European Union court rules that IP addresses are personal data

The *Breyer* case, another landmark ruling on key data protection notions, covers the definition of personal data in relation to dynamic IP addresses and the "legitimate interest" legal basis for data processing. By **Monika Kuschewsky**.

The Court of Justice of the EU (CJEU) has yet again issued an important ruling, interpreting key notions of the EU Data Protection Directive (the Directive) in its recent judgement of 19 October 2016 in the Case Patrick Breyer vs. Bundesrepublik Deutschland (C-582/14). In particular, the CJEU answered two questions, namely: (1) whether dynamic IP addresses constitute personal data for website operators and (2) concerning the permissible scope of Member States' implementing legislation concerning the "legitimate interest" legal basis for data processing under Article 7 lit. f) of the Directive.

The ruling did not come as any great surprise to legal onlookers, as it largely followed the Attorney General's Opinion of 12 May 2016. It also reconfirmed the limits that national legislators need to respect when implementing the Directive, which the CJEU had established previously. Whilst providing important guidance, which will remain relevant under the forthcoming EU General Data Protection Regulation (the "GDPR"), the ruling raises certain questions, which may need to be answered in future cases.

Background

The questions, which were referred to the CJEU for interpretation, arose in court proceedings in Germany that were brought by Patrick Breyer, a German Pirate Party politician, against the German Federal Government. Breyer had challenged the government for its storage of his dynamic IP address, without his express consent, when he accessed the government's websites. The government stored those addresses to defend itself against denial-of-service and similar attacks on its websites and to allow the criminal prosecution of hackers.

Unlike static Internet Protocol (IP) addresses, dynamic IP addresses are only temporarily assigned and change each time there is a new connection from a computer or device to the Internet. Website operators (as opposed to Internet service providers, ISPs) do not usually possess all the information to identify the users behind the IP address.

Though initially dismissed by a lower court, the case was brought before Germany's highest civil court (the *Bundesgerichtshof* or BGH), which referred two questions for a preliminary ruling to the CJEU.

Dynamic IP addresses as personal data

In *Scarlet Extended SA vs. SABAM* (C-70/10) the CJEU had held that the IP addresses of Internet users were protected personal data because they allow those users to be precisely identified. However, in that case, the collection and identification of the IP addresses of Internet users was carried out by an Internet service provider (ISP) who holds the details that, if combined, can identify a particular user.

By contrast, the CJEU had not yet considered the case of a website operator, which does not hold these details, and dynamic IP addresses. In *Breyer*, the CJEU now found that dynamic IP addresses can constitute personal data within the meaning of the Directive, even if the website operator does not hold the details to identify the website user.

Starting from the definition of personal data in Article 2 lit. a of the Directive (which defines personal as "any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly …"), the CJEU considered that dynamic IP addresses do not directly reveal the identity of the natural person who owns the computer from which a website was accessed, or that of another person who might use that computer.

The CJEU then considered whether dynamic IP addresses may be treated as personal data relating to an "identifiable natural person", who can be identified indirectly. In interpreting this provision, the CJEU made two important statements:

- first, "it is not necessary that that information alone allows the data subject to be identified;" and,
- second, "it is not required that all the information enabling the identification of the data subject must be in the hands of one person."

Applying these criteria to the case at hand, the fact that the website operator itself does not have the additional data necessary to identify the user of a website does not exclude the qualification of a dynamic IP address as personal data. The question then is whether it is sufficient that a third party, here the ISP, holds the additional data to qualify the dynamic IP as personal data for the website operator. The CJEU does not think so. Rather, based on recital 26 of the Directive, it must be determined whether the possibility to combine a dynamic IP address with the additional data held by the ISP constitutes "a means likely reasonably to be used to identify the data subject."

The CJEU excludes this possibility in two cases, namely if the identification of the data subject was:

- prohibited by law; or
- practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant.

In its order for reference, the BGH suggested that, in particular in the event of cyberattacks, under German national law, the website operator can contact the competent law enforcement authority which can take steps to

obtain the additional data from the ISP and to bring criminal proceedings. In light of this, the CJEU concluded that it appears that the website operator has the means which may likely reasonably be used in order to identify the data subject, with the assistance of other persons, namely the competent authority and the ISP, on the basis of the IP addresses stored. The case has been referred back to the BGH which will issue its decision based on the CJEU's ruling, subject to verification of the German rules.

Member States have limited room for manoeuvre

The second question referred to the CJEU relates to a provision (section 15) of the German Telemedia Act (*Telemediengesetz* or TMG) which only allows the collection and use of usage data of users of information society services (such as websites), without their consent, to facilitate, and charge for, the specific use of the services by the user concerned. In the case at hand, Germany collected and used the personal data of visitors to its websites, without their consent, for the much broader purpose of ensuring the general operability of its services and of preventing cyber attacks beyond the specific use of the website.

