# CJEU Confirms Strict Limitations of Data Retention

**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
2021, Vol. 16(1) eucrim pp 28 – 30
ISSN: 1862-6947
https://eucrim.eu

In its judgment of 2 March 2021 on the Estonian rules on data retention (Case C-746/18), the CJEU (sitting in for the Grand Chamber) confirmed red lines for access to traffic and location data for law enforcement purposes. In a criminal case that concerned theft, fraud, and violence against persons party to court proceedings, the Estonian criminal courts essentially relied on reports drawn up on the basis of the data obtained from the provider of electronic communications services. In particular, the data provided information on who the accused communicated with, how, when, for how long and from where to where during a certain period of time. In addition, the case questioned which competent authority can grant access to such data.

## Questions referred

The Estonian Supreme Court basically posed two questions to the CJEU:

- Are national data retention regimes admissible in accordance with Art. 15(1) of Directive 2002/58/EC on privacy and electronic communications, read in the light of Arts. 7, 8, 11, and 52(1) CFR, even if they are not confined to the prevention, detection and prosecution of serious crimes, but to the duration of access and the quantity and nature of the data available in respect of such period is limited?
- Can the Estonian public prosecutor's office, in the light of the various duties which are assigned to it by national legislation, be regarded as an "independent" administrative authority (within the meaning of the CJEU's judgment in *Tele2 Sverige and Watson*), that is capable of authorising access for the investigating authority to the data concerned?

For details on the facts of the case and the AG's opinion → eucrim 1/2020, 23-24.

## Findings of the CJEU on the first question

The CJEU recalled the content of its recent ruling on data retention in *La Quadrature du Net and Others* (→ eucrim 2/2020, 3/2020, 184-186):

- Access by public authorities is possible only in so far as traffic and location data have been retained by a provider in a manner that is consistent with Art. 15(1) of Directive 2002/58;
- Legislative measures are precluded that, for law enforcement purposes, provide, as a preventive measure, for the general and indiscriminate retention of traffic and location data;
- Limitations on the rights and obligations laid down in Arts. 5, 6, and 9 of Directive 2002/58 must be assessed by measuring the seriousness of the interference entailed by such a limitation and by

verifying that the importance of the public interest objective pursued by that limitation is proportionate to the seriousness of the interference;
- A public authority's access to a set of traffic or location data that are liable to provide information regarding the communications made by a user of a means of electronic communication or regarding the location of the terminal equipment which he or she uses (and thus allow precise conclusions to be drawn concerning the private lives of persons concerned), is in any event a serious interference with the fundamental rights enshrined in Arts. 7 and 8 CFR;
- Accordingly, only the objectives of combating *serious* crime or preventing *serious* threats to public security are capable of justifying the interference.

Against this background, other factors relating to the proportionality of a request for access, such as the length of the period in respect of which access to the data is sought and the quantity or nature of the data available cannot play a role. Therefore, these factors cannot have the effect that the objective of preventing, investigating, detecting, and prosecuting criminal offences in general is capable of justifying such access.

The CJEU also provided guidance concerning when contraventions of the requirements of EU law may lead to an exclusion of evidence obtained in criminal proceedings. In the view of the judges in Luxembourg, the yardstick is the risk of breach of the adversarial principle, and therefore, of the right to a fair trial entailed by the admissibility of such evidence. To this end, national courts must disregard information/evidence obtained via access to traffic and location data in breach of EU law if the suspects "are not in a position to comment effectively on that information[/]evidence and they pertain to a field of which the judges have no knowledge and are likely to have a preponderant influence on the findings of fact."

### Findings of the CJEU on the second question

The CJEU called to mind its previous case law as regards the substantive and procedural requirements for national legislation under which competent authorities can be granted access to the data in question. This entails that observance of the requirements are subject to a prior review that is either carried out by a court or by an independent administrative body. Since the court or body must reconcile the various interests and rights at issue, the status must be so that they act objectively and impartially and be free from any external influence. In the criminal law field, the requirement of independence implies that the authority entrusted with prior review, first, must not be involved in the conduct of the criminal investigation in question and, second, has a neutral stance vis-à-vis the parties to the criminal proceedings. That is not the case with a public prosecutor's office, like the Estonian public prosecution's office, because it directs the investigation procedure and brings the public prosecution before the court that has jurisdiction. This conclusion is not changed by the consideration that the public prosecutor's office is mandated to verify both the incriminating and exculpatory evidence, to guarantee the lawfulness of the pre-trial prosecution, and to act exclusively according to the law.

### Put in focus

Through its judgment on the Estonian case, the judges in Luxembourg reaffirmed that Union law does not lead to the general ban of data retention. However, they repeatedly stressed that data retention regimes can only be compatible with Union law if access to traffic and location data that allow precise conclusions concerning persons' private lives is limited to the investigation/prosecution of serious crimes or the prevention of serious threats to public security. Substantive and procedural law must regulate access to what is "strictly necessary." Hence, it remains to be seen whether the German data retention regime, which is currently still under scrutiny in Luxembourg (→ eucrim 3/2019, 176), is compatible with the CJEU's guidelines, since it is actually restricted to a catalogue of serious criminal offences and includes further access limitations in respect of the principle of proportionality.

## 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**