OPINION OF ADVOCATE GENERAL
MANUEL CAMPOS SÁNCHEZ-Bordona
of 12 May 2016 (1)

Case C-582/14
Patrick Breyer
against
Federal Republic of Germany

(Preliminary ruling from the Bundesgerichtshof, Germany)
"Processing of personal data - Directive 95/46 / EC -... Article 2 literally a and Article 7 literally f -. Concept personenbezogeneDaten' - IP addresses - storage by a service provider for Telemedia - National legislation consideration the legitimate interest of the data controller does not allow "

1. An Internet Protocol address ('the IP address) is a numerical sequence of binary numbers, which is assigned to a device (a computer, a tablet or a smartphone), identifies this and it allows access to the electronic communications network. For a connection to the Internet, the device must use that assigned by the Internet access providers digit sequence. The IP address is transmitted to the server on which the retrieved website is stored.
2. The Internet access provider (generally the telephone companies) have their customers for each connection to the Internet for a limited period of so-called "dynamic IP address" to that change on subsequent connects. These companies keep a record about which IP address they had assigned to a particular device at the time (2).
3. usually the owner of the web pages, which are accessed by means of dynamic IP addresses lead, also directories where they store what pages were accessed when and by which dynamic IP address. These directories can be stored indefinitely technically after the Internet connection of the respective user.
4. A dynamic IP address is not enough on its own, so the service provider can identify the users of its website. He can, however, if he combines the dynamic IP address with other additional data on the Internet provider offers.
5. In the main proceedings it is being debated whether a dynamic IP address, personal data within the meaning of Art. 2, pt. A to Directive 95/46 / EC (3 are). To answer this question first have to clarify what importance is attached to the fact that the additional data required for the identification of the user are not (specifically the Internet access provider) held by the holder of the website, but is owned by a third party.
6. This question is not decided by the Court. In Rn. 51 of the judgment Scarlet Extended (4) he has indeed found that it is IP addresses "is protected personal data because the precise identification of users possible", but in a context in which the storage and identification of IP addresses by the Internet access provider (5) was carried out and not, as here by the content providers.
7. If the dynamic IP addresses are personal data for the Internet service provider, is then necessary to consider whether their processing falls within the scope of Directive 95/46.
8. may enjoy these addresses, even though they constitute personal data, not the protection of Directive 95/46, if z. B. is manipulating the prosecution of possible attacks on the website. In this case, Directive 95/46 2 first indent under Art. 3, para. Not applicable.
9. In addition, it must be clarified whether the Internet service provider that stores the dynamic IP addresses when users retrieve its websites (the Federal Republic of Germany in this case), acting in the exercise of official authority or as a private person.
10. If Directive 95/46 is applicable, is finally clarify the extent to which national legislation is compatible with Art. 7 literally. F this Directive which restricts the scope of the measures provided for in that provision to justify the processing of personal data.

I - Legal background

A - *Union law*

11. The 26th recital of Directive 95/46 reads as follows:

"(26) The principles of protection must apply to any information concerning an identified or identifiable person. In deciding whether a person is identifiable, all means should be taken into account, which could be reasonably used either by the person responsible for processing or by a third party to identify the said person. The principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable. The rules of conduct within the meaning of Article 27 may be a useful instrument for providing guidance to the, how to anonymize and store in a form, the data that makes the identification of the data subject impossible. "

12. Art. 1 of Directive 95/46 provides:

"(1) Member States shall ensure pursuant to the provisions of this Directive to protect the fundamental rights and freedoms, in particular the protection of privacy of individuals with regard to the processing of personal data.
(2) restrict Member States or prohibit the free flow of personal data between Member States for reasons referred to in paragraph 1 with the protection afforded. "

13. Art. 2 of Directive 95/46 provides:

"For the purposes of this Directive, the expressions
onal data "any information concerning 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 specific elements which are to his physical, physiological, mental, economic, cultural or social identity;
essing of personal data '(' processing ') each operation is performed upon or not by automatic means or any process set of operations upon personal data such as collection, recording, organization, storage, adaptation or alteration, retrieval, the consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
...
controller "means 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. Are the purposes and means of the processing of personal data laid down in national or Community laws or regulations, the data controller or the specific criteria for its nomination may be determined by national or Community law;
...
'a natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons authorized under the direct responsibility of the controller or the processor are to process the data;
... "

14. Art. 3 ("Scope") of Directive 95/46 provides:

"(1) This Directive shall apply to all or part of automated processing of personal data as well as for the non-automated processing of personal data that is stored in a file or to be saved.
(2) This Directive shall not apply to the processing of personal data:
ne course of an activity which falls outside the scope of Community law, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to processing operations concerning public security, defense, the security of the State (including the economic well when processing the State security matters) and the activities of the State in areas of criminal law;
... "

15. Chapter II ("General rules on the lawfulness of the processing of personal data") of Directive 95/46 is introduced by Article 5, which reads:. "Member States shall determine in accordance with this chapter more precisely the conditions under which the processing of personal data is lawful. "

16. Art. 6 of Directive 95/46 provides:

"(1) Member States shall provide that personal data
rocessed fairly and lawfully;
ected for specified, explicit and legitimate purposes and not further processed in a with those purposes incompatible manner. Further processing of data for historical, statistical or scientific purposes is not generally to be considered incompatible with the purposes of the previous data collection, provided that Member States provide appropriate safeguards;
ply with the purposes for which they are collected and / or further processed, are adequate, relevant and not excessive;
ccurate and kept, if necessary, up to date; there are to take all reasonable measures to ensure that inaccurate or incomplete data be deleted or corrected with regard to the purposes for which they are collected or further processed;
o longer than it is for the realization of the purposes for which they are collected or further processed, required to be kept in a form which permits identification of data subjects. The Member States shall provide appropriate

safeguards for personal data stored for longer periods for historical, statistical or scientific purposes.
(2) The data controller is responsible for compliance with paragraph 1. "

