EncroChat's path to Europe's highest courts

After infiltrating an encrypted phone network widely used by criminals (EncroChat), law enforcement authorities in Europe made headlines with high-profile arrests and seizures. Across Europe, defendants are now challenging evidence and convictions, claiming flawed investigations, violations of cross-border evidence-sharing rules and insufficient disclosure of evidence. They argue that authorities violated their rights to a fair trial, effective remedy and privacy. This paper provides background on the EncroChat operations and an overview of the trends in French, German and UK jurisprudence, and calls attention to recent challenges before Europe's highest courts.

Background

EncroChat devices are modified mobile phones (e.g. with the camera, GPS and USB port removed) running two operating systems side-by-side, of which one enables secret and encrypted messaging and voice calls and another runs the inconspicuous native (usually Android) operating system. They were sold on a popular online trading platform for approximately €1 600, which included a six-month subscription with worldwide coverage. Back in 2017, the French Gendarmerie and judicial authorities began investigating such phones after repeatedly finding them connected to organised crime groups. In December 2018 and October 2019, a French judge allowed authorities to copy data linked to the EncroChat domain from a server located in the French city of Roubaix. A partial decryption of obtained 'notes' showed that they were 'beyond doubt, linked to illegal activities, especially drug trafficking' (unofficial translation). On 30 January 2020 (and again on 12 February) a judge authorised the remote installation of an interception tool on end-user devices linked to the server. The prosecution said that this was necessary to identify and arrest users implicated in illegal activities. After obtaining several other authorisations, authorities installed the interception tool, which is classified a national defence secret, on 1 April 2020. After France first shared data with the Netherlands, Eurojust facilitated the creation of a joint investigation team between the two countries and with the participation of Europol. The operation was portrayed as 'an example of good practice' by the two supporting EU agencies and yielded key information for the identification, investigation and prosecution of criminal networks (infographic on procedure). A preliminary report from September 2021 is said to quote 6 700 arrests and 3 800 judicial proceedings. This number will likely need to be revised upwards in light of the many operations reported in Germany and the UK, and also in Spain, Italy, the Netherlands, Sweden and Belgium. EncroChat operations and EU spyware cases both involve government(-backed) mobile phone infiltration. However, EU spyware allegations revolve around the instrumentalisation of commercial spyware against political rivals, while the issues at stake relate to criminal investigations.

Court cases in France, Germany and the UK

Defence lawyers across Europe argue that the messages obtained through the infiltration of EncroChat should not be admissible as evidence in court. In two open letters, 100 lawyers and 22 lawyers, respectively, many directly involved in defending EncroChat users, criticise the fact that defendants face unfair trials because prosecutors refuse to disclose information about the hacking operations.

In **France**, lawyers challenge, for instance, (i) the absence of a time limitation on interception measures in court orders, (ii) the authorisation of far-reaching measures through court orders, which are not covered by their envisaged legal bases, (iii) the 'massive and indiscriminate' interception, and (iv) the refusal of the Gendarmerie to disclose any technical details of the interception operation. Conversely, Eurojust considers that the French investigation was conducted in accordance with the applicable legal rules. Reportedly, the French Gendarmerie stated that it had obtained a favourable opinion on their data impact assessment from the French Data Protection Authority (CNIL), as well as a positive opinion from the ministerial data protection officer. Asked by *Le Monde*, the CNIL specified informally that this opinion was a declarative commitment without the document having been re-examined.

