CJEU Backs Police Access to Retained Data in Minor Offences

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
2018, Vol. 13(3) eucrim pp 155 – 157
ISSN: 1862-6947
https://eucrim.eu

On 2 October 2018, the CJEU delivered another important judgment on data protection and on access by public authorities to retained provider data. The CJEU ruled on the Case C-207/16 (*Ministerio Fiscal*), which was presented together with the Opinion of the Advocate General (AG) in eucrim 1/2018, pp. 21-23.

The CJEU followed the AG's opinion and concluded that law enforcement authorities can also access personal data retained by providers of electronic communications in cases of criminal offences that are not particularly serious. It is a pre-condition, however, that access does not constitute a serous infringement of privacy.

I. Facts of the Case and Legal Questions

The case at issue concerned a request by Spanish police authorities to obtain information on communication data in order to identify the owners/users of SIM cards that were allegedly activated by means of a stolen mobile phone. As part of their investigations of the robbery of the mobile phone and a wallet, they asked various telephone operators to release names, telephone numbers; and addresses of persons who used the mobile phone to activate SIM cards. The Spanish Public Prosecutor's Office (*Ministerio Fiscal*) appealed against the decision of the investigative judge who denied the request for access to said data. The judge believed that the acts giving rise to the criminal investigation in question are not serious enough to justify the collection of data under Spanish law.

The appeal court (*Audiencia Provincial de Tarragona*) sought guidance from the CJEU on whether EU law fixes a certain threshold for the seriousness of offences, above which interference with the individuals' fundamental rights of privacy and of protection of personal data through the access of competent authorities to personal data retained by service providers may be justified.

The request for a preliminary ruling particularly concerned the interpretation of Art. 15(1) of Directive 2002/58/EC as amended by Directive 2009/136/EC – in short, the Directive on privacy and electronic communications. It allows Member States to restrict citizens' rights when such a restriction constitutes a necessary, appropriate, and proportionate measure within a democratic society in order to safeguard national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system.

II. Admissibility of the Request

First, the CJEU had to deal with an objection by the Spanish government that questioned the jurisdiction of the Court. The Spanish government argued that access to telecommunication data is part of national

authorities' exercise of *jus puniendi*. This, however, constitutes activity on the part of the State in areas of criminal law, which makes EC Directives regulating data protection or retention inapplicable in accordance with Art. 1(3) of Directive 2002/58 or Art. 3(2) of Directive 95/46.

The CJEU stated that provisions limiting the scope of said EC Directives only mention activities of the State or of State authorities unrelated to fields in which individuals are active. The Directives also, however, cover legislative measures that govern the activities of providers of electronic communications services. By referring to *Tele2 Sverige and Watson and others* (see eucrim 4/2016, p. 164), the CJEU set forth that the activities of service providers are also affected if legislative measures relate to access of national authorities to data retained by those providers. As a result, it is irrelevant – in contrast to the remarks of the Spanish Government – that the request for access was made in connection with a criminal investigation. It is also irrelevant that the access at issue "only" relates to data in connection with SIM cards. In sum, the CJEU held the request for a preliminary ruling admissible.

III. Reasoning in Substance

The CJEU gave the following arguments to substantiate its findings:

- National authorities' access to personal data retained by providers of electronic communications services constitutes an interference with the fundamental right of respect for private life (Art. 7 CFR). It is irrelevant whether the interference is defined as "serious," the information in question is sensitive, or the persons concerned have been inconvenienced in any way;
- Such access also constitutes interference with the fundamental right to the protection of personal data (guaranteed by Art. 8 CFR), as it constitutes processing of personal data;
- The list of objectives in the directive capable of justifying national legislation governing public authorities' access to such data and thereby derogating from the principle of confidentiality of electronic communications is exhaustive. This means that access must correspond, genuinely and strictly, to one of these objectives.
- As regards the objective of preventing, investigating, detecting, and prosecuting criminal offences, the wording of the directive does not limit that objective to the fight against serious crime alone, but refers to "criminal offences" in general;
- Within the framework of proportionality, the CJEU, in its judgment in *Tele2Sverige/Watson*, defined that the objective of fighting serious crime may justify public authorities' access to personal data retained by electronic service providers if, taken as a whole, the data allow precise conclusions to be drawn about the private lives of the persons. This means that if the interference is serious, it can be justified in that field only by the objective of fighting "serious" crime;
- By contrast, when the interference is not serious, such access is capable of being justified by the objective of preventing, investigating, detecting, and prosecuting "criminal offences" generally;
- In the present case, access to the data concerned cannot be defined as "serious interference," because these data – being cross-referenced with data pertaining to communication with SIM cards and location data – do not make it possible to ascertain the date, time, duration, and recipients of the communications undertaken with the SIM cards. They also do not make it possible to ascertain the locations where these communications took place or the frequency of these communications with specific people during a given period. These data do not therefore allow precise conclusions to be drawn concerning the private lives of the persons whose data is concerned;
- Hence, access to data – as in the case at issue – is legal (under the Directive on privacy and electronic communications), even though it concerns a minor offence (here: robbery of mobile phone).

IV. On Focus

The judgment in the present case (*Minsterio Fiscal*) is an important clarification in the field of data retention. The CJEU drew the line more precisely between admissible and inadmissible law enforcement access to data retained initially for commercial purposes by private providers of electronic communications services. It set a counterpoint to its landmark decision on national data retention regimes in *Tele2 Sverige/Watson*.

The CJEU clarified that there is a correlation between the level of seriousness of interference and the seriousness of crimes to be fought against. This is deducted from the principle of proportionality. In other words: if police seek sound revelations of the persons' communications, the criminal offence involved must be a serious one.

In this way, the CJEU avoided deciding on the Spanish appeal court's initial question, i.e. how the judges in Luxembourg would concretely define the "seriousness" of a criminal offence. The AG added statements in this regard at the end of his opinion. Nonetheless, the matter may be subject to subsequent references for a preliminary ruling.

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