be classified as personal data. What is relevant is the capacity of a person who has access to data to use his own resources to identify an individual from those data.

10 — An issue addressed by the Court in the judgments in *Scarlet Extended* (C-70/10, EU:C:2011:771, paragraph 51), and *Bonnier Audio and Others* (C-461/10, EU:C:2012:219). In paragraphs 51 and 52 of the latter judgment, the Court held that communication 'of the name and address of an Internet … user using the IP address from which it is presumed that an unlawful exchange of files containing protected works took place, in order to identify that person ... constitutes the processing of personal data within the meaning of the first paragraph of Article 2 of Directive 2002/58, read in conjunction with Article 2(b) of Directive 95/46'.

11 — Concerning the two positions adopted in academic writings, see, for example, Schreibauer, M., in *Kommentar zum Bundesdatenschutzgesetz. Nebengesetze*, Esser, M., Kramer, P., and von Lewinski, K. (eds.), Carl Heymanns Verlag/Wolters Kluwer, Colonia, 2014, 4th edition, § 11 Telemediengesetz (4 to 10). Nink, J., and Pohle, J.: 'Die Bestimmbarkeit des Personenbezugs. Von der IP-Adresse zum Anwendungsbereich der Datenschutzgesetze', in *Multimedia und Recht*, 9/2015, pp. 563 to 567. Heidrich, J., and Wegener, C.: 'Rechtliche und technische Anforderungen an die Protokollierung von IT-Daten. Problemfall Logging', in *Multimedia und Recht*, 8/2015, pp. 487 to 492. Leisterer, H.: 'Die neuen Pflichten zur Netz– und Informationssicherheit und die Verarbeitung personenbezogener Daten zur Gefahrenabwehr', in *Computer und Recht*, 10/2015, pp. 665 to 670.

54. Whatever the terms of that dispute in national law, the answer of the Court must be limited to interpreting the two provisions of Directive 95/46, to which both the referring court and the parties to the dispute in the main proceedings have referred, that is Article 2(a) [12] and recital 26 thereof. [13]

55. Dynamic IP addresses, merely by providing information on the date and time of accessing a web page from a computer (or other device), show some patterns of Internet users' behaviour and therefore involve a potential interference with the right to respect for private life, [14] guaranteed by Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms and by the Article 7 of the Charter, in whose light, as well as that of Article 8 thereof, Directive 95/46 must be interpreted. [15] In fact, the parties to the dispute do not call into question that premiss, which is not the subject matter, as such, of the question referred.

56. The person to which those particulars relate is not an 'identified natural person'. The date and time of a connection and the numerical address from which it originated do not reveal, directly or immediately, the identity of the natural person who owns the device used to access the website or the identity of the user operating the device (who could be any natural person).

57. However, in so far as a dynamic IP address helps to determine — either alone or in conjunction with other data — who is the owner of the device used to access the website, it may be classified as information relating to an 'identifiable person'. [16]

58. According to the approach adopted by the Bundesgerichtshof (Federal Court of Justice), a dynamic IP address is not sufficient, in itself, to identify the user who has accessed a web page through it. If the provider of a service on the Internet could, on the contrary, identify the user through the dynamic IP address, it would, no doubt, be personal data within the meaning of Directive 95/46. However, this does not appear to be the issue underlying the question referred, in which the providers of Internet services involved in the dispute in the main proceedings cannot identify the user exclusively from the dynamic IP address.

59. The fact that a dynamic IP address, when combined with other data, facilitates the 'indirect' identification of a user is a matter which is not in dispute. Does the possibility that there may be such additional data, capable of being linked to the dynamic IP address, in itself make it possible to classify a dynamic IP address as personal data under the directive? It will be necessary to determine whether it is sufficient, for that purpose, that there is a mere possibility, in the abstract, of ascertaining those data or whether, on the contrary, they must be available to the person who already knows the dynamic IP address or to a third party.

