ECJ Ruled in EncroChat Case

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
2024, Vol. 19(1) eucrim pp 40 – 43
ISSN: 1862-6947
https://eucrim.eu

On 30 April 2024, the ECJ delivered its judgment in the EncroChat case (Case C-670/22, *M.N.*). The case concerned the retrieval of German user data stored on a Europol server by the German Federal Criminal Police Office. The French police had been able to infiltrate the encrypted telecommunications service EncroChat, whose devices were often being used by criminals. This French operation led to several follow-up investigations, also in Germany.

The ECJ responded to a number of issues put forward by the Regional Court of Berlin (*Landgericht Berlin*) that cast doubt on the lawfulness of European Investigation Orders issued by the Frankfurt General Public Prosecution Service of Frankfurt a.M. The aim had been to receive consent from France for use of data from the infiltration of EncroChat devices by French and Dutch authorities as evidence in German criminal proceedings.

Background of the case before the ECJ

The service company EncroChat provided encrypted mobile phones that were often used by criminals, e.g., for the purpose of illegal drug trafficking – as in the case before the Regional Court of Berlin. With the assistance of Dutch experts and authorisation by a French investigative judge, the French police were able to install a Trojan software on the terminal devices via a simulated update and thus read the chat messages of thousands of users in real time, including those who used the network for criminal activities. This led to several follow-up investigations, including in Germany.

The German Federal Police Office (*Bundeskriminalamt – BKA*) was able to retrieve the intercepted data relating to EncroChat users in Germany from a Europol server. By means of European Investigation Orders (EIOs), the General Public Prosecution Service of Frankfurt sought *ex post* authorisation for the transmission and use of these data in German criminal proceedings.

The Regional Court of Berlin submitted a series of questions on the lawfulness of the EIOs to the ECJ relating to the following issues:

- 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.

For further information on the background of the referral → eucrim 3/2022, 197-198. For the Advocate General's opinion → eucrim 3/2023, 264-265. For the law enforcement operation against EncroChat → eucrim 1/2021, 22-23 and eucrim 2/2023, 163-164.

The ECJ's replies

The ECJ partly divided the questions into subtopics, partly reformulated them, and considered them together. In general, the judges in Luxembourg considered it decisive that the EIO had been issued in order to obtain evidence that was already in the possession of the competent authorities in the executing State (here: France) and not to seek specific evidence that first would have had to be collected in the executing State by carrying out investigative measures. In detail, the judges in Luxembourg gave the following replies to the Regional Court of Berlin:

Had the EIO to be issued by a judge?

With its first question, the Regional Court of Berlin asked whether Arts. 2(c) and 6(1) of Directive 2014/41 (the EIO Directive) should be interpreted as meaning that an EIO for the transmission of said evidence must necessarily be issued by a judge.

The ECJ noted that the Directive includes a public prosecutor among the authorities, who, like a judge, court, or investigating judge, is understood to be a "judicial authority" competent to issue EIOs without the necessity of validation. It is crucial for the ECJ whether, in purely domestic situations, public prosecutors can issue orders for the transmission of evidence already in the possession of another competent national authority. In this context, the ECJ pointed to Section 100e(6) no 1 of the German Code of Criminal Procedure (*Strafprozessordnung – StPO*), which regulates the use of personal data obtained by covert remote search of information technology systems for *other* criminal proceedings. The ECJ acknowledged the German government's statement that, in this case, the transmission of the data could be ordered by a public prosecutor and does not need prior approval by a judge (as is necessary for the original order for a covert remote search).

Under which conditions could the EIO be issued?

As to the second question, the ECJ verified whether and, if so, under what conditions Art. 6(1) of the EIO Directive precludes a public prosecutor from issuing an EIO for the transmission of evidence already in the possession of the competent authorities of the executing State in which that evidence was acquired. Evidence in said case had been acquired via the interception – by those authorities on the territory of the issuing State – of telecommunications of all the users of EncroChat mobile phones that enabled end-to-end encrypted communication through special software and modified hardware.

Looking at the required review of the necessity and proportionality of issuing the EIO (Art. 6(1)(a) of the EIO Directive), the ECJ found that the assessment must be carried out in the light of the national law of the issuing State, taking into account that evidence already in the possession of the competent authorities of the executing State has been transmitted. Against this backdrop, the ECJ provided the following two clarifications:

- It is not necessary that, at the time when the EIO in question is issued, suspicion, based on specific facts, of a serious offence in respect of each person concerned exists if no such requirement arises under the national law of the issuing State (here: German StPO);
- It is irrelevant that the integrity of the data gathered by the interception measure cannot be verified because of the confidentiality of the technology underpinning that measure, provided that the right to a fair trial is guaranteed in the subsequent criminal proceedings.