The CJEU first briefly considered whether the processing of personal data at issue is excluded from the scope of the Directive under Article 3 (2). Pursuant to this Article, the Directive does not apply to processing operations concerning state activities in the area of criminal law. However, in the present case it appears that the German federal government acts like any other website operator in the private sector.

The CJEU then looked at the issue of whether a provision like section 15 of the TMG is in line with Article 7 lit. f of the Directive, which allows data processing if necessary for the purposes of the legitimate interests pursued by the controller or third party, subject to a balancing with the interests of the data subject.

In its response, the CJEU referred to its previous ruling in Joined Cases C-468/10 and C-469/10 *ASNEF and FECEMD*. In that case the CJEU had held that Member States can establish guidelines in respect of the balancing of interests, but cannot definitively prescribe the result of the balancing exercise, and thereby exclude the possibility of processing certain categories of personal data, without allowing a different result by virtue of the particular circumstances of an individual case.

In *Breyer*, the CJEU confirmed this previous ruling and held that Article 7 lit. f of the Directive precludes national legislation which allows website operators to collect and use a user's personal data only in limited circumstances, thus excluding the collection and use for the purpose of ensuring the general operability of those services.

The CJEU thereby also implicitly recognised that ensuring the general operability and prevention of cyberattacks can constitute a legitimate interest within the meaning of Article 7 lit. f of the Directive, which may justify the collection and use of personal data. The BGH will now have to assess whether Germany has carried out the balancing of interests properly.

Wider implications of the Breyer ruling

The ruling is relevant to all parties that collect and use IP addresses, including for website analytics or online advertising. This is because the definition of personal data in the GDPR is largely the same as under the Directive, although it specifically includes online identifiers by way of example. The ruling might even have ramifications outside the online world in the context of the use of pseudonymous data and anonymization.

Unfortunately, ambiguity still remains in the light of the CJEU's ruling in the *Breyer* case. It is noteworthy that the CJEU seems to have looked primarily at the ability of a competent authority to obtain the additional data to identify website users rather than the ability of the website operator itself. In fact, the CJEU was told by the BGH that German law does not allow the Internet service provider to transmit directly to the online media services provider the additional data necessary for the identification of the data subject.

The CJEU did not go as far as to suggest that it would be sufficient that any third party worldwide can identify the data subject. However, as long as the mere possibility that a third party (such as a competent authority) as opposed to the website operator himself may obtain the additional information required for identification suffices, it can be questioned to what extent:

- the criterion of "means which may likely reasonably be used" really effectively limits the scope of what constitutes personal data; and
- how website operators can ever be certain that no third party can obtain the additional information.

The CJEU specifically referred to possible legal avenues under German law in the particular event of a cyber attack. As a result, it seems possible that the outcome (and hence the qualification of the same type of information) can be different in other Member States, depending on the available legal avenues under the respective national law, or in other circumstances (e.g. other types of violations). The CJEU only explicitly ruled out two cases in which the information does not qualify as personal data, namely, where the identification is prohibited by law or where it is practically impossible. However, it is unclear whether this test will be met if (only) the law of the country in which the website operator is established prohibits the identification. Or do website operators potentially have to assess the possible legal avenues of third parties (including competent authorities) under the national laws of other EU Member States or even third countries, too? It is also unclear what it would take to meet the threshold of a disproportionate amount of time, money or workforce.

In light of the objective of the GDPR to achieve harmonisation, it is in any event rather concerning that the CJEU has linked the definition of personal data to judicial remedies that are or are not available under national law, which risks undermining that objective.

The CJEU ruling has an immediate impact on section 15 (3) of the TMG, which is one of the strictest provisions to date dealing with profiling in the EU. This provision can no longer be applied as it is contrary to EU law. It now remains to be seen whether the German government will try to adopt a revised version of section 15 TMG in line with the

Directive or the GDPR.

However, more generally, the Breyer ruling serves as a timely reminder of the limited room for manoeuvre that national legislators have when implementing the Directive, in particular the legal bases in Article 7. This has implications far beyond section 15 (3) of the TMG. In fact, sector-specific legislation in Germany in many cases contains provisions which set out and limit the circumstances in which personal data may be collected, processed and used in specific scenarios. All these provisions should be put under scrutiny in light of the *Breyer* ruling, and the legislators in Germany, but also in other Member States, will need to pay close attention to these limits when implementing the GDPR.

AUTHOR

Monika Kuschewsky is a Partner at Squire Patton Boggs (UK) in Brussels.
Email: monika.kuschewsky@squirepb.com
www.squirepattonboggs.com

