EncroChat – A Judicial Chronology

Interpretations from Paris, Strasbourg and Luxembourg Courts

Maxime Lassalle, Salomé Lannier

eucrim
European Law Forum: Prevention • Investigation • Prosecution

Article

ABSTRACT

The EncroChat investigation marks a turning point in European criminal justice, revealing unprecedented legal and technical challenges that arose from the hacking of encrypted communication devices ("cryptophones"). The operation originated in France and escalated with the deployment of Trojan-style malware, which enabled the collection of data from over 66,000 cryptophone users worldwide. This article provides a detailed timeline of the case, tracing its development from national proceedings to significant rulings by the European Court of Justice and the European Court of Human Rights. It examines the former's interpretation of the Directive on the European Investigation Order and the latter's rejection of challenges arising from the European Convention on Human Rights. By bridging French and European case law and literature, this article fills a gap in existing literature and contributes to ongoing discussions on digital surveillance, privacy, and procedural safeguards in transnational criminal investigations.

AUTHORS

Maxime Lassalle

Maître de conférences
Université de Bourgogne

Salomé Lannier

Post-doctoral researcher
University of Luxembourg, Luxembourg

CITATION SUGGESTION

M. Lassalle, S. Lannier, "EncroChat – A Judicial Chronology", 2025, Vol. 20(4), eucrim. DOI: https://doi.org/10.30709/eucrim-2025-024

Preprint eucrim 2025, Vol. 20(4)
ISSN: 1862-6947
https://eucrim.eu

I. Introduction

Emerging as landmarks in the evolution of investigative techniques, the EncroChat case, and shortly thereafter, the SkyECC case, signalled the onset of a data-centric era in criminal justice. These cases undoubtedly embody a profound transformation in investigative methods. *Oerlemans* and *Royer* refer to this phenomenon as the rise of data-driven investigations, which they define as "the processing of data that has been collected by law enforcement authorities in an earlier phase, which is then enriched and linked with other data for future investigations."[1]

The EncroChat case was the first major investigation to involve the use of cryptophones, or encrypted messaging services, which are designed to guarantee the anonymity of communications often allegedly led by criminals.[2] The case has become emblematic of both the technical limits of such systems and the legal challenges arising from the investigative techniques employed to bypass encryption.

The case's scale prompted courts in various jurisdictions to review the circumstances under which data were collected in France, and how these data were transferred and subsequently used in criminal proceedings throughout Europe. Three key dimensions can be distinguished:

- The collection of data in France, in the context of an investigation targeting the EncroChat system, considering that the systems itself was deemed illegal, and conducted without any individualised suspicion against its users;
- The cooperation among countries, notably the sharing of data through European instruments of mutual legal assistance in criminal matters;
- The use of these data in domestic proceedings, both in France and abroad.