Looking at the requirement that the EIO "could have been ordered under the same conditions in a similar domestic case" (Art. 6(1)(b) of the EIO Directive), the judges in Luxembourg reiterated that a distinction must be made between two differing situations. The first situation concerns circumstances in which the investigative measure indicated in the EIO consists of obtaining existing evidence already in the possession of the competent authorities of the executing State, that is to say, the transmission of that evidence to the competent authorities of the issuing State. The second situation concerns circumstances in which the collection of evidence is sought via a specific investigative measure, i.e., the evidence does not yet exist. Since the first situation applies in the present case, the ECJ ruled that the issuing of an EIO is not subject to the same substantive conditions as those that apply in the issuing State in relation to the gathering of that evidence. Moreover, the fact that, in this case, the executing State (here: France) gathered evidence on the territory of the issuing Sate (here: Germany) and in its interest is irrelevant in that respect.

The judges in Luxembourg added, however, that the EIO Directive also guarantees judicial review of compliance with the fundamental rights of the persons concerned. Therefore, it is necessary that a party must be "in a position to comment effectively on a piece of evidence that is likely to have a preponderant influence on the findings of fact." If this is not the case, the national court must find an infringement of the right to a fair trial and exclude that evidence in order to avoid such an infringement.

Who must be notified under Art. 31 of the EIO Directive, if at all?

In another set of questions, the Regional Court of Berlin asked, in essence, whether Art. 31 of Directive 2014/41 must be interpreted as meaning that a measure entailing the infiltration of terminal devices for the purpose of gathering the traffic, location and communication data of an internet-based communication service constitutes an "interception of telecommunications", within the meaning of that article. And, if answered in the affirmative, whether this interception must be notified to a judge of the Member State on whose territory the subject of the interception is located.

The ECJ first clarified that the concept of "telecommunications" used in Art. 31 of the EIO Directive must be given an independent and uniform interpretation throughout the EU. Considering the wording, context, and objective of Art. 31, the ECJ found that the infiltration of terminal devices for the purpose of gathering communication data as well as traffic or location data from an internet-based communication service indeed constitutes an "interception of telecommunications" within the meaning of Art. 31(1) of Directive 2014/41.

Secondly, as to the question of which authority must be notified, the ECJ observed that both the wording of Art. 31(1) ("competent authority") and the EIO form leave this question open. It follows that the Member States on whose territory the subject of the interception is located must designate the authority for the purpose of notification. However, the intercepting Member State (here: France) can submit the notification to any appropriate authority of the notified Member States (here: Germany) if it is not in a position to identify the competent authority in that State.

What is the scope of protection of Art. 31 of the EIO Directive?

In the context of Art. 31 of the EIO Directive, the Regional Court of Berlin also asked whether this provision intends to protect the rights of users affected by a measure for the "interception of telecommunications" within the meaning of that article, and whether that protection would extend to the use of the data thus collected in the context of a criminal prosecution initiated in the notified Member State.

The ECJ pointed out that the interception of telecommunications amounts to an interference with the right to respect for the private life and communications – enshrined in Art. 7 CFR – of the target of the interception. Thus, Art. 31 intended not only to guarantee respect for the sovereignty of the notified Member State but

also to ensure that the guaranteed level of protection in that Member State with regard to the interception of telecommunications is not undermined, in short: it also protects the rights of the affected users.

Does EU law require the exclusion of unlawfully obtained evidence?

With this last question, the Regional Court of Berlin queried whether the principle of effectiveness requires national criminal courts to disregard information and evidence obtained in breach of the requirements of EU law in criminal proceedings against a person suspected of having committed criminal offences.

The ECJ reiterated its case law on the admissibility of information obtained contrary to EU law in criminal proceedings. As a rule, the principle of procedural autonomy enables the Member States' powers to establish procedural rules for actions intended to safeguard the rights that individuals derive from EU law. However, this rule has two limits:

- The national rules cannot be less favourable than the rules governing similar domestic actions (the principle of equivalence);
- They cannot render impossible in practice or make excessively difficult the exercise of rights conferred by EU law (the principle of effectiveness).

Referring to Art. 14(7) of the EIO Directive, the judges in Luxembourg clarified in this respect that, in criminal proceedings against a person suspected of having committed criminal offences, national criminal courts are required to disregard information and evidence if that person is not in a position to comment effectively on that information and on that evidence and the said information and evidence are likely to have a preponderant influence on the findings of fact.

Put into focus

At first glance, the ECJ appears to strengthen those in favour of the usability of the data from the EncroChat police hack operation in the EU Member States. As Advocate General *Carpeta's* Opinion (→ eucrim 3/2023, 264-265) already suggested, the arguments against their use on the grounds of a breach of EU law are weak. According to both the Advocate General and the ECJ, the decisive fact is that the EIO issued by the Frankfurt public prosecutor in the present case was in order to obtain evidence already in possession of the competent authorities in the executing State. In such cases, the ECJ considers the requirements for such an EIO to lawfully obtain existing information to be significantly lower compared to a case in which an EIO is issued in order to initiate the collection of evidence.