12 — Reproduced in point 13.

13 — Reproduced in point 11.

14 — As recalled by Advocate General Cruz Villalón in his Opinion in *Scarlet Extended* (C-70/10, EU:C:2011:255, point 76), and as concluded by the European Data Protection Supervisor in his Opinions of 22 February 2010 on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA) (OJ 2010 C 147, p. 1, paragraph 24) and of 10 May 2010 on the proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA (OJ 2010 C 323, p. 6, paragraph 11).

15 — See, in that regard, the judgment in *Österreichischer Rundfunk* (C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraph 68), and the Opinion of Advocate General Kokott in *Promusicae* (C-275/06, EU:C:2007:454, point 51 et seq.).

16 — It may be presumed, in the absence of proof to the contrary, that that person is the one who surfed the Internet and accessed the corresponding web page. However, even disregarding that last presumption, information concerning the date and time of access to a web page and the numerical address from which it originated would allow that access operation to be linked to the owner of the device and to be linked indirectly with his patterns of behaviour on the Internet. A possible exception would be IP addresses allocated to computers on premises such as cyber cafés, whose anonymous users are unidentifiable and concerning whose owners the traffic generated at the premises provides no relevant personal information. This is, moreover, the only exception to the principle that IP addresses are personal data accepted by the Working Party on the Protection of Individuals with regard to the Processing of Personal Data, established by Directive 95/46 ('the Article 29 Working Party'). Its Opinion No 4/2007 of 20 June 2007 on the concept of personal data, WP 136, can be read at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

60. The parties have focused their observations on the interpretation of recital 26 of Directive 95/46, whose content includes the expression 'means likely reasonably to be used either by the controller or by any other person to identify the said person'. The question of the referring court does not refer to additional data held by the service providers involved in the main proceedings. Nor does it refer to any third party holding that additional data (which in combination with the dynamic IP address facilitates the identification of the user), but refers instead to the Internet service provider.

61. In this case, therefore, it is not necessary for the Court to analyse all the means which the defendant in the main proceedings might 'reasonably' use in order for it to be possible to classify as personal data the dynamic IP addresses held by the defendant. Since the Bundesgerichtshof (Federal Court of Justice) refers only to additional data held by a third party, it can be inferred: (a) either that the defendant does not have its own additional data allowing identification of the user; (b) or that, if it has available those data, it is not in a position reasonably to use them for that purpose, as the controller, in accordance with recital 26 of Directive 95/46.

62. Both situations depend on a finding of fact which it is for the referring court alone to make. The Court could provide general criteria for interpreting the expressions 'means likely reasonably to be used … by the controller', if the Bundesgerichtshof (Federal Court of Justice) has any doubts concerning the ability of the defendant reasonably to use its own additional data. Since that is not the case, I take the view that it would be misplaced for the Court to lay down criteria for interpretation which the referring court does not need and has not requested.

63. The heart of the question referred is therefore concerned with whether it is relevant, in order to classify dynamic IP addresses as personal data, that a very specific third party — the Internet access service provider — has additional data which, combined with those addresses, may identify a user who has visited a particular web page.

64. Again, it is necessary to refer to recital 26 of Directive 95/46. The expression 'means likely reasonably to be used … *by any other person*' [17] could give rise to an interpretation according to which, in order to regard that address as constituting personal data in itself, it would be sufficient that any third party might obtain additional data (capable of being combined with a dynamic IP address in order to identify a person).

65. That overly strict interpretation would lead, in practice, to the classification as personal data of all kinds of information, no matter how insufficient it is in itself to facilitate the identification of a user. It would never be possible to rule out, with absolute certainty, the possibility that there is no third party in possession of additional data which may be combined with that information and are, therefore, capable of revealing a person's identity.