17. Art. 7 of Directive 95/46 provides:

"Member States shall provide that the processing of personal data is allowed only if one of the following conditions is met:
lata subject has unambiguously given his consent;
processing is necessary for the performance of a contract, the contracting party is the person, or for the performance of pre-action carried out at the request of the person concerned;
essing is necessary for compliance with a legal obligation to which the subject of the data controller;
essing is necessary for the protection of the vital interests of the data subject;
essing is necessary for the performance of a task in the public interest or in the exercise of official authority vested in the data controller or the third party to whom the data are disclosed;
essing is necessary for the fulfillment of the legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the interest or the fundamental rights and freedoms of the data subject, in accordance with Article 1, paragraph 1 are protected, predominate. "

18. Art. 13 of Directive 95/46:

"(1) Member States may adopt legislative measures which the duties and rights under Article 6, paragraph 1, Article 10, Article 11, paragraph 1, Articles 12 and 21 when such a restriction is necessary for:
a) national security;
b) national defense;
c) public security;
prevention, investigation, detection and prosecution of criminal offenses or of breaches of ethics for regulated professions;
nportant economic or financial interest of a Member State or the European Union, including monetary, budgetary and taxation matters;
nitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority for the purposes referred to in points c), d) and e);
rotection of the data subject and the rights and freedoms of others.
... "

B - *National law*

19. § 12 Telemedia Act (hereinafter TMG) (6) provides:

"(1) The service provider may only collect and use personal data for the provision of telemedia, unless this Act or another law, which expressly refers to Telemedia, permits or the user has consented.
(2) The service provider may use the data collected for the provision of telemedia personal data for other purposes, unless this Act or another law, which expressly refers to Telemedia, permits or the user has consented.
(3) Unless otherwise determined, the current rules for the protection of personal data are to be applied, even if the data are not processed automatically. "

20. § 15 TMG is as follows:

"(1) The service provider may only collect and use, to the extent necessary to permit the use of tele-media and invoice (user data), personal data of a user. Usage data is particularly
1. Features to identify the user,
2. Information on the start and end and the extent of the current use and
3. Information about the utilized by the user telemedia.
(2) The service provider may merge user data of a user about the use of different telemedia, insofar as is necessary for billing purposes with the user.
...
(4) The service provider may use usage data beyond the end of user activity beyond the extent necessary for the purpose of billing the user (accounting data). To comply with existing legal, statutory or contractual retention periods of service provider may block the data. ... "

21. In accordance with § 3 para 1 Federal Data Protection Act (hereinafter the Act). (7) are "[p] ersonenbezogene data ... details of personal or material circumstances of an identified or identifiable natural person (data subject) ..."

II - Facts

22. Mr. Breyer has raised against the Federal Republic of Germany brought an action for failure to storing IP addresses.

23. Many public sector bodies in Germany operate publicly accessible Internet portals where they provide updated information. To prevent attacks and to allow for the prosecution of attackers, all accesses are recorded in log files in most of these portals. This even after the end of each use operation, the name of the file or page, entered in search boxes terms, the time of retrieval, the amount of data transmitted, the determination of the successful retrieval and the IP address of the accessing computer are stored.

24. Mr. Breyer, who has called several such sites, sought an order the Federal Republic of Germany, to refrain,

to save the IP address of the accessing host system or to be stored by a third party, provided that the storage is not in case of failure to restore the availability is the tele medium required.

25. The action brought by Mr Breyer was dismissed at first instance. His appointment, however partially succeeded, and the Federal Republic of Germany was ordered to refrain from storing on the end of each user activity beyond. The injunction was subject to the condition that the applicant during the use process his personal data, in the form of an e-mail address, indicating and that the storage is not in case of failure to restore the availability of Tele medium required.

III - Questions

26. After both parties have lodged an appeal, has the VI. The following questions for a preliminary ruling Civil Division of the Federal December 17, 2014:

t. 2, pt. A to Directive 95/46 / EC be interpreted as meaning that an Internet Protocol address (IP address) that stores a service provider in connection with the access to its website, for this already then a piece of personal data represents, if a third party (in this case access provider) has the additional knowledge required to identify the person concerned?

; Article. 7 literally. F the Data Protection Directive a provision of national law according to which the service provider may only collect and use personal data without the user's consent, to the extent necessary to the actual implementation of the tele medium through the respective to enable users and settle, and what the purpose of ensuring the general functioning of the tele medium, the use can not be justified on the end of each user activity beyond?

27. According to the referring court, the plaintiff could demand a halt to the storage of the IP addresses under German law, if their storage under the Privacy Law unlawful interference in his general personality rights, specifically his right to informational self-determination (§ 1004 Abs would. 1, § 823 para. 1 of the Civil Code in conjunction with Art. 1 and 2 of the basic law) represent.

28. This would be the case if a) the IP address (in any case, together with the date of access to an Internet site) to the "personal information" within the meaning of Art. 2, pt. A in conjunction with the 26th recital set 2 of Directive 95/46 or within the meaning of § 12 para. 1 and 3 TMG in conjunction with § 3 para. 1 BDSG counted, and b) a permission event within the meaning of Art. 7 literally. f Directive 95/46 or within the meaning of § 12 para. 1 and 3 and § 15 para. 1 and 4 TMG were not present.

29. The Bundesgerichtshof According it is 2 for the interpretation of national law (§ 12 Abs. 1 TMG) depends on how the personal reference in Art. Pt. A Directive is to be understood 95/46.

30. Moreover, should, as the Court of Appeal of the service provider in accordance with § 15 Abs. 1 TMG only collect and use, as far as this is necessary to allow the use of tele-media and account (user data) (personal data of a user 8). The interpretation of this provision of national law depends on the interpretation of Art. 7 literally. F Directive 95/46 from.