The French Cour de cassation (supreme court) has ruled on two EncroChat cases, after asking the Conseil constitutionnel (constitutional court) whether Articles 706-102-1 and 230-1 et seq. of the French Code of

Author: Hendrik Mildebrath, Members' Research Service
PE 739.268 – December 2022

Criminal Procedure are constitutional. The **Conseil consitutionelle** ruled in its decision of 8 April 2022 that the criminal code provisions allowing investigators to place technical information under national defence secrecy do not violate defendants' rights to an effective judicial remedy, their right to privacy, freedom of expression, or any other right guaranteed by the Constitution (EN and FR summary). Incidentally, the decision draws attention to legal requirements and the necessary disclosure of certain information to justify the removal of certain technical information from the adversarial process. In turn, on 11 October 2022 the **Cour de cassation** found that the Court of Appeals did not adequately address the absence of a certificate validating the results of the operations, partially quashed the contested decision of the Nancy Court of Appeals, and referred the case to the Metz Court of Appeals for a new ruling (summary). On similar grounds, it also partially quashed another contested decision of the Nancy Court of Appeals two weeks later and referred it to the Paris Court of Appeals. The French cases could affect prosecutions and legal challenges across Europe, which rely on the information provided by French authorities (evidentiary 'black hole').

So far, **UK** challenges to the use of the European Investigation Order (EIO), requiring the French authorities to give the Crown Prosecution Service access to EncroChat Data, and to the admissibility of evidence in EncroChat cases have remained unsuccessful. The Administrative Court, part of the English High Court, refused the application for permission to judicially review the EIO on which the claimant's criminal proceedings depended (summary), and the Court of Appeal (Criminal Division) ruled that the communications collected are admissible as evidence (summary). The latter commented that, if similar appeals were launched, 'those involved should not be surprised if the trial judges deal with them rather more briskly' and refused leave to challenge the evidence in the UK Supreme Court. Forensic expert witnesses involved in EncroChat cases point out that the Court of Appeal's decision 'fundamentally changes UK policy on intercept evidence' and that law enforcement agencies may attempt to rely on the permissive legal basis for 'equipment interference' to intercept transiently saved data. Reports emerged that the Investigatory Powers Tribunal, responsible for complaints against intelligence services, is hearing cases related to EncroChat – this redress avenue was recommended by experts and mentioned by the Administrative Court.

Conversely, **German** prosecutors suffered a setback when the Berlin Regional Court found EncroChat evidence inadmissible in July 2021. The court held that the evidence was obtained in breach of the European Investigation Order Directive and that the facts of the case did not give rise to a sufficient level of suspicion that would warrant the surveillance measures applied. Consequently, it recognised a violation of the constitutional fundamental right to confidentiality and integrity of information technology systems, as well as the fundamental right to secrecy of telecommunications (summary). On appeal by the Prosecutor's Office, the Berlin Higher Regional Court reversed the decision in August 2021, in line with a number of other Higher Regional Court rulings from across Germany (e.g. Karlsruhe, Brandenburg, Düsseldorf, Rostock, Schleswig). Exceptionally, the Frankfurt (Oder) Regional Court expressed sympathy with the position of the Berlin Regional Court. In a recent decision, the **Federal Supreme Court** determined that EncroChat data may be used for the investigation of serious criminal offences (press release). The admissibility of evidence is not contingent on whether French investigations operationally satisfy German legal standards, nor did French investigations violate basic human rights or constitutional requirements rendering evidence inadmissible, nor does delayed disclosure of surveillance operations relating to German territory prejudice admissibility. The **Federal Constitutional Court** announced that it had received a constitutional complaint against a judgment of the Rostock Regional Court and the related Federal Supreme Court decision.

Applications to the CJEU and the ECtHR

The division of the Berlin Regional Court that had previously declared EncroChat evidence inadmissible recently requested a preliminary ruling from the Court of Justice of the European Union (CJEU) on 14 critical questions concerning another EncroChat case (summary). In addition, two British detainees have lodged applications with the European Court of Human Rights (ECtHR).

In a similar case, *'the Italian Supreme Court ruled that encrypted messages obtained by an international police operation to hack a [second] phone network used by organised crime groups cannot be used in a pre-trial hearing unless prosecutors explain how the evidence was obtained. Italy's Corte di Cassazione found that a defendant should not only have the ability to ask questions about the contents of messages police obtained from the Sky ECC phone network, but also to question how the investigative process was carried out.'*