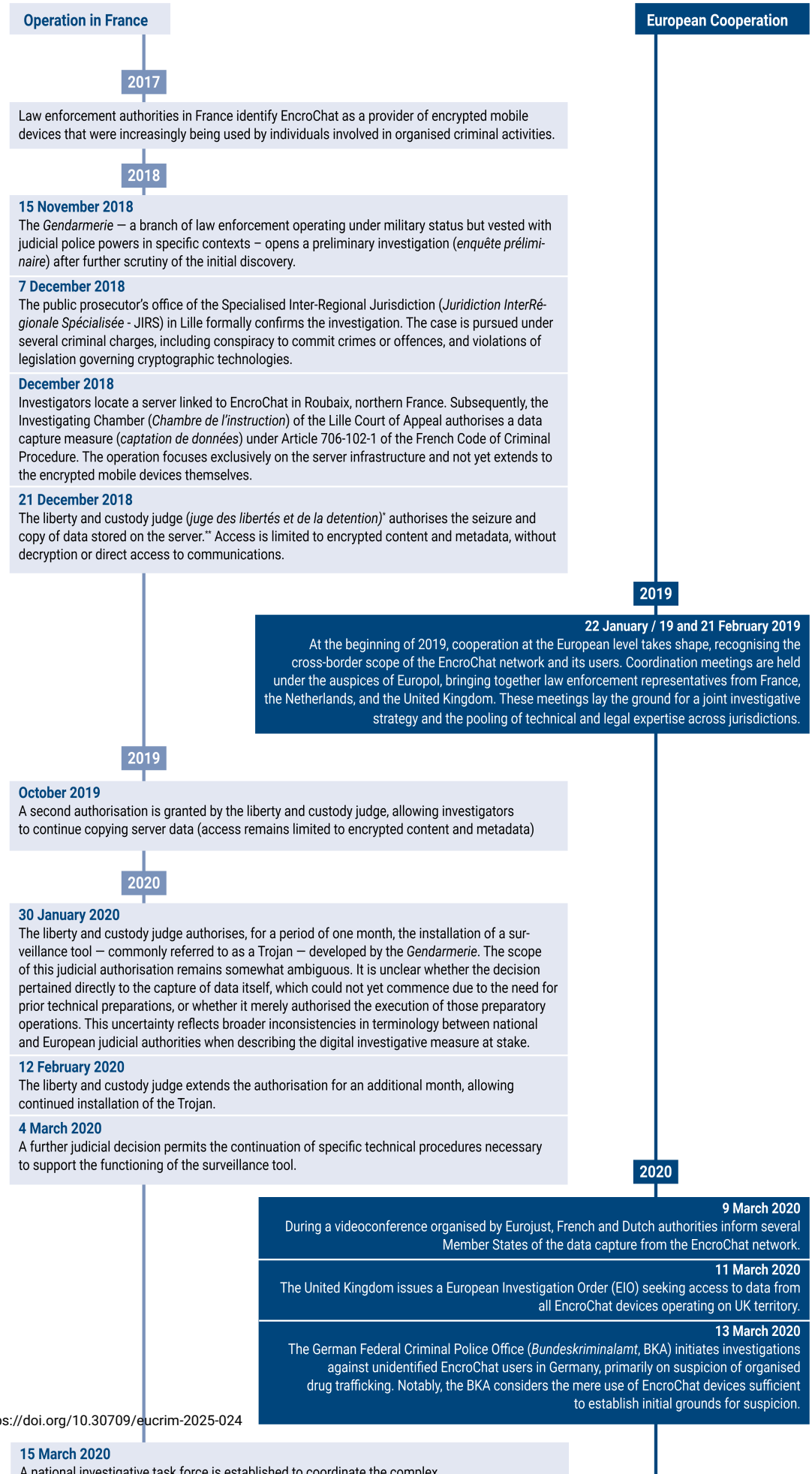
Each of these dimensions raises novel and fundamental questions, prompting referrals to both the European Court of Justice (ECJ) in Luxembourg and the European Court of Human Rights (ECtHR) in Strasbourg. In France, the Constitutional Council (*Conseil constitutionnel*) and the Court of cassation (*Cour de cassation*)[3] were also called upon to rule on various aspects of the case.

Language barriers may have kept scholars from providing a comprehensive account of the origins, legal framework, and subsequent case law relating to the EncroChat case in France. So far, most analyses have focused on the broader fundamental rights implications before European supranational courts. Yet, the peculiarities of French criminal procedure and the early judicial decisions adopted at the national level have directly impacted subsequent European proceedings. Against this backdrop, this article seeks to address this gap by connecting French and European case law, and by consolidating critical perspectives on relevant judicial outcomes. It provides a review of the case from the initial investigation to the most recent domestic and European decisions delivered in 2025 concerning the French operation itself.

II. The EncroChat Investigation

The EncroChat chronology is difficult to piece together, as dates, translations and explanations have been scattered among European reports as well as national and European court decisions. According to the documents referred to here,[4] the EncroChat investigation can be retraced as outlined in the following timeline chart. It distinguishes between the events that happened in France and events that involved European cooperation.