IV - Procedure before the Court and arguments of the parties

31. Written observations have been submitted by the German, Austrian and Portuguese Governments and the Commission. For hearing on February 25, 2016, only the Commission and Mr Breyer appeared, while the German government has decided not to participate.

A - *Arguments of the parties on the first question*

32. Mr. Breyer contends, as personal data are also such data to look at, their combination is only theoretically possible, d. H. When they claimed that a possible abstract danger, when it did not matter whether the data would actually combined in practice. The fact that a point is possibly largely unable to identify a person by their IP address, does not mean that there is not such a risk for this person. It should also be of significance that Germany its IP data store, where appropriate, to identify or prosecute what was 113 Telecommunications Act allowed and often happen to § Author any attacks.

33. According to the German Government, the first question is in the negative. Dynamic IP addresses are not stored, the identity of a "certain" person within the meaning of Art. 2, pt. A to Directive 95/46 open. In order to determine whether they contained information about an "identifiable" person within the meaning of that provision, the question which must *determinability* for a "relative" measure to be checked. This follows from the 26th recital of Directive 95/46, according to which only the means necessary to take account the "reasonably" either could be used by the data controller or by a third party to identify the said person. This would clarify that the European Union legislature in such cases do not have the scope of Directive 95/46 want to include, where an identification by any third party is objectively possible.

34. The German Government also considers that the term "personal data" within the meaning of Art. 2, pt. A to Directive 95/46 for the purpose of this Directive, namely to guarantee fundamental rights, must be interpreted accordingly. The need for protection of individuals could be represented differently, depending on who own the data and whether it had the resources to use them to identify the persons concerned.

35. The identity of Mr. Breyer let not be determined using the IP address in conjunction with the additional information that would be stored by the providers of content. For this purpose the information was necessary, at their disposal, the Internet access provider, which this but the providers of the content is not likely to make it accessible, because it it is no legal basis.

36. For the Austrian Government is in the affirmative the question, however. After Recital 26 of Directive 95/46 it is not necessary for the identifiability of a person that befänden all data to identify them in the hands of a single body. So can an IP address be regarded as piece of personal data, if a third party (such. As the Internet access provider) had the resources to identify the owner of that address without a disproportionate effort.

37. The Portuguese Government also tends to answer in the affirmative. In its submission, the IP address in conjunction with the time of the query process, a piece of personal data is, as far as they could, through a different location than the one store the IP address to identify the user.

38. The Commission also proposes to answer in the affirmative, and relies on the Court's decision in the Scarlet Extended case (9). Since the storage of IP addresses just to serve to identify in case of cyber attacks, users, spot the use of additional data stored by the Internet access providers a means represents that "reasonably" used in the sense of recital 26 of Directive 95/46 could be. The Commission considers Ultimately speak both the objective pursued by that directive and the purpose of Article 7 and 8 of the Charter of Fundamental Rights of the European Union ('the Charter')... For a broad interpretation of Article 2 of Directive 95/46 literally a ,

B - *Arguments of the parties on the second question*

39. Mr. Breyer believes that Art. 7 literally. F of Directive 95/46 constitutes a general clause, which needed for their practical implementation of concrete. In accordance with the Court of Justice, the circumstances of the individual case must be assessed and determined whether there are groups with a legitimate interest within the meaning of that provision. If this is the case, it is not only permissible but essential for the application of this article to provide special arrangements for these groups. In the present case 7, the national legislation with Art. Literally. F Directive 95/46 compatible, since no interest of the provider of the public portal to the storage of personal data exists or outweighed the interest in protecting the anonymity. Nevertheless, a systematic personal data storage is a democratic society incompatible and neither necessary nor appropriate in order to ensure the operability of Telemedia, which without storage of such personal data is quite possible, as the websites of some ministries showed.

40. The German Government submits that the second question should not be answered, because it had been made only in the event that the first question should be answered in the affirmative, what in their view is not the case for the reasons mentioned above.

41. The Austrian Government proposes a reply that Directive 95/46 of storage such as the issue here data not generally precluded provided that it is indispensable to ensure the proper functioning of the Telemedia. A limited storage of the IP address for the duration of the call of a website would also help in view of the commitment of the processing of personal data in charge, which apply from Art. 17 para. 1 of Directive 95/46 necessary measures to protect such data be lawful. The fight against cyber attacks might justify it, to analyze data, which refer to previous attacks, and specific IP addresses to deny access to the website. The proportionality of the storage of data such as those in the main proceedings at issue must in the light of the purpose, to ensure the proper functioning of the Telemedia, and taking into account the in Art. 6 para. 1 of Directive tested principles set 95/46 in each individual case will.

42. The Portuguese Government takes the view that Art. 7 literally. F of Directive 95/46 does not preclude the issue in the main proceedings national legislation, because the German legislature prescribed in that provision balance of interests between the legitimate interests of the processing of personal data controllers on the one hand and the rights and freedoms of the holders of these data have on the other hand already made.

43. The Commission considers that national legislation which Art. 7 literally. F of implementing Directive 95/46, must define the purpose of the processing of personal data so that they are predictable for the individuals concerned. The German legislation does not satisfy this requirement in that it provides in § 15 para. 1 TMG that the storage of IP addresses may be permitted "to the extent necessary to permit the use of tele-media".

44. The Commission therefore proposes to answer the second question as meaning that Art. 7 literally. F an interpretation of a national provision precludes which an agent working as a service provider Hoheitstrager could without his consent to collect personal information of a user with the purpose and use , the general functioning of the tele medium to ensure, when the national provision lays down the purpose is not sufficiently clear and precise.

V - Findings

A - *First question*

1. Delimitation of the question

45. According to the wording chosen by the Bundesgerichtshof should be answered to the first question, whether an IP address used to access the on a website that is for the public body, the owner of this page, a piece of personal data (as defined in Art. 2, pt. a to Directive 95/46 / EC) is when the Internet access provider has the additional knowledge required for the identification of the person concerned.