On closer inspection, however, the ECJ deviates in part from the Advocate General's conclusions and various backdoors remain open. This leaves glimmers of hope for defence lawyers of clients against whom criminal proceedings were initiated as a result of the surveillance. These backdoors must be skillfully exploited in further proceedings before German courts. The following statements by the ECJ may serve as starting points:

- The ECJ reinforces the importance of Art. 31 of the Directive. It is now beyond question that the French authorities should have informed the German side of the measure. It may be true that the German Federal Criminal Police Office and the German Public Prosecutor General's Office were informed in this case. However, they should have forwarded the information to the judge/court responsible under German law. This was a deliberate circumvention of the requirement for a court decision (*Richtervorbehalt*). Under German law, circumventing this requirement of jurisdiction normally leads to a ban on the use of evidence.
- The ECJ emphasises the individual-protecting nature of Art. 31. This was still questioned by the Federal Court of Justice (*Bundesgerichtshof – BGH*; on the BGH decision in the EncroChat case → eu-

crim 1/2022, 26-37). The individual-protecting function of Art. 31 must therefore be given greater weight than has been accorded by the German courts to date when striking a balance between the interest in criminal prosecution and safeguarding the interests of the person concerned. It is also important that the function of protecting the individual cannot be reduced to whether or not the person concerned can seek legal protection in the intercepting state (here: France): the ECJ makes it clear that the notified state must ensure legal protection, as the notified state is where the person concerned must seek appropriate legal review.

- The ECJ emphasises that Art. 6(1)(b) of the EIO Directive applies, meaning that the measure could also be ordered in a comparable (purely) domestic case. The German Federal Court of Justice still rejected the applicability of this standard to cases in which evidence is in the possession of the executing State (→ eucrim 1/2022, 26-37). The ECJ follows the German Federal Government's submission that the public prosecutor's office could also have requested disclosure of the information under German law in accordance with Section 100e StPO and that this does not imply suspicion of a specific criminal offence in cases of "chance discovery". It is questionable, however, whether the federal government's view is correct, because it overlooks the fact that, under German law, the basic measure (the overt remote search of information technology systems, also called the online search) must at least be based on a concrete suspicion of an offence and does not permit mass access to unspecified information systems. Another important issue is: at least this basic measure should have been ordered by a special division of the regional court (and not just by the local judge, as is usual for other investigative measures). It cannot be denied that, in the entire chain of information transfers, the legality of the basic measure was never examined by a court in accordance with German law, but could easily be overridden by the much more far-reaching possibilities of French law. This would amount to inadmissible forum shopping on the part of law enforcement.
- Finally, the ECJ stresses in two areas that the defence could "comment effectively" on the evidence and the method of its collection. It is probably undisputed that the evidence had a preponderant influence on the criminal court's findings, as the criminal convictions in almost all instances were based on the analysis of the chats on the EncroChat devices. The ECJ goes even further: if the defence was not able to take a proper legal stance, there is an absolute ban on the use of evidence following a breach of EU law. In this context, it should be recalled that the EncroChat case was primarily characterised by the secrecy of the Trojan used. In particular, the French authorities invoked military secrecy and thus refused to disclose their method. The ECJ now requires that the integrity of the transmitted evidence can be examined by the defence, at least at the time the evidence was actually handed over to the competent German authorities. However, the ECJ leaves open which data the defence could actually have accessed to check for integrity and what an "effective comment" means in practice. It is to be feared that these issues will continue to be disputed in court.

The question of the use of EncroChat data as evidence is sure to keep German courts busy due to – and despite – the ECJ's ruling. The decision leaves room for manoeuvre for both supporters and opponents of the use of the EncroChat data. Due to unclear statements by the ECJ, particularly regarding the scope of the rights of the defence with regard to the integrity of the data, the EncroChat case may keep the judges in Luxembourg busy again. In this context, it should be recalled that, in November 2023, the Regional Court of Berlin submitted the second reference for preliminary ruling to the ECJ in relation to criminal proceedings from the EncroChat outcome (the case was registered on 19 April 2024 as Case C-675/23, M.R. v Staatsanwaltschaft Berlin → related link). The Berlin court was dissatisfied with the Advocate General's application of the facts in the case analysed here. In the new referral, the court once again emphasised the unspecific mass surveillance by the EncorChat police operation and the serious interference with fundamental rights of telecommunication users, including the lack of adequate legal remedies. It remains to be seen whether the ECJ will provide the Berlin court with clearer answers in this second case.

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