Timeline of the EncroChat Investigation



The scale and impact of the investigation became fully visible only after the operation. According to a press release issued by Eurojust in 2023, the operation led to the arrest of 6,558 individuals. Authorities seized, among others, over 100 tonnes of cocaine, 160 tonnes of cannabis, 923 weapons, 68 explosive devices, 271 properties, 83 boats, and 40 planes. In total, nearly €900 million in criminal assets were either seized or frozen, marking one of the most significant law enforcement operations against encrypted criminal communications networks in Europe.[5]

III. Complaints against the EncroChat Operation in France

Before outlining the litigation of the EncroChat operation before the French Court of Cassation, a brief introduction to the legal background of the data capture measure will provide the necessary context. We can also label this investigative measure as “legal hacking”.

1. Legal background of the data capture measure in France

In French criminal procedure, data capture operations were introduced in 2011 under Articles 706-102-1 to 706-102-5 of the *Code de procedure pénale* (Criminal Procedure Code, CPC).[6] The general framework set out in Articles 706-95-11 to 706-95-19 CPC also applies. This legislation permits investigators, under judicial authorisation, to access, record, retain, and transmit various forms of digital data without the knowledge or consent of the targeted individuals. The scope of authorised data includes: [7]

- Visual data displayed on the user’s screen, captured via screen-logging software;
- Keystrokes entered on the device, recorded through keyloggers;
- Audiovisual data transmitted through peripherals such as webcams or microphones, (though the data protection authority has explicitly prohibited remote activation of such devices[8]);
- Stored data — both content and metadata — accessed via backdoor mechanisms.

These operations may involve physical or remote installation of technical devices, including entry into private premises or vehicles, subject to strict judicial oversight. Authorisation may be granted either by the liberty and custody judge[9] during the preliminary investigation (for up to one month) at the request of the public prosecutor, or by the investigating judge during the judicial inquiry (for up to four months)[10]. The authorisation can be renewed but cannot exceed a total duration of two years. The authorisation must be made in writing and state reasons, specifying the offence, the targeted system, and the duration of the operation. Operations are carried out under the authority of the authorising judge and may involve qualified agents from services under the Ministry of the Interior or Ministry of Defence. Detailed reports must be drawn up, including the timing and nature of the operations, and only data relevant to the authorised offences may be retained. Private life footage unrelated to the offences must be excluded from the case file. Recordings and data are sealed and ultimately destroyed upon expiry of the limitation period for prosecution. Article 706-102-5 CPC explicitly governs the conditions under which technical devices may be installed or removed, including entry into private premises outside legal hours, and transmission via electronic networks — all subject to judicial control.

2. Initial complaint before the Court of Cassation

The EncroChat case first reached the Court of Cassation in February 2022.[11] The defendants challenged the admissibility of the data gathered during the operation, arguing that the access to the clear (unencrypted) content had been made possible through technical means protected by national defence secrecy. Thus, the complaint did not directly address the legal framework governing the data capture itself, but rather focused on the decryption process. The use of such classified technical means is regulated under Articles 230-1 to 230-5 CPC. In effect, the defendants raised questions of a constitutional dimension, alleging that Articles 230-1 to 230-5 infringe upon the right to a fair trial and access to an effective remedy. Their arguments centred on two main points:

- The authorisation of the data capture measure by the public prosecutor, who is not considered an independent judicial authority in France due to their hierarchical subordination to the executive,[12] undermined judicial guarantees;
- When the technical methods used are classified under national secrecy, the defence is denied access to essential technical information, including the certificate signed by the head of the technical body "attesting the sincerity of the transmitted results" ("*certifiant la sincérité des résultats transmis*").[13]

The Court of Cassation deemed these concerns sufficiently serious and referred the legal questions to the Constitutional Council.