46. The question is sufficiently precise formulated to other questions about the legal nature of IP addresses that are *abstract* might ask *,* excluded in connection with the protection of personal data from the outset.

47. First, the Bundesgerichtshof relates solely to "dynamic IP address", d. H. On those that are assigned for a limited period for the respective connection to the Internet and modified in subsequent connections. The so-

called "fixed" or "static" IP addresses that are immutable and allow the permanent identification of network-connected device, thus disregarded.

48. Second, the national court starts from the assumption that the provider of the internet in the main proceedings not to be able to determine on the dynamic IP address, who is visiting its pages, yet itself has the extra data that it in connection with the IP address would allow the identification of this person. The Federal Court is obviously believes that the dynamic IP address in this context *for the provider of the internet* is not a piece of personal data within the meaning of Art. 2, pt. A to Directive 95/46.

49. The doubts of the referring court relate to the question whether the dynamic IP address for the provider of the internet can be a piece of personal data, *if a third party has the additional knowledge* , which, in conjunction with the IP address to identify the persons, calling its websites. It applies to the Federal Court, which is another important clarification, not limited to any third party who is in possession of additional information, but only to the Internet access provider (which he others who may have such data excludes).

50. Thus, inter alia, the following question is not the subject of discussions.. A) Are static IP addresses, personal data within the meaning of Directive 95/46 (10)? b) Are dynamic IP addresses, always and under all circumstances personal information under the Directive? c) Are finally inevitable qualify dynamic IP addresses as personal data as soon as a third party, who it may be, is able to use it to identify Internet users?

51. It is therefore solely to the determination of whether a dynamic IP address for the provider of an Internet service is a piece of personal data when the telecommunications company offering the Internet (access providers) additional data has in his hands, with associated the issue IP address enable the identification of the person who calls the system operated by the service provider website.

2. To answer the question

52. The issue raised in this reference question is very controversial in the German doctrine and jurisprudence, with two opinions are against (11). After a (the one "objective" or "absolute" approach pursued) is a user definable - and thus the IP address of a legitimate piece of personal data - if its identification regardless of the capabilities and resources of the Internet service provider alone by connecting the dynamic IP address with a third party (eg. as the Internet access provider) provided data is possible.

53. For the representatives of the other view (the one "relative" approach represented) extends the opportunity to serve for the purpose of the final identification of the user the help of a third party, is not sufficient to affirm the personal references with a dynamic IP address , What matters is that the one who has access to the date have, could take advantage of this with its own resources use and in this way to identify someone.

54. Notwithstanding this opinion dispute in national law the Court's answer must confine itself to interpreting the two provisions of Directive 95/46, to which both the referring court and the parties to the dispute relate, d. H. Art. 2, pt. A (12) and the 26th recital (13).

55. Dynamic IP addresses lay alone in that they provide information on date and time of access of a computer (or other device) to an internet site, certain patterns of behavior of Internet users open and therefore constitute a possible interference with the right to respect for for private life (14), which is guaranteed in Art. 8 of the European Convention for the protection of human rights and fundamental freedoms and in Art. 7 of the Charter, so that Directive 95/46 in the light and in the light of Art. 8 of the Charter interpreted is (15). In fact, the parties to the dispute does not consider this premise in doubt which is also not as such the subject of the question.

56. The person to whom the said single data relate, is not a "particular individual". The date and time of connection and their numeric origin can not directly or immediately recognize who is the natural person who owns the device, is visited by the of the website, nor the identity of the user, operating it (this may be any natural person).

57. Nevertheless, a dynamic IP address, to the extent that with their help - can find out who is the owner of the device used to access the Internet, as information about an "identifiable person" - alone or in conjunction with other data be considered (16).

58. The Bundesgerichtshof considers a dynamic IP address alone is not sufficient to identify the user who has called her a website. Could the Internet service provider on the other hand to identify the user based on the dynamic IP address, this would clearly as a piece of personal data within the meaning of Directive 95/46 to be regarded. Then, however, the question does not seem to aim in which it is assumed that the Internet service provider, at issue in the main proceedings, the user can not identify, using only the dynamic IP address.

59. In conjunction with other data, the dynamic IP address allows "indirect" identification of the user. At this point they all agree. Now allows the possible presence of such additional data, which can be connected to the dynamic IP address, without further ado, their classification as piece of personal data within the meaning of the Directive? It will be necessary to clarify whether this is sufficient the mere abstract possibility of access to this data or if a factor will be that they are available for those who already know the dynamic IP address, or a third party.

60. The parties focused in their observations on the interpretation of recital 26 of Directive 95/46 and set it on its formulation "means ... that could be reasonably used either by the person responsible for processing or by a third party to the to determine person "from. The question of the referring court does not refer to additional

information in the hands of the issue in the main process service provider. Nor is it to any third party who has these additional data (which, in combination with the dynamic IP address to determine the user), but the Internet access provider.

61. In this case is thus not necessary that the Court checks all agents that "reasonably" could put the defendant in the main proceedings, so that dynamic IP addresses at its disposal, to be categorized as personal data. That court refers only to additional knowledge in the hands of third parties, it follows that a) either the defendant does not have its own for determining the user's required additional knowledge or b) if it has access to derartigem knowledge, unable is it as a data controller in accordance with the 26th recital of Directive 95/46 reasonably be used for this purpose.

62. Both assumptions depend on findings of fact, is the exclusive responsibility of the national court. The Court could his general guidance on the interpretation of the phrase "means ... that ... might reasonably be used by the person responsible for processing ..." enter when the Federal Court had doubts as to whether the defendant could use their own additional knowledge reasonably. But since this is not the case, it would in my view misplaced, if the Court were now specify design criteria that are not essential for the national court and to which it has not even asked.

