CJEU: German Rules on Data Retention Not in Line with EU Law

Thomas Wahl

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

On 20 September 2022, the CJEU (Grand Chamber) ruled that the German legislation on data retention is incompatible with EU law (Joined Cases C-793/19 and C-794/19, *SpaceNet and Telekom Deutschland*). The regulation provided for the indiscriminate, ten-week storage of telephone and internet connection data as well as a four-week storage of location data and has been on hold since 2017.

AUTHOR

Thomas Wahl
Senior Researcher
Max Planck Institute for the Study of Crime, Security and Law

Published in
2022, Vol. 17(3) eucrim pp 188 – 189
ISSN: 1862-6947
https://eucrim.eu

The reference for a preliminary ruling

The referring German Federal Administrative Court (Bundesverwaltungsgericht - BVerwG) doubted the incompatibility of the German rules on the basis of the CJEU's previous case law on data retention, because the retention obligation in the German Telecommunications Act (TKG) concerns fewer data and a shorter retention period (→ eucrim 3/2019, 176). In the referring court's view, those characteristics reduce the possibility that the retained data may allow to draw very precise conclusions on the private life of a person whose data have been retained. In addition, the BVerwG believed that the TKG ensures the effective protection of retained data against risks of abuse and unlawful process.

The CJEU's decision

The CJEU counters these arguments and referred to its established case law on the retention of and access to personal data in the electronic communications sector, in particular the most recent judgments in *La Quadrature du Net and Others* of October 2020 (→ eucrim 3/2020, 184-186) and *G.D. v Commissioner of An Garda Síochána* of April 2022 (→ eucrim 2/2022, 115). The CJEU particularly reiterated its line of argument that EU law (Art. 15(1) of Directive 2002/58/EC, read in light with Arts. 7, 8 and 11 and Art. 52(1) CFR) precludes national legislative measures which provide, on a preventive basis, for the purposes of combating serious crime and preventing serious threats to public security, for the general and indiscriminate retention of traffic and location data.

The CJEU's reasoning

First, the CJEU noted that the retention obligation laid down in the TKG applies to an extensive set of data, which corresponds, in essence, to those which led to the previous judgments (in particular *La Quadrature du Net and Others*), and which is indiscriminate as to persons, time and geography. Thus, the data retention obligation such as that at issue cannot therefore be regarded as targeted data retention.

Second, the CJEU stated that, in view of the quantity and diversity of the data retained, the storage period of 4 or 10 weeks cannot discard the possibility to draw very precise conclusions about the private life of the person or persons whose data have been retained and, in particular, make it possible to establish a profile of the person or persons concerned. Consequently, the retention of traffic or location data is serious in any event, irrespective of the length of the retention period and of the amount or nature of the data retained, provided that the set of data retained is capable of giving rise to such inferences.

Third, as regards the safeguards intended to protect the data stored against risks of misuse and against any unauthorised access, the CJEU called to mind that the retention of data and access to them constitute separate interferences with the fundamental rights of the data subjects which require separate justification. It follows that national legislation ensuring full respect for the conditions established by the case law interpreting Directive 2002/58 as regards access to retained data cannot, by its very nature, be capable of either limiting or even remedying the serious interference with the rights of the persons concerned which results from the general retention of those data.

The exceptions

However, the CJEU stressed that, in line with its previous case law, national legislation can provide for a data retention regime in the following situations:

- General and indiscriminate retention of traffic and location data if the Member State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable;
- A limited targeted retention of traffic and location data for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security;
- General and indiscriminate retention of IP addresses for a limited period in time and limited to what is strictly necessary (for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security);
- General and indiscriminate retention of data relating to the civil identity of users of electronic communications (for the purposes of safeguarding national security, combating serious crime and safeguarding public security);
- Expedited retention of traffic and location data in the possession of service providers on the basis of an instruction by a competent authority (that is subject to effective judicial review) and for a specific period of time (for the purposes of combating serious crime and, a fortiori, safeguarding national security).

However, all the aforementioned legal measures must ensure, by means of clear and precise rules, that the retention of data at issue complies with the substantive and procedural conditions applicable to it and that the persons concerned have effective safeguards to protect them against the risk of abuse. These different legal provisions may be applied together, at the choice of the national legislator and within the limits of what is absolutely necessary.

Put in focus

Taking into account the CJEU's previous case law on data retention, the verdict for Germany have already become apparent (→ *Gerhold*, Verfassungsblog). In the end, the CJEU shared the opinion by Advocate General *Campos Sánchez-Bordona,* which was submitted in November 2021 (→ eucrim 4/2021, 222-223) and which already clearly stated the incompatibility of the German data retention regulation with EU law. The CJEU provides, however, for a legal framework, which would give Member States leeway to regulate certain forms of data retention for the purposes of safeguarding national security and combating serious crime.

The future of data retention in Germany is open. Germany's Federal Minister of the Interior, *Nancy Faeser*, announced after the judgment that she wishes to use the leeway given by the CJEU and to especially provide rules on the retention of IP addresses for the purposes of combating and preventing crime. By contrast, Federal Minister of Justice, *Marco Buschmann*, advocates for the "quick freeze" model. Accordingly, law enforcement officers would be allowed to have communications data "frozen" if there is suspicion of a respective serious criminal offence and a judge authorised the freeze. Thus, the imminent deletion of the data is prevented when an offence was committed. The judicial emergency order could also be issued without naming a specific person and refer, for example, to connection data at a specific crime scene and its surroundings. If the suspicion becomes concrete, law enforcement officers can then "unfreeze" the secured data and use it for their work.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union