Germany: European Court opinion kicks questions over EncroChat back to national courts

Bill Goodwin ⋮ 10-13 minutes ⋮ 10/27/2023

The European Court of Justice (ECJ) has issued a preliminary opinion which opens the way for data obtained from an encrypted phone network hacked by French police to be lawfully used as evidence in prosecutions in Europe, but leaves critical legal questions for national courts to resolve.

The advocate general of the European Court of Justice said in a legal opinion yesterday (26 October 2023) that Germany lawfully used a European warrant to obtain data intercepted by French investigators from German EncroChat phone users.

But the opinion said that the ECJ was unable to give any view whether the evidence is legally admissible in Germany or other member states, leaving it up to member states to decide on the admissibility of evidence under their own laws.

The 24-page legal opinion also concluded that member states were bound by the principle of mutual recognition, which required them to accept the lawfulness of the French interception operation that had been approved by the French courts.

The opinion suggests that people charged with EncroChat offences would be able to challenge the lawfulness French interception warrants in France, a point that has been disputed by the French government in separate submissions to the European Court of Human Rights.

The European Court of Justice in Luxembourg, which usually follows the advocate general's opinion but is not bound by it, is expected to make a final decision early next year.

Defence lawyers predict further delays

German defence lawyer Christian Lödden said the advocate general had failed to clarify legal questions over EncroChat, and if adopted by the ECJ, would kick the critical questions back to national courts to resolve.

“We all hoped they would make a clear European decision because in every country we see the same problems because it is the same operation. But what we see now from the advocate general is, ‘No we don’t want to decide on a European level, go back to a national level’,” he told Computer Weekly.

Lödden said it would be at least another year before legal questions around EncroChat were resolved, leaving thousands of people across Europe potentially waiting in pre-trial detention.

“We have over 16,000 people in prison in Germany, in some cases for more than three years. We have people in pre-trial detention or custody, so it’s not okay,” he said.

The police operation against EncroChat has proved controversial, leading to a series of legal challenges in the French Constitutional Court, the Berlin Regional Court, the UK’s Investigatory Powers Tribunal, and a forthcoming case at the European Court of Human Rights.

The joint operation by French and Dutch police against EncroChat, which was widely used by organised criminals and drugs gangs, has led to more than 6,500 arrests worldwide and the seizure of nearly €900m following three years of investigation, Computer Weekly reported in June.

Questions raised by Berlin court

The court’s legal opinion follows a decision by the Berlin Regional Court last year to refer a series of questions to the European Court of Justice seeking clarification on whether France’s sharing of hacked EncroChat messages with other countries was lawful under European law.

These include whether Germany should have asked the German courts – which offer independent oversight – to issue European Investigation Orders (EIOs) to obtain the French data, rather than issue an order through the public prosecutor’s office.

The European court had also been asked to assess whether it was proportionate to intercept data from all EncroChat handsets in Germany when there was no concrete evidence of criminality against any individual phone user in Germany.

Prosecutors from France, Germany, the Netherlands, Spain, Hungary, Sweden, the Czech Republic and Ireland gave oral evidence about the lawfulness of the novel police hacking operation during a seven-hour hearing in July 2023.

European Investigation Orders lawful

The case centres on whether EIOs issued by the Frankfurt Public Prosecutor's Office to obtain EncroChat evidence from France were legally valid under European law.

The EIO Directive allows a member state to request another member state to conduct an investigation on condition that the investigative measure requested is lawful in the requesting country.

According to the advocate general, Tamara Ćapeta, Germany did not use EIOs to require France to intercept data from German EncroChat phones. It merely sought to transfer evidence already intercepted by France from EncroChat to Germany.

Ćapeta found that this was equivalent to a domestic case in Germany where evidence was transferred from one criminal procedure in one part of Germany to another criminal procedure in another part of Germany.

She concluded that whether such a transfer was lawful in Germany was a question for German law rather than the European Court of Justice.

However, she added that she believed it was likely to be lawful, as the German government had confirmed to the court that the transfer of evidence gathered through interception of communications was possible under German law.

No forum shopping took place

Ćapeta rejected suggestions that German authorities had turned to their French counterparts to obtain evidence contrary to German law.

"The circumstances of the present case do not lead to the suspicion of an abuse of cross-border investigation procedures," she wrote in her opinion.