66. In my opinion, the possibility that advances in technical means will, in the more or less immediate future, significantly facilitate access to increasingly sophisticated instruments for collecting and processing data justifies the safeguards put in place in defence of privacy. Efforts have been made, when defining the relevant legal categories in the field of data protection, to include factual scenarios which are sufficiently broad and flexible to cover any conceivable situation. [18]

17 — Emphasis added.

18 — That precautionary and preventive objective forms the basis of the position adopted by the Article 29 Working Party, which, as I have stated, considers that it is necessary to start from the assumption that IP addresses are personal data, the only exception being where a service provider is in a position to determine with absolute certainty that those addresses relate to unidentifiable persons, such as the users of a cyber café. See footnote 16, *in fine*.

67. However, I think that that concern — which, moreover, is quite legitimate — must not result in a failure to take account of the terms in which the legislature has formulated its intentions and that a systematic interpretation of recital 26 of Directive 95/46 would be 'the means likely reasonably to be used' *by certain third parties*.

68. Just as recital 26 refers not to any means which may be used by the controller (in this case, the provider of services on the Internet), but only to those that it is likely 'reasonably' to use, the legislature must also be understood as referring to 'third parties' who, *also in a reasonable manner*, may be approached by a controller seeking to obtain additional data for the purpose of identification. This will not occur when contact with those third parties is, in fact, very costly in human and economic terms, or practically impossible or prohibited by law. Otherwise, as noted earlier, it would be virtually impossible to discriminate between the various means, since it would always be possible to imagine the hypothetical contingency of a third party who, no matter how inaccessible to the provider of services on the Internet, could — now or in the future — have additional relevant data to assist in the identification of a user.

69. As previously stated, the third-party to whom the Bundesgerichtshof (Federal Court of Justice) refers is an Internet service provider. This is surely the third party whom it is more reasonable to think that the service provider will approach to collect any additional data required, if it aims to identify in the most effective, practical and direct way a user who has accessed its website using the dynamic IP address. This is by no means a hypothetical, unknown and inaccessible third party, but a main player in the structure of the Internet, who is known with certainty to be in possession of the data required by the service provider to identify a user. In fact, as stated by the referring court, it is that particular third party which the defendant in the main proceedings intends to approach in order to collect the necessary additional data.

70. The Internet access service provider is, typically, the third party referred to in recital 26 of Directive 95/46 who might most 'reasonably' be approached by the service provider in the main proceedings. It remains to be established, however, whether obtaining the additional data held by that third party can be described as 'reasonably' feasible or practicable.

71. The German Government argues that, since the information held by the Internet access service provider is personal data, the latter simply cannot disclose it, save in accordance with the legislation on the processing of such data. [19]

72. No doubt this is the case, since in order to access that information regard must be had to the legislation applicable to personal data. Information may be obtained 'reasonably' only if the conditions governing access to that kind of data are satisfied, the first of which being the legal possibility of retaining and transferring it to others. It is true that the Internet access service provider may refuse to reveal the data concerned but the opposite is also possible. The possibility that the data may be transferred, which is perfectly 'reasonable', itself transforms the dynamic IP address, in accordance with recital 26 of Directive 95/46, into personal data for the provider of services on the Internet.

73. That is a practical possibility *within the framework of the law* and, therefore, 'reasonable'. The reasonable means of access referred to in Directive 95/46 must, by definition, be lawful means. [20] That is, naturally, the premiss on which the referring court proceeds, as the German Government points out. [21] Thus, the legally relevant means of access are reduced significantly, since they must be exclusively lawful. However, so long as they exist, no matter how restrictive they may be in their practical application, they constitute a 'reasonable means', for the purpose of Directive 95/46.

19 — Paragraphs 40 and 45 of its written observations.

20 — It is irrelevant, in that context, that access to the personal data is possible *de facto* by infringing data protection laws.

21 — Paragraphs 47 and 48 of its written observations.

