CJEU Clarifies Exceptions to Data Retention in Irish Case

Thomas Wahl

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

AUTHOR

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

Published in
2022, Vol. 17(2) eucrim p 115
ISSN: 1862-6947
https://eucrim.eu

On 5 April 2022, the CJEU added another chapter to the long history of the admissibility of data retention in the EU. In Case C-140/20 (*G.D. v The Commissioner of An Garda Síochána*), the CJEU confirmed its established case law that general and indiscriminate retention of traffic and location data relating to electronic communication is contrary to Union law even if it intends to combat serious crime. In the Irish case at issue, a convicted murderer contested the use of evidence in the form of his traffic and location data in criminal proceedings and proceeded against the Irish provisions on data retention (for the AG's opinion → eucrim 4/2021, 222-223).

The CJEU's main arguments

The CJEU again stressed that the national legislature must comply with the principle of proportionality (in the narrower sense) and strike a balance between the various rights and interests in question. As a result, the Court rejected the submission that particularly serious crime, such as murder, could be treated in the same way as a threat to national security which is genuine and current or foreseeable and could, for a limited period of time, justify a measure for the general and indiscriminate retention of traffic and location data (→ CJEU in *Privacy International* and *La Quadrature du Net*, eucrim 3/2020, 184-186).

The CJEU, however, specified the limits of the fundamental ban on data retention. As indicated in previous case law, the following categories of measures are permissible, in order to combat serious crime and to prevent serious threats to public security:

- Targeted retention of traffic and location data on the basis of categories of persons concerned or by means of a geographical criterion;
- General and indiscriminate retention of IP addresses assigned to the source of an internet connection;
- General and indiscriminate retention of data relating to the civil identity of users of electronic communication systems;
- The quick freeze of traffic and location data in the possession of service providers.

Therefore, it is in line with Union law, for instance, to use data retention measures for combating serious crime in areas with a high average crime rate or strategic places, e.g. airports, stations, maritime ports or tollbooth areas. It will also not be queried if expedited retention is ordered from the moment when authorities commence an investigation into a possible serious crime. Such measure could even be extended to persons other than those who are suspected or having planned or committed a serious criminal offence, provided that such data can – on the basis of objective and non-discriminatory factors – shed light on such an offence or acts.

Put in focus:

The specified catalogue of exceptions will further fuel the debate on national regulations or even a new European regulation on data retention. NGOs still warn of the dangers of data retention for the fundamental rights of those affected. Meanwhile, further relevant proceedings are pending before the CJEU. The judges in Luxembourg have to decide, among others, on the cases C-793/19 and C-793/19 (*SpaceNet and Telekom Deutschland*) regarding the admissibility of the German regulation on data retention and cases C-339/20 and C-397/20 (*VD and SR*)seeking clarification on a French approach to data retention for investigations in the financial market (→ eucrim 4/2021, 222-223).

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