France gathered evidence from EncroChat phones in the course of its own investigation and was not acting to enable a German criminal investigation, she found.

Even if a German judge refused to authorise a similar interception operation in Germany, the French authorities had undertaken the interception in accordance with French law, and it was lawful for Germany to request the intercepted data, Ćapeta concluded.

The advocate general found that questions over the legal validity of the French interception measures were a matter for French law, rather than the European Court of Justice.

Member states were bound by the principle of mutual recognition for judicial cooperation in the European Union (EU). That means they must accept the legality of the French data interception operation which had been approved by the French courts.

“The legal challenge against those interception measures is a matter of the competent French courts,” she wrote.

The advocate general suggested that individuals charged with EncroChat offences would be able to challenge the legality of the French interception warrants in France.

But lawyers have questioned whether France would allow such a legal challenge. The French government has made it clear in a separate submission to the European Court of Human Rights that it would not be able to do so.

“As long as you are a member of the European Union, you can’t challenge whether the evidence was correctly obtained by France,” said Lödden.

Proportionality is a matter for national law

Ćapeta said the EIO must be necessary and proportionate and take into accounts the rights of those accused or suspected of crimes, adding it was irrelevant whether the criminal investigation into EncroChat was successful and resulted in numerous convictions for serious crimes.

“The relevant question is whether the level of intrusion into private lives ... may be justified by the importance of the public interest in the criminal investigation,” Ćapeta wrote.

She found that the access by German authorities to communications data transferred from France may be characterised as a serious interference with fundamental rights. However, she said it was not for the ECJ to decide whether it was disproportionate to order the transfer of the data of all EncroChat users in Germany if there was no concrete evidence of the crimes committed.

That question would have to be decided by national courts.

EncroChat hack was not mass surveillance

Ćapeta wrote in her opinion that the data transferred from France to Germany was not “indiscriminately gathered” from the entire population. The data was limited only to EncroChat users in Germany “in the context in which a suspicion existed that this service is used primarily for committing criminal offences”.

The operation is not “comparable to the mass surveillance of the general population”, she wrote.

The EIO Directive provided additional safeguards, which require member states to ensure that legal remedies are available, and that suspects should be able to challenge the proportionality assessment made by the public prosecutor when issuing the EIO.

Should Germany have obtained a court order?

Ćapeta said it was also a matter for German law whether prosecutors should have asked a German court to issue an EIO to obtain the French data, rather than issue an EIO through a public prosecutor.

A court order would only have been required if German law also required a court order in a comparable domestic case, for example, the transfer of evidence from one prosecution case to another prosecution case. “That does not seem to have been the case under German law,” she wrote.

“In the present case, all the steps taken in order to gather data via the EncroChat server in France were authorised by the competent French courts. I therefore see no reason why a German public prosecutor would not be able to issue an EIO for the transfer of that evidence,” Ćapeta wrote.

Admissibility of EncroChat evidence is a matter for national courts

The advocate general said EU law does not yet govern whether evidence is admissible in criminal procedures, in effect referring the matter back to German and other national courts to decide.

“The question of whether evidence obtained in breach of domestic or EU law is admissible is governed by laws of the member states,” Ćapeta found.

However, admissibility of evidence must comply with Article 47 of the European Charter of Fundamental Rights, which guarantees the right to a fair trial, and Article 48, which requires that defendants are presumed innocent and have the right to a legal defence.

Germany’s Federal Criminal Police Office, the BKA, began investigating EncroChat encrypted phones after discovering that organised criminals were using the phones in 2018.

The BKA argued that the use of an EncroChat phone was grounds for suspicion of criminal activity, because its encryption capabilities, coupled with its high cost – €1,000 to €2,000 for a six-month contract – meant it was unlikely to be used for legal purposes.

EncroChat users in 122 countries, including 4,600 users in Germany, were impacted by the French interception operation.

Germany's constitutional court disclosed in a ruling in September that, with five constitutional complaints over EncroChat waiting to be heard, it was as yet unclear whether evidence from EncroChat could be lawfully used to bring prosecutions in Germany.

The impact of the ECJ's final ruling on hundreds of prosecutions underway in the UK is uncertain because the UK is no longer under the jurisdiction of the ECJ following Brexit.