74. As a result, I am of the view that, as formulated by the Bundesgerichtshof (Federal Court of Justice), the first of its questions should be answered in the affirmative. A dynamic IP address must be classified, for the provider of Internet services, as personal data in view of the existence of a third party (the Internet service provider) which may reasonably be approached in order to obtain other additional data that, combined with a dynamic IP address, can facilitate the identification of a user.

75. I think that my proposal is strengthened by the result to which the contrary solution would lead. If dynamic IP addresses do not constitute personal data for a provider of services on the Internet, it could keep them indefinitely and could request at any time from the Internet access service provider additional data to combine with the IP address in order identify the user. In those circumstances, as the German Government accepts,[22] the dynamic IP address would become personal data, since it would already have available additional data to identify the user, applying in that respect the data protection legislation.

76. However, they would be data which it had been possible to retain only because they had not, until then, been regarded as personal data for the service provider. The legal classification of a dynamic IP address as personal data would thus be left to the latter, conditional upon the possibility that, in the future, it may decide to use them to identify the user by combining that data with additional data that it would have to collect from a third party. In my opinion, however, the decisive factor according to Directive 95/46 is the — reasonable — possibility of the existence of an 'accessible' third party, having the means necessary to facilitate the identification of a person, not the possibility that an approach will be made to that third party.

77. It might even be accepted, as the German Government argues, that the dynamic IP address only becomes personal data when the Internet service provider receives it. However, it would then have to be accepted that that classification was applied retroactively, as regards the period of retention of the IP address, and therefore the IP address regarded as non-existent if it has been retained beyond the period which would have been permitted had it been classified from the outset as personal data. If that approach is adopted it will bring about a result contrary to the spirit of the legislation on the protection of personal data. The reason that the retention of such data is justified only temporarily would be circumvented by any delay in determining the relevance of a quality which is inherent that data from the outset: their potential as a means of identifying — by themselves or together with other data — a natural person. For that purely logical reason, it is more reasonable to attribute that nature to the data from the outset.

78. Therefore, as a first conclusion, I consider that Article 2(a) of Directive 95/46 must be interpreted as meaning that an IP address stored by a service provider in connection with access to its web page constitutes personal data for that service provider, insofar as an Internet service provider has available additional data which make it possible to identify the data subject.

B – *Second question*

79. By its second question the Bundesgerichtshof (Federal Court of Justice) seeks to ascertain whether Article 7(f) of Directive 95/46 precludes national legislation which allows the collection and use of a user's personal data, without his consent, only to the extent necessary in order to facilitate, and charge for, the specific use of the telemedium by the user concerned, and under which the purpose of ensuring the general operability of the telemedium cannot justify use of the data after the use of the telemedium.

22 — Paragraph 36 of its written observations.

80. Before answering that question it is necessary to make an observation concerning the information provided by the Bundesgerichtshof (Federal Court of Justice), according to which the data at issue are retained to ensure the proper functioning of the websites involved in the main proceedings, making it possible, where appropriate, to bring criminal proceedings in connection with possible cyber attacks against those websites.

81. It is therefore necessary, above all, to raise the question of whether the processing of IP addresses referred to in the order for reference is covered by the derogation provided for in the first indent of Article 3(2) of Directive 95/46. [23]

1. The applicability of Directive 95/46 to the processing of the data at issue

82. It appears that the Federal Republic of Germany is acting in the main proceedings as a mere provider of services on the Internet, that is to say as an individual (and, therefore, *sine imperio*). This fact suggests that, in principle, the processing of the data at issue in this dispute is not excluded from the scope of Directive 95/46.

83. As the Court stated in the judgment in *Lindqvist*, [24] the activities in Article 3(2) of Directive 95/46 'are, in any event, activities of the State or of State authorities and unrelated to the fields of activity of individuals'. [25] Insofar as the controller for the processing of the disputed data is, despite its status as a public authority, actually acting as a private individual, Directive 95/46 is applicable.

