AG: EncroChat Data Can, in Principle, Be Used in Criminal Proceedings

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

Thomas Wahl

AUTHOR

Thomas Wahl

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

Published in
2023, Vol. 18(3) eucrim pp 264 – 265

ISSN: 1862-6947

https://eucrim.eu

On 26 October 2023, Advocate General (AG) *Tamara Ćapeta* released her opinion on the reference for a preliminary ruling with regard to the EncroChat case. In the case at issue, the Regional Court of Berlin, Germany, asked several questions as to the lawfulness of a European Investigation Order that was issued by the General Public Prosecution Service of Frankfurt in order to receive consent from France for the use of the infiltration of EncroChat devices by French and Dutch authorities. The AG takes the view that the transfer of evidence was, in principle, in line with the EIO Directive. The case is referred as C-670/22 (*Staatsanwaltschaft Berlin v M.N.*). For the reference by the Berlin court → eucrim 3/2022, 197-198.

Facts of the case and questions referred

EncroChat was an enterprise that provided encrypted phone networks. After suspicion that the EncroChat devices had often been used by criminals, French and Dutch law enforcement authorities conducted a joint operation and succeeded in installing a piece of Trojan software on the terminal devices via a simulated update. They were thus able to read the chat messages of thousands of users in real time, including those who used the network for criminal activities. EncroChat users in 122 countries were affected by that interception, including approximately 4600 users in Germany. In the present case, the accused is charged with drugs trafficking before the Berlin court. He argued that German law enforcement authorities unlawfully received the evidence from France and the evidence cannot be used in the criminal proceedings against him. The Regional Court of Berlin posed a number of questions on the interpretation of Directive 2014/41/EU regarding the European Investigation Order in criminal matters (the EIO Directive). The questions particularly concern:

- The German public prosecutor's competence to issue an EIO;
- The admissibility of the EIO pursuant to Art. 6(1) EIO Directive;
- Correct application and interpretation of Art. 31 EIO Directive, which regulates the surveillance of telecommunications without the technical assistance of a Member State;
- The consequences of a possible infringement of EU law for the national criminal proceedings.

The AG's conclusions

AG *Ćapeta* first stressed that the present reference is not about the validity of the French investigation measures, but the set of facts are to be assessed under the EIO Directive. Second, she clarified that the EIO in question concerns the transfer of evidence that France already had in its possession and not the gathering

of data in France through the interception of telecommunications. Subsequently, she reorganised the groups of questions and concluded in detail as follows:

- The requirement under Art. 6(1)(b) EIO Directive that an EIO can be issued on the condition that the investigation measure is available *under the same conditions in a similar domestic case* means - if existing evidence is sought - that the relevant conditions of the national law for the transfer of evidence gathered through the interception of communication between criminal procedures domestically must be established. Due to the close interconnection with Art. 2(c)(i) EIO Directive, it also means that the EIO need not be issued by a court if national law provides that a public prosecutor may order such a transfer in a similar domestic case.
- When an underlying measure in the executing State (here: France) was authorised by a judge (here: juge d'instruction in Lille), an EIO for the transfer of such evidence does not need to issued by a judge as well, even if under the law of the issuing State (here: Germany) the underlying gathering of evidence would have to be ordered by a judge.
- The assessment of the necessity and proportionality of an EIO (Art. 6(1)(a) EIO Directive) requesting the transfer of the existing evidence is a matter for the issuing authority, with a possibility of review by the competent national court. Such an assessment must take into consideration that the access of the national authority to the intercepted communication data represents a serious interference with the private lives of the persons concerned. That interference must be counterbalanced by a serious public interest in the investigation and prosecution of crimes.
- Under Art. 31 EIO Directive, France should have informed the German authorities as soon as it realised that part of the intercepted data originated from mobile phones in Germany. However, since the EIO Directive does not impose an obligation on the Member States to flag the national authority competent to receive such notifications, France (as intercepting state) could have submitted the notification to any authority that it considered appropriate in Germany (as the notified State). With regard to the purpose of Art. 31 EIO Directive, AG *Ćapeta* clarified that it protects both the individual telecommunications users and the sovereignty of the notified Member State.
- Looking at the questions as to whether inadmissibility of evidence results from EIOs issued contrary to the EIO Directive, the AG points out that the EIO Directive and Union law do currently not regulate admissibility of evidence. Therefore, this is a matter of national law. It can only be inferred from Art. 14(7) EIO Directive that national law must protect the rights of the defence in Arts. 47 and 48 CFR. The principles of equivalence and effectiveness do not apply in the given context of (in)admissibility of evidence.

Put in focus

AG *Ćapeta* seems to object in some point the findings by the German Federal Court of Justice, which saw no hindrances to accept the evidence exchanged between German and French authorities (→ eucrim 1/2022, 37-38). Nonetheless, the findings of her opinion may not provide many arguments for the defence to plead, in the light of Union law, for the exclusion of the EncroChat data received from the French-Dutch interception. *Ćapeta* particularly does not see any contradiction to the ECJ's case law on data retention. Even though Advocate Generals' opinions are not binding on the ECJ, they are an important point of reference in practice.

The question of the admissibility of the use of evidence remains of crucial importance and will continue to be the subject of intense debate. Defense lawyers and academics have voiced massive concerns. They criticize, *inter alia*, that the facts of the operation have never been fully clarified and that the judicial and law enforcement authorities involved, including the Federal Criminal Police Office (BKA) and Europol, disregarded the rights of the accused.

.

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