BREYER
Court of Justice of the European Union
Case C-582-14
Judgment of the Court of 19 October 2016

«Mr. Breyer has accessed several websites operated by German Federal institutions. On the websites, which are accessible to the public, those institutions provide topical information.

With the aim of preventing attacks and making it possible to prosecute 'pirates', most of those websites store information on all access operations in logfiles. The information retained in the logfiles after those sites have been accessed include the name of the web page or file 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.

IP addresses are series of digits assigned to networked computers to facilitate their communication over the internet. When a website is accessed, the IP address of the computer seeking access is communicated to the server on which the website consulted is stored. That connection is necessary so that the data accessed maybe transferred to the correct recipient.

Furthermore, it is clear from the order for the reference and the documents before the Court that internet service providers allocate to the computers of internet users either a 'static' IP address or a 'dynamic' IP address, that is to say an IP address which changes each time there is a new connection to the internet. Unlike static IP addresses, dynamic IP addresses do not enable a link to be established, through files accessible to the public, between a given computer and the physical connection to the network used by the internet service provider.

Mr. Breyer brought an action before the German administrative courts seeking an order restraining the Federal Republic of Germany from storing, or arranging for third parties to store, after consultation of the websites accessible to the public run by the German Federal institutions' online media services, the IP address of the applicant's host system except in so far as its storage is unnecessary in order to restore the availability of those media in the event of a fault occurring.

Since Mr. Breyer's action at first instance was dismissed, he brought an appeal against that decision.

The court of appeal varied that decision in part. It ordered the Federal Republic of Germany to refrain from storing or arranging for third parties to store, at the end of each consultation period, the IP address of the host system from which Mr. Breyer sought access, which was transmitted when he consulted publicly accessible websites of the German Federal institutions' online media, where that address is stored together with the date of the consultation period to which it

relates and where Mr. Breyer has revealed his identity during that use, including in the form of an electronic address mentioning his identity, except in so far as that storage is not necessary in order to restore the dissemination of those media in the event of a fault occurring.

According to the court of appeal, a dynamic IP address, together with the date on which the website was accessed to which that address relates constitutes, if the user of the website concerned has revealed his identity during that consultation period, personal data, because the operator of that website is able to identify the user by linking his name to his computer's IP address.

However, the court of appeal held that Mr. Breyer's action could not be upheld in other situations. If Mr. Breyer does not reveal his identity during a consultation period, only the internet service provider could connect the IP address to an identified subscriber. However, in the hands of the Federal Republic of Germany, in its capacity as provider of online media services, the IP address is not personal data, even in combination with the date of the consultation period to which it relates, because the user of the websites concerned is not identifiable by that Member State.

Mr. Breyer and the Federal Republic of Germany each brought an appeal on a point of law before the *Bundesgerichtshof* (Federal Court of Justice, Germany) against the decision of the appeal court. Mr. Breyer sought to have his application for an injunction upheld in its entirety. The Federal Republic of Germany sought to have it dismissed.

The referring court states that the dynamic IP addresses of Mr. Breyer's computer stored by the Federal Republic of Germany, acting in its capacity as an online media services provider, are, at least in the context of other data stored in daily files, specific data on Mr. Breyer's factual circumstances, given that they provide information relating to his use of certain websites or certain internet files on certain dates.

Nevertheless, the data stored does not enable Mr. Breyer to be directly identified. The operators of the websites at issue in the main proceedings can identify Mr. Breyer only if the information relating to his identity is communicated to them by his internet service provider. The classification of those data as 'personal data' thus depends on whether Mr. Breyer is identifiable.

The *Bundesgerichtshof* (Federal Court of Justice) refers to the academic disagreement relating to whether, in order to determine whether someone is identifiable, an 'objective' or 'relative' criterion must be used. The application of an 'objective' criterion would have the consequence that data such as the IP addresses at issue in the main proceedings may be regarded, at the end of the period of use of the websites at issue, as being personal data even if only a third party is able to determine the identity of the data subject, that third party being, in the present case, Mr. Breyer's internet service provider, which stored the additional data enabling his identification by means of those IP addresses.

According to a 'relative' criterion, such data may be regarded as personal data in relation to an entity such as Mr. Breyer's internet service provider because they allow the user to be precisely identified […], but not being regarded as such with respect to another entity, since that operator does not have, if Mr. Breyer has not disclosed his identity during the consultation of those websites, the information necessary to identify him without disproportionate effort.

If the dynamic IP addresses of Mr. Breyer's computer, together with the date of the relevant consultation period, were to be considered as constituting personal data, the referring court asks whether the storage of those IP addresses at the end of that consultation period is authorized by Article 7(f) of that directive.

In that connection, the *Bundesgerichtshof* (Federal Court of Justice) states, first, that […] online media services providers may collect and use the personal data of a user only to the extent that that is necessary to facilitate and charge for the use of those media. Second, the referring court states that, according to the Federal Republic of Germany, storage of those data is necessary to guarantee the security and continued proper functioning of the online media services that it makes accessible to the public, in particular, enabling cyber attacks known as 'denial-of-service' attacks, which aim to paralyze the functioning of the sites by the targeted and coordinated saturation of certain web servers with huge numbers of requests, to be identified and combated.

According to the referring court, if and to the extent it is necessary for the online media services provider to take measures to combat such attacks, those measures may be regarded as necessary to 'facilitate … the use of telemedia' […]. However, academic opinion mostly supports the view, first, that the collection and use of personal data relating to the user of a website is authorized only in order to facilitate the specific use of that website and, second, that those data must be deleted at the end of period of consultation concerned if they are not data required for billing purposes. Such a restrictive reading […] would prevent the storage of IP addresses from being authorized in order to guarantee in a general manner the security and continued proper functioning of online media.

[…] In those circumstances the *Bundesgerichtshof* (Federal Court of Justice) decided to stay the proceedings before it and to refer the following questions to the Court for a preliminary ruling:

'(1) Must [*data protection legislation*] … be interpreted as meaning that an internet protocol address (IP address) which an [online media] 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?