84. The referring court, by highlighting the main purpose pursued by the German administration through the storage of dynamic IP addresses, points out that it seeks 'to guarantee and maintain the security and operationality of its telemedia' and, in particular, to contribute in 'recognising and protecting against denial-of-service attacks, which frequently occur and which involve paralysing the telecommunications infrastructure by means of targeted and coordinated saturation of individual web servers with huge numbers of requests'. [26] Website owners of a certain size commonly retain dynamic IP addresses for that purpose and this does not imply, directly or indirectly, the exercise of public powers, so their inclusion within the scope of Directive 95/46 does not involve excessive difficulty.

85. The Bundesgerichtshof (Federal Court of Justice) asserts, however, that the retention of dynamic IP addresses by the service providers involved in the main proceedings is also intended to allow criminal proceedings, where appropriate, to be brought against the perpetrators of possible cyber attacks. Is that intention sufficient to exclude the processing of such data from the scope of Directive 95/46?

86. In my opinion, if 'criminal proceedings' are understood to mean exercise of the State's *ius puniendi* by the service providers who are defendants in the main proceedings, this case would be concerned with 'activities of the State in areas of criminal law' and, therefore, with one of the exceptions provided for in the first indent of Article 3(2) of Directive 95/46.

87. In those circumstances, pursuant to the rule established by the Court in the judgment in *Huber*, [27] the processing of personal data by service providers in the interests of the security and technical operation of their telemedia, falls within the scope of Directive 95/46, while the processing of data concerning the activities of the State in areas of criminal law falls outside its scope.

23 — 'Processing operations concerning public security, defence, State security … *and the activities of the State in areas of criminal law*' do not fall within the scope of Directive 95/46 (emphasis added).

24 — C-101/01, EU:C:2003:596, paragraph 43.

25 — To the same effect, see judgment in *Satakunnan Markkinapörssi and Satamedia* (C-73/07, EU:C:2008:727, paragraph 41).

26 — Paragraph 36 of the order for reference.

27 — C-524/06, EU:C:2008:724, paragraph 45.

88. In the same way, even where the Federal Republic of Germany, acting merely as a service provider *sine imperio*, is not responsible for bringing criminal proceedings as such, but, like any other individual, simply transfers the IP addresses at issue to a State body for the purposes of prosecution, the objective of processing the dynamic IP addresses would also be an activity excluded from the scope of Directive 95/46.

89. This is clear from the judgment in *Parliament* v *Council and Commission*,[28] in which the Court stated that the fact that certain personal data 'have been collected by private operators for commercial purposes and it is they who arrange for their transfer to a third country' does not mean that that transfer 'is not covered by' the first indent of Article 3(2) of Directive 95/46 when the purpose of the transfer is activities of the State in areas of criminal law, since in that case it 'falls within a framework established by the public authorities that relates to public security'.[29]

90. However, if, as I think, 'criminal proceedings' is to be understood, as is clear from the order for reference, as being concerned with a person's entitlement to initiate the State's exercise of *ius puniendi*, through appropriate proceedings, then it is not possible to argue that the purpose of processing dynamic IP addresses is an activity of the State in areas of criminal law which is excluded from the scope of Directive 95/46.

91. The retention and storage of those data would serve as a further means of proof which could be used by the owner of a website to request that the State prosecute unlawful conduct. It would, in short, be an instrument for upholding in criminal proceedings the legally recognised rights of an individual (in this case, a public entity acting under private law). It is no different, from that perspective, than the initiative of any other provider of a service on the Internet seeking State protection in accordance with the procedures for initiating criminal proceedings established by law.

92. As a result, to the extent that the German administration is acting as a provider of services on the Internet having no public authority powers, an assessment which it is for the referring court to make, its processing of dynamic IP addresses, as personal data, falls within the scope of Directive 95/46.