63. Thus, it comes in the question referred to the core question of whether it is for the qualification of dynamic IP addresses as personal data of importance that a very specific third party, namely the Internet access provider, has additional data associated with these addresses allow the identification of the user who has visited a certain website.

64. Again, we refer to the 26th recital of Directive 95/46. The formulation "means ... that reasonably ... *from a third party* could be used" (17) could be interpreted as meaning that it is sufficient that any third party can obtain additional data (which are connected to identify a person with a dynamic IP address can), so that such an address *eo ipso* is regarded as piece of personal data.

65. This widest possible interpretation would in practice mean that any kind of information would be classified as a piece of personal data, so inadequate they alone would be also be able to determine a user can. Never will exclude yourself with absolute certainty that there is not a third party who is in possession of additional information which may be connected to the information in question and thus allows to determine a person's identity.

66. The possibility that the development of technical means will facilitate in a more or less near future access to increasingly sophisticated instruments for the recovery and processing of data noticeably, justifies in my view the safeguards protected by those privacy in advance shall be. It has been taken to detect when determining the relevant legal categories within data protection sufficiently broad and flexible combined behavior to cover every conceivable case design can (18).

67. Nevertheless, I think that this - very legitimate incidentally - concern can not lead to make the wording of reflecting the intention of the legislator expressed unheeded, and that the systematic interpretation of recital 26 of Directive 95/46 on "means ... that reasonably ... *from a third party* could be used," limited.

68. As well as the 26th recital does not include any means that might use the data controller (in this case, the Internet service provider), but only those that "reasonably" could occur, is also assumed that the legislator on "third party" refers to which of, the data controller who wishes to gain possession of the necessary data for identification additional knowledge *also reasonably* could turn. That is not the case when the contact with them in fact would require a very high human and economic cost or when it would be convenient not prohibited feasible or legally. Otherwise, it is, as already pointed out, virtually impossible to distinguish between the different means, because always it is conceivable that there is a third party, so inaccessible it may be for the Internet service provider and who - now or in the future - relevant additional data features that can assist in identifying a user.

69. As I have already pointed out, is in the taken by the Bundesgerichtshof in relation to third parties by an Internet access provider. This is certainly the third party, is to think of the reasonably first, when it comes to whom the service provider can turn to in order to obtain the required additional data, if he wants most efficient, practical and immediately identify the user who with using dynamic IP address has accessed his website. So it's not a hypothetical, unknown and inaccessible to third parties, but one of the major players in the network of the Internet, which is known with certainty that he is in possession of the data required by the service provider to identify a user. Indeed, it is, as the referring court points out, that particular third party to whom the defendant in the main proceedings would turn to obtain the additional knowledge necessarily required of her.

70. The Internet access provider is typically the third party to which the 26th recital of Directive 95/46 refers and to the service providers could apply in the main proceedings "most sensible". However, it remains to be determined whether it is "reasonably" feasible or practicable to obtain the additional data that are owned by this third party.

71. According to the German Government of the Internet access provider shall not disclose information available to him - because they are personal data - not easily, but only in accordance with the statutory provisions on the processing of such data be made available (19).

72. This is undoubtedly true. This information may be used only if the laws on personal data are complied

with. Information can only be "reasonably" obtained when the conditions of access to this type of data are fulfilled. The first requirement is the legal possibility of their storage and disclosure to others. Of course, the Internet access provider is entitled to refuse to provide the relevant data, but the opposite is also possible. The very quite "reasonable" possibility of transmission of data makes the wording of recital 26 of Directive 95/46 from the dynamic IP address for the Internet service provider, a piece of personal data.

73. There is a possibility that *within the law* be implemented and therefore "reasonable" is. The reasonable access to which Directive 95/46 refers, must by definition be lawful (20). From this premise, of course, comes from the national court, as the German Government points out (21). Thus, the legally relevant access significantly reduce because only coming rightful into consideration. But as far as they are - so they limited in its practical application may be -, hire constitutes "reasonable means" within the meaning of Directive 95/46.

74. Consequently, I consider that the first of the questions submitted by the Bundesgerichtshof, as it has been formulated by him, is in the affirmative. The dynamic IP address for the Internet service provider because of the existence of a third party (the Internet provider), to whom he could turn reasonably to obtain other additional data, in combination with the IP address identifying a user, as person-related classify date.

75. The result of the reverse would result speaks for my proposed answer. If dynamic IP addresses would not be considered as personal data for the Internet service provider, this could save unlimited and anytime ask the Internet access provider to the additional data, to connect them with the IP address to identify the user. In that case, as well as the German Government admits (22), from a dynamic IP address piece of personal data when he scored the additional data suitable to identify the user without violating privacy policy.

76. It would then be a date whose storage would only have been possible, therefore, because it had not been considered up to this point as a piece of personal data for the Internet service provider. The legal characterization of the dynamic IP address as a piece of personal data would thus in the hands of the Internet service provider, because they depended on it that these were to decide at a later date, the address in conjunction with the additional information that he may have to obtain from a third party, to use to identify the user. In my view, however, the wording of Directive 95/46 crucial that - reasonably - "accessible" of the existence of a third party can be expected, which has the necessary resources to enable the identification of a person, and not that of the opportunity to consult those third parties, actually use it.

77. One might take the German Government also considers that the dynamic IP address is transformed first into a piece of personal data when the Internet access provider receives them. Then one would have to accept that these qualifications retroactively made in respect of the period for which the IP address, and therefore view this address as non-existent, if the period has been exceeded, in which they could have been saved if they from the beginning would have been classified as a piece of personal data. So you came to a conclusion that the spirit of the legislation on the protection of personal data contrary. The reason that a storage of such data is permitted only for a limited period, would be distorted if a property that is inherent in this information from the beginning, may unfold late effect: their potential - alone or in conjunction with other data - to serve to identify a natural person. For this purely practical reason, it makes more sense, the IP address of awarding this property from the outset.

