ECJ: Requirements for Access to Telephone Connection Data for the Purpose of Identifying Offenders

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

Thomas Wahl

In its judgment of 30 April 2024, the ECJ clarified under which conditions law enforcement authorities can have access to a set of traffic and location data in the context of criminal investigations. The ECJ held that, in principle, the Italian legislation implementing a certain level of punishment of the offence for which access is sought compatible with Union law.

AUTHOR

Thomas Wahl

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

Published in
2024, Vol. 19(2) eucrim
ISSN: 1862-6947
https://eucrim.eu

Facts of the case and question referred

In the case at issue (Case C-178/22, *Procura della Repubblica presso il Tribunale di Bolzano*), the judge in charge of preliminary investigations at the District Court, Bolzano, Italy, objected a request by the public prosecutor who had sought judicial authorisation to obtain the records of stolen telephones from all the telephone companies in order to identify the thieves. The public prosecutor qualified the criminal investigations as "aggravated theft" and pointed to the Italian legislation (Article 132(3) of the Legislative Decree No 196, establishing the Personal Data Protection Code) which, *inter alia*, would allow access to all data concerning the telephone conversations and communications and the connections made with those telephones if law prescribes the penalty for the offence under investigation with a maximum term of imprisonment of at least three years.

The judge at the District court (the referring court) argued that the Italian legislation would allow law enforcement access to personal data for offences which cause only a limited social disturbance, such as low-value thefts like mobile phones or bicycles. In addition, Italian courts have no margin of discretion to assess the actual seriousness of the offence concerned and cannot refuse authorisation under this aspect.

Hence, the referring court doubted compatibility of the Italian legislation with Art. 15(1) of Directive 2002/58/EC, read in the light of the Charter of Fundamental Rights of the European Union, and as interpreted by the ECJ case law. This case law only allows exceptions from the obligation to ensure confidentiality of electronic communications under narrow conditions.

The ECJ's decision: "Seriousness" of interference affirmed

The ECJ, sitting in for the Grand Chamber, held first that the interference with the fundamental rights to privacy and the protection of personal data (Arts. 7, 8 of the Charter), caused by access to telephone records, is likely to be classified as serious. In this context, neither the short periods for data collection as requested by the public prosecutor (for less than two months) nor the fact that the requests targeted not the owner of the mobile phones but the assumed offenders are relevant to come to an opposite assessment.

Justification: Requirements for national law on access to retained data

Consequently, such access can be justified only by the objectives of combating serious crime or preventing serious threats to public security (in accordance with previous case law).

The ECJ clarified that it is for the Member States to define "serious offence" for the purpose of applying the exceptions allowed by the EU Directive. Criminal legislation falls within the competence of the Member States in so far as the EU has not legislated in that field.

However, Art. 15(1) of Directive 2002/58 in connection with Arts. 7, 8 and 11 and Art. 52(1) of the Charter sets limits for the Member State's discretion for definitions. In material terms, these limits are:

- The definition given in national law cannot be so broad that access to data (allowing precise conclusions to be drawn concerning the private lives of the persons concerned) becomes the rule rather than the exception;
- The Member State's measure must comply with the general principles of EU law, which include the principle of proportionality, and ensure the fundamental rights of respect for private life and protection of personal data.

In procedural terms, the ECJ requires:

- A court or an independent administrative body must be able to prior review that there is no distortion of the concept of "serious offence".

Conclusions for the "Italian" case

With regard to the concrete rules of the Italian legislation, the ECJ observed that it makes access to traffic and location data subject to the twofold condition that there must be "sufficient evidence of the commission of an offence" and that those data be "relevant to establishing the facts". Furthermore, the condition that access to data by law enforcement authorities may be granted for offences for which the maximum term of imprisonment is at least equal to a period determined by law is an objective criterium that defines the circumstances and conditions. Given the concrete requirements of the Italian law, in particular the minimum period fixed by reference to a maximum term of imprisonment of three years, do not set the "seriousness of the offence" to an excessive low level and does not appear to be disproportional.

However, the court or independent administrative body, acting in the context of a prior review carried out following a reasoned request for access, must be entitled to refuse or restrict that access where it finds that the interference with fundamental rights which such access would constitute is serious even though it is clear that the offence at issue does not actually constitute serious crime. Only such a review enables to strike a fair balance between, on the one hand, the legitimate interests relating to the needs of the investigation in the context of combating crime and, on the other hand, the fundamental rights to privacy and protection of personal data of the persons whose data are concerned by the access. It is finally for the Italian court to determine whether the Italian legislation complies with these requirements.

Put in focus

The judgment of 30 April 2024 further develops the ECJ's case law on law enforcement access to retained data. It clarifies two aspects of the judgment in Prokuratuur: the concept of "serious crime" and the scope of the prior review that a court must carry out under a provision of national law that requires it to authorise access to data retained by providers of electronic communications services. In Prokuratuur (Case C-746/18 → eucrim 1/2021, 28-30), the ECJ held that access to data that enables precise conclusions to be drawn

concerning a user's private life, pursuant to measures adopted under Art. 15(1) of Directive 2002/58, constitutes a serious interference with the fundamental rights and principles enshrined in Arts. 7, 8 and 11 and Art. 52(1) of the Charter. Such access may not be authorised for the purposes of the prevention, investigation, detection and prosecution of "criminal offences in general". It may be granted only in procedures and proceedings to combat "serious crime" and must be the subject of a prior review by a court or independent administrative body in order to ensure compliance with that requirement.

Under the new case law, the ECJ limits the Member States' discretion to define the "seriousness" of the offence for which access to retained telecommunications data is allowed to a minimum. Protection is rather to be assured by prior court review. However, this review is more or less seen as a control against abuse ("ascertain that there is no distortion of the concept of serious offence").

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