AG: Minor Offences Can also Justify Police Access to Retained Data

Thomas Wahl

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

On 3 May 2018, Advocate General (AG) *Henrik Saugmandsgaard Øe* delivered a notable opinion on the scope of data protection in criminal law enforcement situations. According to the AG, Union law does not preclude investigative measures by which national authorities seek identification data from certain mobile phones held by electronic communication service providers, even if the criminal offense is not of a serious nature. The reference for the case is C-207/16 (*Ministerio Fiscal*).

AUTHOR

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

ISSN: 1862-6947
https://eucrim.eu

The case relates to the interpretation of Art. 15(1) of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communication sector. According to Art. 15(1), Member States may restrict the scope of certain rights and obligations laid down in the Data Protection Directive 95/46 if such restrictions constitute a necessary, appropriate, and proportionate measure in a democratic society to safeguard [*inter alia*] the investigation, detection, and prosecution of criminal offences.

The case is seen in the light of the CJEU's previous case law on data protection, in particular regarding its judgments in C-293/12 and C-594/12 ("*Digital Rights Ireland*") and C-203/15 and C-698/15 ("*Tele2 Sverige*"). The question arose as to whether the exception made by secondary Union law allowing access to retained data is restricted to "serious" criminal offenses only, in order to be compatible with the fundamental rights guaranteed in Art. 7 and 8 GRC, i.e., the right to respect private and family life and the right to protection of personal data. As a consequence, another question emerged, i.e., how the seriousness of crime must be determined, so that an interference into said fundamental rights can be justified.

These questions were posed in an action before the Provincial Court, Tarragona/Spain, where an appeal was brought against a previous judicial decision that denied police authorities the possibility to obtain communication data held by mobile phone operators. In the case at issue, Spanish police were investigating the robbery of a wallet and a mobile phone and therefore wanted various telephone operators to release telephone numbers that had been activated within a certain time period (approx. 12 days) after the robbery as well as the personal data of the owners/users of these telephone numbers corresponding to the SIM cards activated. The court of preliminary investigation refused this request on the grounds that Spanish law limits the communication of the data retained by the telephone operators to serious offences only, i.e., offences punishable by a term of imprisonment of more than 5 years.

Upon appeal by the Ministerio Fiscal (Spanish Public Prosecutor's Office), the Provincial Court of Tarragona referred the following two questions to the CJEU:

- Can the sufficient seriousness of the offences, as a criterion which justifies interference with the fundamental rights recognized in Art. 7/8 GRC, be determined by taking into account only the sentence that may be imposed in respect of the offence investigated, or is it necessary to identify in the criminal conduct particular levels of harm to individual and/or collective legally-protected interests?
- If the CJEU follows the first alternative, what should be the minimum threshold? Would it be compatible with a general provision setting a minimum of 3 years of imprisonment (corresponding to the present Spanish law that came into force after the decision of the court of preliminary investigation)?

First, the AG confirms the admissibility of the reference for a preliminary ruling. He considers Directive 2002/58 applicable in the present case, since the CJEU in *Tele2* confirmed that national legislation relating to the retention of data for the purpose of combating crime falls within the scope of that directive. In addition, the Directive encompasses situations such as those at issue, even if the data to be collected only refer to the users' "identity" and not to "location" or "communication" as such.

Secondly, as regards the *res materiae*, the AG recommends that the CJEU not directly answer the first question but instead reformulate it. In the AG's opinion, the concept of the "seriousness" of criminal offences had been developed by the CJEU in the cases *Digital Rights* and *Tele2* to address other situations than those dominating the case at issue. He clarifies that, from the previous CJEU's case law, a link can be discerned between the seriousness of the interference into fundamental rights and the seriousness of the reason justifying the interference, in particular with regard to the proportionality principle. The AG opines that the CJEU would apply the concept of the seriousness of the offence only in case of data retention where no differentiation, limitation, or exception is made as regards the persons affected, the means of electronic communication, and the type of data. The AG further points out that the case at issue shows several differences in comparison to the situations decided by the CJEU in *Digital Rights* and *Tele2*, such as:

- Targeted measure;
- Data solely relate to identity;
- Restricted category of subscribers or users;
- Specific means of communication;
- Data sought for a limited period;
- Harmful effects for the persons concerned only slight and circumscribed.

The AG therefore concludes that, in the present case, the interference is not serious (i.e., the disclosure of the sought data does not entail a serious infringement of privacy), as a consequence of which even criminal offences that are not particularly serious may justify such interference (i.e., the disclosure of data requested from the telephone operators). The AG further justifies this conclusion by pointing out that the wording of Art. 15(1) of Directive 2002/15 does not limit an exception to the confidentiality of telecommunications to "serious" offences but only to "criminal offences."

Last but not least, the AG makes further alternative suggestions on the possible criteria for determining the sufficient seriousness of an offence should the CJEU not follow his approach. In this context, the AG concludes the following:

- The concept of "serious crime" within the meaning of the case law in *Digital Rights* and *Tele2* is not an autonomous concept of EU law (its content therefore need not be defined by the CJEU);
- Only a non-exhaustive body of assessment criteria can classify a criminal offence as "serious" within the meaning of the relevant CJEU's case law.

If the CJEU were to answer the second question, the AG recommends that the Member States should be free to set the minimum level of the penalty relevant for that purpose, provided that they comply with the requirements of EU law, in particular the requirement set by the fundamental rights of the CFR.

In terms of balancing fundamental rights and the effectiveness of law enforcement action, the opinion contains some explosive points. Among them, the AG introduces a new category of data retention to which nearly unlimited access on the part of law enforcement authorities is possible. Lawyers have already criticized the AG's approach as a step backwards in the protection of fundamental rights and freedoms.

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