78. Therefore, I come to a first result, alleging Art. 2, pt. A to Directive 95/46 is to be interpreted as an IP address, which stores a service provider in connection with the access to its website, for this a person-related represents date and where an Internet access provider has the additional knowledge required to identify the person concerned.

B - *Second question*

79. By the second question, the Bundesgerichtshof asks whether Article. 7 literally. F of Directive 95/46 precludes national legislation is that personal information of a user may be without his consent only collected and used, to the extent necessary to the to enable specific use of the tele medium by this user and account, whereas the purpose of ensuring the functioning of the tele medium, the use of these data can not be justified on the end of each user activity beyond.

80. Before an answer to this need for a clarification regarding the submitted by the Bundesgerichtshof information indicating that the disputed information is stored in order to ensure the operability of the issue in the main proceedings websites and compared these sites directed cyber attacks possibly being able to prosecute.

81. therefore arises in advance whether the processing of IP addresses, referred to by the order for reference, under the Art. 3, para. 2, first indent of Directive 95/46 provided exceptional falls (23).

1. Applicability of Directive 95/46 on the processing of the data at issue

82. It appears that the Federal Republic of Germany is in the main proceedings as a pure provider of internet services, d. H. A private individual (and therefore *sine imperio*). It follows that the processing of the issue here data is not in principle excluded from the scope of Directive 95/46.

83. In the words of the Court in Lindqvist (24) 2, first indent of Directive 95/46 actions listed in Art. 3 para. "Any event, activities of the State or of State authorities and have nothing to do with the scope of activity of individuals do "(25). As far as the processing of the data at issue is carried out by a manager who is a government agency while, but in fact acting like a private entity, Directive 95/46 application.

84. The referring court emphasizes that the main purpose, the German administration pursued with the

storage of dynamic IP addresses, which is "ensuring and maintaining the security and functionality of their telemedia"; in particular the promotion of "detection and prevention of frequently occurring, denial of service 'attacks, where the telecommunications infrastructure is paralyzed by targeted and coordinated floods single server with a variety of requests" (26). The storage of dynamic IP addresses for this purpose can equally be for anyone with an Internet site of some importance and implies directly or indirectly, the exercise of public authority, which is why Directive 95/46 can be applied without any particular difficulty in such storage.

85. The Bundesgerichtshof stresses, however, that the storage of dynamic IP addresses by those at issue in the main proceedings service providers also serve to prosecute the perpetrators of possible cyber attacks possibly criminal. Enough of this purpose to exclude the processing of data from the scope of Directive 95/46?

86. In my view, is if by "law enforcement" the exercise of the *penalizing authority* of the State is to be understood by the defendant in the main proceedings service provider, an "action of the State in areas of criminal law" before and thus the in Art. 3 para. 2 first indent of Directive 95/46 provided for exceptions.

87. In this case, in accordance with the Court's case in the Huber case, (27) comprises the processing of personal data by the service providers in the interests of safety and technical operation of their telemedia from the scope of Directive 95/46, while the processing of data for the purpose of activities of the State in areas of criminal law does not fall under the Directive.

88. would also, even if the Federal Republic of Germany is not in their capacity as a pure service provider without sovereign powers to law enforcement in the true sense and, like any private person limited to forward the disputed IP addresses of a public body for the purpose of prosecution, processing of dynamic IP addresses have a purpose that does not fall within the scope of Directive 95/46.

89. This follows from the case-law in Case Parliament / Council and Commission (28), in which stated the Court held that the fact that certain personal data of "private ... where [n] operator [n] for commercial purposes ... and [were t] to a third country over medium ", does not mean that this submission" does not fall within the scope "of Art. 3, para. 2, first indent of Directive 95/46, if the purpose of the transfer activities of the State in areas of criminal law the subject has, as long as they "[found] in a set up by government bodies and frames instead of ... public safety [is]" in the case in question (29).

90. In contrast, when, as in my opinion, the order can be found, with "law enforcement" the actions of a private individual is meant having the right to the state to exercise its *penalizing authority* invite by appropriate action, then you can not assume that processing of dynamic IP addresses has activities of the State in areas of criminal law and the subject is excluded from the scope of Directive 95/46.

91. In reality, storage and recording of this data then serve as a further evidence, which the owner of the website of the State may require the prosecution of unlawful conduct on request. It is a criminal agent in defense of rights that accord to individuals the legal system (in this case, a public body which is private). So considered, this procedure does not differ from the action of any other internet service provider, seeking state protection in accordance with the foreseen in the legal prosecutions.

92. As far as the German administration acts as Internet Service Provider without sovereign powers, what the referring court must decide, therefore, the distinction made by their processing of dynamic IP addresses is includes as personal data from the scope of Directive 95/46.

2. To answer the question

93. § 15 Abs. 1 TMG entitled only to the collection and use of personal data of a user, to the extent necessary to enable the actual implementation of a tele medium and settle. Specifically, the service provider may only the so-called "usage data" collect and use, d. H. The personal data of a user, which are necessary in order "to allow the utilization of telemedia and settle". These data must be erased as soon as the use process is completed (ie when the actual implementation of the tele medium is finished), unless they have according to § 15 Abs. 4 TMG be kept "for accounting purposes".

94. When the connection is completed, closes § 15 TMG it apparent from to store usage data for other reasons, not to ensure "the [general] use of tele-media". Since the provision of TMG refers only to accounting purposes as a justification for the retention of data, could they so understood (although its final interpretation the national court belongs) that it requires that the user data may be used only to enable a concrete connection and after its termination must be deleted.

95. Art. 7 literally. F of Directive 95/46 (30) allows the processing of personal data under conditions that are in focus (for the controller) in my opinion, more generous than the formulated in § 15 TMG. The German regulation may be referred to in this point as more restrictive than the European Union law, because they, in principle does not provide for the realization of another legitimate interest, which is not in connection with the billing of the service, although the Federal Republic of Germany as an Internet Service Provider also a legitimate interest might have to guarantee the functionality of their web pages about each usage case beyond (31).