2. Substance

93. Paragraph 15(1) of the TMG authorises the collection and use of a user's personal data only to the extent necessary in order to facilitate, and charge for, a specific use of the telemedium. More specifically, a service provider can collect and use only so-called 'data concerning use', that is the personal data of a user which are necessary in order to 'facilitate, and charge for, the use of telemedia'. Those data should be deleted after the operation has ended (that is as soon as the particular use of the telemedium ends), unless they must be kept 'for the purposes of charging', as provided for in paragraph 15(4) of the TMG.

94. When a connection has been terminated, paragraph 15 of the TMG seems to rule out the storage of data concerning use for other reasons, including that of safeguarding 'the use of telemedia' in general. By referring exclusively to the purposes of invoicing as justification for the retention of data, that provision of the TMG could be read (though its definitive interpretation is a matter for the referring court) as requiring that data concerning use should be used only to allow a particular connection and should be deleted when it ends.

28 — C-317/04 and C-318/04, EU:C:2006:346, paragraphs 54 to 59.

29 — Ibid., paragraph 59. It related to personal data whose processing was not necessary for the provision of the services constituting the business of the private operators concerned (airlines), but which they were obliged to transfer to the US authorities to prevent and combat terrorism.

95. Article 7(f) of Directive 95/46 [30] authorises the processing of personal data in terms which I would describe as more generous (for the controller) than those laid down in the actual wording of paragraph 15 of the TMG. The German provision may be classed, in that regard, as more restrictive than that of the European Union, since, in principle, it fails to provide for the purposes of a legitimate interest other than that linked to the invoicing of the service, even though, as the provider of services on the Internet, the Federal Republic of Germany could also have a legitimate interest in ensuring the proper functioning of its web pages, beyond each period of use. [31]

96. The case-law of the Court in the judgment in *ASNEF and FECEMD* [32] provides guidance in answering the second question referred. The Court stated in that judgment that from the objective pursued by Directive 95/46 'it follows … that Article 7 of Directive 95/46 sets out an exhaustive and restrictive list of cases in which the processing of personal data can be regarded as being lawful'. [33] Therefore, 'Member States cannot add new principles relating to the lawfulness of the processing of personal data to Article 7 of Directive 95/46 or impose additional requirements that have the effect of amending the scope of one of the six principles provided for in Article 7'. [34]

97. Paragraph 15 of the TMG does not add an additional requirement to those provided for in Article 7 of Directive 95/46 for the lawfulness of processing data — as occurred in *ASNEF and FECEMD* [35] — but, if it is interpreted in the restrictive way referred to by the referring court, it limits the material scope of the condition referred to in Article 7(f) thereof: whereas the legislature of the Union refers, in general, to the purposes of the 'legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed', paragraph 15 of the TMG covers only the need to 'facilitate, and charge for, the [specific] use of telemedia'.

98. As in *ASNEF and FECEMD*, [36] in this case to a national measure — again, if interpreted in the restrictive way explained above — would amend the scope of a principle of Article 7 of Directive 95/46, rather than merely defining it, which is all that the authorities of each Member State have the discretion to do pursuant to Article 5 of Directive 95/46.

99. According to that latter provision, 'Member States shall, within the limits of the provisions of this Chapter, [[37]] determine more precisely the conditions under which the processing of personal data is lawful'. However, as was stated in the judgment in *ASNEF and FECEMD*, [38] 'under [that provision], Member States also cannot introduce principles relating to the lawfulness of the processing of personal data other than those listed in Article 7 thereof, nor can they amend, by additional requirements, the scope of the six principles provided for in Article 7'.

30 — Reproduced in point 17.

31 — See point 84. Certainly, owners of web pages have a legitimate interest in preventing and combating denials of service, as mentioned by the referring court, that is, the massive and concerted attacks sometimes launched against web sites to overwhelm them and render them inoperative.

32 — C-468/10 and C-469/10, EU:C:2011:777.

33 — Ibid., paragraph 30.

34 — Ibid., paragraph 32.