3. Decision by the Constitutional Council

In a brief eight-page decision issued in April 2022, the Constitutional Council dismissed said constitutional objections involving Articles 230-1 to 230-5 CPC.[14] The Council found that the procedural safeguards embedded in the legal framework for data capture sufficiently compensated for the limitations imposed by national secrecy. These safeguards include the requirement that data capture may only be authorised for a limited list of serious offences linked to organised crime; that the data must be sealed; and that the case file must contain a report on the installation of the technical device, as well as a description or transcription of the data deemed relevant to establishing the truth. Furthermore, all decrypted material must be accompanied by a certificate signed by the head of the technical body, attesting the "*sincérité*" ("sincerity") of the transmitted results. This is the only way under French law to testify that the data is correctly decrypted without omissions or tampering.[15]

Lastly, the Council noted that, if necessary, courts retain the power to request the declassification and disclosure of information protected by national defence secrecy, in accordance with the procedures set out in the Defence Code. On this basis, the Constitutional Council concluded that the legal framework does not violate the right to a fair trial.

In fact, the Constitutional Council's ruling means that there is in fact no transparency as regards the methods used, and this opacity is not subject to any specific legal framework. In other words, French law does not seek to regulate or limit the use of secret methods as such, as opposed to methods that are open or transparent.

4. Follow-up decisions by the Court of Cassation (2022)

After the legal battle before the Constitutional Council, the French Court of Cassation issued two significant decisions on the EncroChat case in October 2022.[16] In the first decision,[17] the Court mainly endorsed the Constitutional Council's reasoning; but also clarified other aspects.

One of the questions concerned the role of the certificate attesting the "sincerity" of the decrypted data (see above). In the first decision, the Court of cassation clarified that, in the decision challenging the admissibility of the evidence, the judge should not have disregarded this claim. In other words, the judge should have ruled whether the absence of the certificate was an issue. The decision also clarified the scope of the data capture under Article 706-102-1 CPC. The issue was whether the wording of the provision was limited to stored data, thereby excluding access to data in transit. Without truly ruling on the merits, the Court of Cassation clarified that the provision at issue does not distinguish between the forms of data — whether stored or in transit — and that there is therefore no need to address this question.

In its second decision,[18] the Court of Cassation addressed the legal implications of internal data transfers between separate investigations. In the case at issue, the original investigation in Lille had led to the opening of a case in a different city, i.e., Nancy. The defendant argued that he had been denied the opportunity to challenge the legality and fairness of the evidence originating from the Lille proceedings, as key documents had not been included in the Nancy case file. He claimed that this prevented him from verifying the quality and legality of the communication transcripts. The Court of Cassation rejected this argument, holding that the defendant had the right to request access to the original investigation file from the investigating judge (here: Lille) and to appeal any refusal.

In addition, the defendant questioned the integrity of the data, claiming that there was no proof that it had been properly sealed. The Court dismissed this claim as well, stating that procedural irregularities do not justify annulment unless the defendant can demonstrate actual prejudice.

The defendant finally sought to nullify the data capture on the grounds that it constituted an unfair investigative measure the result of which would be self-incrimination if a complaint were to be filed. The Court acknowledged that requiring a defendant to prove that they were affected by an irregularity, for example, by admitting their use of EncroChat – could infringe their right against self-incrimination. Therefore, it held that, in order to determine whether a person has standing to challenge the legality of a measure taken during an investigation, a defendant may either assert a personal interest in the matter or, where such an assertion would risk self-incrimination, the investigating chamber must assess the case file to determine whether the individual is potentially affected by the measure. As a result, even if a defendant denies using EncroChat, they retain standing to contest the legality of the evidence if the investigation attributes a device to them.[19]

5. Further decisions by the Court of Cassation (2023)

In 2023, the Court of Cassation issued two other brief decisions on EncroChat. In the first decision in February 2023,[20] the Court dismissed a challenge against the validity of one of the authorisations issued by the liberty and custody judge, arguing that it did not indicate a specified duration of the operation. According to the Court, a time limit is not required when the decision merely concerns "additional orders specifying the specific technical measures that must accompany the use of this device". This distinction, made by the Court, underscores a broader ambiguity in the legal framework: Does a judicial authorisation pertain to the data capture itself or to the technical operations accompanying it? The difference is not merely semantic, as each type of authorisation is subject to distinct procedural safeguards. The Court concluded that the data capture had been validly authorised by the liberty and custody judge on 30 January 2020, and that the one-month duration began only once the capture became technically operational, i.e., on 1 April 2020. This required no further judicial decision.