96. The Court of Justice in accordance with its judgment ASNEF and FECEMD (32) provides the criteria for answering the second question. The Court there found that "results ... that Art. 7 of Directive 95/46, an exhaustive and final list of cases provided for, where a processing of personal data can be considered to be lawful" from the aim of Directive 95/46 (33). Accordingly, "Member States may neither new principles relating to the admissibility of the processing of personal data in addition to Art. 7 of Directive 95/46 to introduce, nor impose

additional conditions that would alter the scope of the six provided for in this Article principles" (34) ,

97. Although § 15 TMG provides no additional condition besides those which are provided for in Article 7 of Directive 95/46 on the legality of the processing of personal data -. As it was in Cases ASNEF and FECEMD the case (35) -, but it limits if you interpret it as restrictive as the national court, the condition in subparagraph f of the provision of content a. Where the EU legislature generally to the attainment of a "legitimate interest [relates] that of the data controller perceived or of the third party or parties to whom the data are disclosed ", considered to § 15 TMG solely the need to" [specify] use to enable a medium telephoto and settle ".

98. Just as in the ASNEF and FECEMD Case (36) also changed in this case a national measure - unless they, as I said, interpreted as restrictively as explained above - the scope of the principle of Article 7 of Directive 95/46. instead the provision merely to regulate in detail what is the only thing in which the authorities of the Member States in accordance with Art. 5 of Directive 95/46 have a degree of latitude.

99. . This Article 5 provides: 'Member States shall designate pursuant to this Chapter [(37)] more precisely the conditions under which the processing of personal data is lawful. "Nevertheless, may, as in Cases ASNEF and FECEMD (38) found , "provides that Member States by [that provision] no other principles relating to the admissibility of the processing of personal data than in Art. 7 of this Directive enumerated principles and not by additional conditions the scope of six provided for in this Art. 7 principles change".

100. § 15 TMG reduced compared to Art. 7 literally. F Directive 95/46 the scope of legitimate interest, which may justify the processing of data, significantly and regulates this interest in the context of Art. 5 of the Directive provided for authorization not only closer or accurate. He also does this categorically and absolutely, and does not allow that the protection and ensuring the general mobilization of the tele medium of art. 7 literally. F Directive 95/46 against "the interest for fundamental rights and freedoms of the data subject, in accordance with protected Article 1 paragraph 1 ", can be weighed.

101. Ultimately, the German legislature as well as in Cases ASNEF and FECEMD (39) "the result of balancing the conflicting rights and interests [of certain types of personal data] conclusion [prescribed], without leaving room for a result that due to special circumstances of the case would be different ", so that it is" no longer a qualifier for the purposes of [the] Art. 5 [of Directive 95/46 is] ".

102. In those circumstances, I consider that the Bundesgerichtshof is required to interpret the national legislation in accordance with Directive 95/46, which means: a) As regards the reasons that may justify the processing of so-called "usage data" may also the legitimate interest of the provider of telemedia are to ensure the general use of these media. b) This interest of the service provider can be weighed in individual cases against the interests or the fundamental rights and freedoms of the user, in order to clarify the interest according to Art. 1 para. 1 of Directive 95/46 is to protect (40).

103. For the manner how this balance of interests is carried out in the case referred to it is, in my opinion, nothing more to say. The Federal Court this presented no question, but worrying about the solution of this assessment made previous question, namely whether this assessment can be carried out.

104. Finally, I also note seems redundant, that the referring court may take into account any legislation that d of the Member State under the authorization pursuant to Art. 13 para. 1 literally. Directive adopted 95/46 which in Art. 6 may limit foreseen duties and rights, where this is necessary - in addition to other legal interests - to ensure "the prevention, investigation, detection and prosecution of criminal offenses". Also on this point the national court refers not related, although it is certainly known that there are these two articles.

105. Accordingly, I propose to answer the second question as meaning that Art. 7 literally. F Directive 95/46 interpreting a provision of national law precludes, after which a service provider is prevented from personal data without the user's consent on the end of each user activity to raise addition and process in order to ensure the functioning of the tele medium.

VI - Result

106. I therefore propose that the Court should answer the questions referred as follows:

rding to Art. 2, pt. A to 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 is a dynamic IP address through which a user has accessed the website of a telemedia provider, for the latter, a "piece of personal data", in so far as an Internet access provider has other additional data, in combination with the dynamic IP address identifying the user.

7 literally. F of Directive 95/46 must be interpreted as meaning that the purpose is to ensure the operability of the video medium, in principle, is to be regarded as a legitimate interest, the realization of which the processing of this personal date justify unless override him against the has been awarded interests or fundamental rights of the person concerned. National legislation which does not allow the inclusion of this legitimate interest is incompatible with that article.

---

riginal 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) contains, inter alia, the obligation for the purpose of investigation, detection and prosecution of serious offenses "date and time of logon and logoff the Internet access service, ... together with the Internet access provider to a communication assigned dynamic or static IP address and to store the user ID of the subscriber or registered user. "

3 - 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) Directive.

4 - judgment of 24 November 2011 (C-70/10 EU: C: 2011: 771, para. 51).

5 - See also the judgment of 19 April 2012, Bonnier Audio and Others.. (C-461/10 European Union. C: 2012: 219, paras 51 and 52).

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

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

8 - According to the Bundesgerichtshof is at the usage data to the characteristics to identify the user as well as information on the beginning, end and extent of usage and the utilized by the user telemedia.

9 - Judgment of 24 November 2011 (C-70/10 EU: C: 2011: 771, para. 51).