35 — A situation in which the national legislation added to the requirements in Article 7(f) of Directive 95/46 the requirement that the data which are the subject of processing be in sources accessible to the public.

36 — C-468/10 and C-469/10, EU:C:2011:777.

37 — Chapter II, entitled 'General rules on the lawfulness of the processing of personal data', which comprises Articles 5 to 21 of Directive 95/46.

38 — C-468/10 and C-469/10, EU:C:2011:777, paragraph 36.

100. Paragraph 15 of the TMG would substantially reduce, with regard to Article 7(f) of Directive 95/46, the scope of the relevant legitimate interest justifying the processing of data and not merely define or qualify it within the limits authorised by Article 5 of that directive. Moreover, it would do so in such a categorical and absolute manner that it would not be possible for the protection and safeguarding of the general use of a telemedium to be balanced against the 'interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1)' of Directive 95/46, as laid down in Article 7(f) thereof.

101. Ultimately, as in the judgment in *ASNEF and FECEMD*,[39] 'it is no longer a precision within the meaning of Article 5 of Directive 95/46' if the German legislature 'definitively' prescribes for particular categories of personal data 'the result of the balancing of the opposing rights and interests, without allowing a different result by virtue of the particular circumstances of an individual case'.

102. In those circumstances, I am of the view that the Bundesgerichtshof (Federal Court of Justice) is required to interpret the national legislation in a manner consistent with Directive 95/46, which means that: (a) the justifications for processing 'data concerning use' may include the legitimate interest of the provider of telemedia to protect the general use of telemedia, and (b) that interests of the service provider can be balanced, on a case-by-case basis, against the user's interests or fundamental rights and freedoms, in order to clarify which merits protection under Article 1(1) of Directive 95/46.[40]

103. In my view nothing further can be said concerning the basis on which that balancing exercise must be carried out in the case which gave rise to the reference for a preliminary ruling. The Bundesgerichtshof (Federal Court of Justice) raises no question on this point, since it is concerned with the solution to a question prior to that balancing exercise; that is to say whether that exercise can be carried out.

104. Finally, it seems superfluous to point out that the referring court may take into account any legal provisions adopted by the Member State within the framework of the authorisation contained in Article 13(1)(d) of Directive 95/46 to restrict the scope of the obligations and rights provided for in Article 6 of that directive, when necessary to safeguard, inter alia, '… the prevention, investigation, detection and prosecution of criminal offences …'. Nor does the referring court refer to that matter, aware no doubt of the existence of both articles.

105. I therefore suggest as a response to the second question referred that Article 7(f) of Directive 95/46 precludes national legislation the interpretation of which prevents a service provider from collecting and processing a user's personal data after each period of use, without his consent, in order to ensure the functioning of the telemedium.

VI – Conclusion

106. In view of the foregoing I propose that the Court answer the questions referred to it as follows:

(1) Pursuant to Article 2(a) 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, a dynamic IP address, through which a user has accessed the web page of a provider of telemedia, constitutes for the latter 'personal data', to the extent that an Internet service provider has other additional data which, when linked to the dynamic IP address, facilitates identification of the user.

39 — Ibid., paragraph 47.

40 — At the hearing, Mr Breyer's submission rejected the argument that the storage of dynamic IP addresses is necessary to protect the proper functioning of Internet services against possible attacks. I do not think that a categorical answer can be given in relation to that problem, whose solution, on the contrary, must be preceded, in each particular case, by a balancing of the interests of the website owner and the rights and interests of users.

(2) Article 7(f) of Directive 95/46 must be interpreted as meaning that the objective of ensuring the functioning of a telemedium can, in principle, be regarded as a legitimate interest, the purposes of which justify the processing of personal data, subject to an assessment that that interest prevails over the interests or fundamental rights of the person concerned. A national provision which did not allow that legitimate interest to be taken into account would be incompatible with that article.