In its second decision in March 2023,[21] the Court of Cassation apparently contradicted the dominant narrative surrounding the EncroChat case to date, i.e., its focus on the potential illicit use of decryption techniques and the invocation of national defence secrecy. The defence relied on prior case law from both the Constitu-

tional Council and the Court of Cassation interpreting Article 230-3 CPC, which requires that any decryption measure obtained through technical means be accompanied by sufficient technical information and a certificate attesting their sincerity (see also III.2. above). According to the defence, this requirement should have been respected in this case. Interestingly, the Court of Cassation held that Article 230-3 was inapplicable. After reviewing the case file, including elements not accessible to the defence, it asserted that the data had been captured and processed in clear form, and had never been accessed in an encrypted form. Consequently, no decryption had taken place. In this way, the Court effectively reclassified the case: Despite framing it as a matter of decryption and secrecy in public and legal discourse, the EncroChat operation was, in the Court's view, not an encryption case at all.

6. Scholars' reception

Most of the French academic criticism has focused on the ruling of the Constitutional Council (see above 2.).[22] A central concern is the opacity surrounding the technical means used to decrypt the data. Critics argue that this recourse to secrecy effectively removes key technical information from the adversarial process, undermining the principle of equality of arms. The absence of clear criteria or judicial oversight, either *ex ante* or *ex post*, over the classification of these methods is seen as granting prosecutors a level of discretionary power incompatible with guarantees of a fair trial. The Constitutional Council's justification for upholding this framework has been deemed inadequate, particularly given the potential for abuse and the lack of legal provisions explicitly protecting intelligence techniques from disclosure.

Beyond concerns about secrecy, the decision has also been criticised for its impact on defence rights. Defendants are unable to verify the origin or integrity of the data used against them because they are denied access to the raw files and must rely solely on selected transcripts prepared by investigators. The procedural documents made available, such as the reasoned authorisations and reports on the installation and receipt of decrypted material, are considered inadequate for enabling meaningful scrutiny of the operation's legality and reliability.

The focus on the decision of the Constitutional Council, and consequently the focus on the use of secretive technological methods led most commentators, and the Court of Cassation itself, to overlook other essential issues. Consequently, some French scholars have noted that the legal and constitutional debates surrounding EncroChat in France have largely overlooked the core issue of the data capture operation itself. In particular, regarding the legality principle, given that such operations entail significant intrusion into private life, the legal framework authorising them should be "all the more clear and precise". Especially this point has been largely ignored by the Court of Cassation.[23]

IV. Complaints on the EncroChat Hacking before European Courts

1. EncroChat at the European Court of Justice

In the EncroChat case, the French authorities autonomously undertook the data capture; this meant that authorities in other Member States, such as the German authorities, were requesting data already in the possession of the French authorities. Thus, the EIOs issued were not requests for the execution of a data capture, but for the mere transfer of part of the stored data. This use of EncroChat data in criminal proceedings, obtained within the Joint Investigation Team and through EIOs, gave rise to significant legal controversy especially in Germany.[24]

In March 2022, the German Federal Court of Justice (*Bundesgerichtshof*) held that the Frankfurt Prosecutor's Office was competent to issue EIOs for the purpose of data transmission (a "transfer EIO") under the legal framework of the Directive regarding the European Investigation Order in criminal matters (EIO Directive),[25] and that the transferred data could be used as admissible evidence in criminal proceedings against individuals in Germany.[26] By contrast, the Regional Court of Berlin (*Landgericht Berlin*) questioned the admissibility of evidence for several reasons. The Berlin court found that only a judge (and not a prosecutor) should have issued the EIOs under the existing legal framework, given the seriousness of the interferences with fundamental rights and the absence of individualised suspicions. It further expressed doubts as to whether the EIOs complied with the requirements of necessity and proportionality, considering that the data collection had been broad, indiscriminate, and not linked to any specific case. Additional concerns were raised regarding the ability to challenge the integrity of the encrypted data (impossible to raise in France on grounds of "defence secrecy," see Section III) and regarding the notification obligations under Art. 31 of the EIO Directive. Ultimately, the Berlin court referred a comprehensive set of questions to the ECJ for a preliminary ruling.[27] On 30 April 2024, the ECJ delivered a landmark judgment interpreting the EIO Directive in the context of the EncroChat case.[28]