10 - This question was already by the Court in its judgments of 24 November 2011, Scarlet Extended (C-70/10, EU: C: 2011: 771, para. 51), and of 19 April 2012, Bonnier Audio and Others (C-461/10 EU: C: 2012: 219), decided. Add to Rn. 51 and 52 of that judgment, the Court held that the information "about the name and the address of an Internet subscriber or -nutzers ... that uses an IP address, were exchanged illegally from which probably files with protected works, [to] ... identify him [to] may [,] ... a processing of personal data within the meaning of Art. 2 para. 1 of Directive 2002/58 in conjunction with Art. 2 literally. b of Directive 95/46 ".

11 - For the two schools of thought see eg cry Bauer, M., in. *Comment on the Federal Data Protection Act. Nebengesetze* , Esser, M., Kramer, P., and von Lewinski, K. (ed.), Carl Heymann Verlag / Wolters Kluwer, Cologne, 2014, 4th ed., § 11 Telemediengesetz (4 to 10). Nink, J., and Pohle, J., "The identifiability of the person reference. From the IP address of the scope of data protection laws "in *Multimedia und Recht* , 9/2015, pp 563 to 567. Heidrich, J., and Wegener, C.," Legal and technical requirements for the logging of IT data. Problem case Logging ", in *Multimedia und Recht* , 8/2015, pp 487 to 492. Leisterer, H.," The new requirements for network and information security and the processing of personal data security ", in *Computer and Law* , 10/2015 , pp 665-670.

12 - Cited in # 13..

13 - Cited in # 11..

14 - Then Advocate General Cruz Villalón has in his Opinion in the Scarlet Extended (Case C-70/10 EU: C: 2011: 255, # 76)., Pointed, and it also provides the EDPS in its opinions of 22 February 2010 on the current negotiations of the European Union on an agreement to combat counterfeiting and piracy (anti-Counterfeiting Trade Agreement, ACTA) (OJ. 2010 C 147, p 1, para. 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 and sexual exploitation of children and child pornography, repealing framework Decision 2004/68 / JHA (OJ. 2010 C 323, p 6, Rn . 11).

15 - See to that effect of 20 May 2003, Österreichischer Rundfunk (C-465/00, C-138/01 and C-139/01, EU: C: 2003: 294, para. 68), and the. Opinion of Advocate General Kokott in Promusicae (C-275/06, EU: C: 2007:. 454, points 51 ff).

16 - Until proven otherwise is to suggest that it was this person who has surfed the Internet and accessed the website. Thus allowing, apart from this assumption, the information about the date, bringing the time and numerical origin of the access to a website that access to the owner of the device connected and indirectly to relate to his behavior in the network. A possible exception are IP addresses assigned to computers in rooms such as Internet cafes, which anonymous users can not be identified and the owner of the data traffic in these premises does not provide any relevant personal information. Incidentally, this is the only exception to the

principle that IP addresses are personal data, the (so-called "Article 29 Working Party") accepts the established by Directive 95/46 group for the protection of individuals with regard to the processing of personal data Has. Your Opinion 4/2007 of 20 June 2007 on the term "personal data", WP 136, takes on itself

17 - Emphasis added.

18 - based on these protective and preventive function, as I have said, the Article 29 Working Party its view that IP addresses in principle personal data are. Excluded is only the case that the service provider can say with absolute certainty that the IP addresses belonging to unidentified persons, as it could happen with the users of Internet cafes. See. Fn. 16 at the end.

19 - Rn. 40 and 45 of its written observations.

20 - In this context it does not matter that the access to the personal date *de facto* by a violation of the rules on data protection is possible.

21 - Rn. 47 and 48 of its written observations.

22 - Rn. 36 of its observations.

23 - Do not fall within the scope of Directive 95/46 "processing [personal] data ... concerning public security, defense, state security ... and the *activities of the State in areas of criminal law* " (emphasis added).

24 - Judgment of 6 November 2003 (C-101/01, EU: C: 2003: 596, para. 43).

25 - Similarly, they the judgment of 16 December 2008, Satakunnan Markkinapörssi and Satamedia (C-73/07, EU: C: 2008: 727, para. 41).

26 - Rn. 36 preliminary ruling.

27 - Judgment of 16 December 2008 (C-524/06, EU: C: 2008: 724, para. 45).

28 - Judgment of 30 May 2006 (C-317/04 and C-318/04, EU: C: 2006: 346, paras 54 to 59.).

29 - Ibid. (Para. 59). It was about personal data processed for the provision of services, which represented the activities of the relevant private operators (airlines) were not necessary, but the operator is of to their transfer to the US authorities for the purpose of preventing and combating terrorism saw committed.

30 -. In No. 17 reproduced.

31 -. See No. 84. The owner of the web pages certainly have a legitimate interest in that the national court refers "denial of service" attacks, ie massive attacks that coordinates occasionally made against individual websites to overloading them and to paralyze, to prevent and fight.

32 - Judgment of 24 November 2011 (C-468/10 and C-469/10 EU: C: 2011: 777).

33 - Ibid. (Para. 30).

34 - Ibid. (Para. 32).

35 -. In this case, the national legislature Attraction Directive had 7 literally f 95/46 supplemented by the condition that the data to be processed had to be included in public sources..

36 - Judgment of 24 November 2011 (C-468/10 and C-469/10 EU: C: 2011: 777).

37 - Chapter II ("General rules on the lawfulness of the processing of personal data"), consisting of Articles 5 to 21 of Directive 95/46..

38 - Judgment of 24 November 2011 (C-468/10 and C-469/10 EU: C: 2011: 777, para. 36).

39 - Judgment of 24 November 2011 (C-468/10 and C-469/10 EU: C: 2011: 777, para. 47).

40 - In the minutes of the meeting of the representatives of Mr. Breyer rejected the argument that the storage of dynamic IP addresses to protect the functioning of the Internet services from possible attacks is necessary. I do not think that can be solved for all cases abstract problem. The solution must rather be preceded in each case a comparison of the interest of the proprietor of the website and the rights and interests of users.