The questions referred to the ECJ essentially concerned the extent to which a Member State receiving data from another may review how the latter obtained such data. The Berlin Court raised questions about the conditions under which, (1) the data had been collected and (2) a "transfer EIO" could legitimately be issued. As the EIO Directive refers mostly to national law, it imposes few substantive safeguards. The questions referred to the ECJ were largely intended to highlight the absence of stronger guarantees under EU law.

Looking at the first question concerning the authority competent to issue a "transfer-EIO", it is important to note that, under German criminal procedural law, only a judge may order a legal hacking measure as that carried out in France. However, the ECJ departed from the approach, holding that the EIO did not need to be issued by a judge, on the ground that the "transfer EIO" merely sought the transmission of data already collected by the French authorities. In the absence of mandatory judicial authorisation for such transfer between two criminal proceedings at the national level, the EIO could thus be issued by a prosecutor.

With regard to the second question, the Berlin court enquired whether safeguards related to its own provisions on legal hacking, such as the need for an individualised suspicion against the persons targeted by the investigation, and whether the verification of data integrity apply, given that both safeguards are not explicitly provided for in the regulation of legal hacking in France. However, the ECJ barred the issuing state from requiring such safeguards. The ECJ stressed again that the EIO related to the mere transfer of data, not the implementation of legal hacking. Furthermore, as the EIO Directive does not prescribe such requirements, the ECJ declined to create new safeguards.

Nevertheless, the ECJ opened the door to a limited review by the issuing state: Where a "transfer-EIO" appears disproportionate in light of the fundamental rights of the persons concerned, "the court seized of the action brought against the EIO ordering that transmission would have to draw the appropriate conclusions from this as required under national law".[29] In this context, the ECJ referred to Art. 14(7) EIO Directive, according to which rights of the defence and the fairness of proceedings must be upheld, particularly by providing the opportunity to effectively comment on the evidence. If national courts consider these rights to have been violated, data resulting from a "transfer-EIO" can be rendered inadmissible.[30] However, this possibility remains confined to the domestic legal order.

Finally, the ECJ determined the meaning of "interception of telecommunications" as set out in Arts. 30 and 31 EIO Directive. The Court transformed the notion into an autonomous concept of EU law, independent of national definitions. Here, the ECJ interprets the word "interception" broadly, including any infiltration of devices for the purpose of gathering communication data, even internet-based data. As a consequence, in-

terception not only includes the interception of data in transit, but also the mere gathering of stored data, as in the EncroChat case. Hence, if the subject of the operation is located in another Member State, the state from which the interception originates (here: France) must notify each state in which users are located. This notification, deriving from Art. 31 EIO Directive, enables the notified state to request the termination of the measure or to impose conditions, such as additional safeguards, necessary for evidence to be admissible in later proceedings.

Thus, the ECJ largely left significant questions, and particularly the one as to the admissibility of the evidence, entirely to national law and courts. While the German courts seemed wary of the conditions under which the legal hacking took place in France, the ECJ refocused the case in direction of the provisions surrounding the data transfer between criminal proceedings. The ECJ's decision has triggered ample literature from different perspectives, namely EU law, fundamental rights and technical guarantees.[31] Conversely, to our knowledge, the ECtHR's decision, which we will discuss next, remains largely absent from the debate.

2. EncroChat at the European Court of Human Rights

The ECtHR also had the opportunity to rule on the EncroChat case.[32] In this particular instance, the applicants were prosecuted in the United Kingdom. The British authorities had relied on data transferred by the French authorities following a corresponding EIO. Notably, the application before the ECtHR was lodged against France, which collected and transferred the data, rather than against the United Kingdom, which used this data in domestic criminal proceedings. The applicants alleged that France violated their right to privacy, their right to a fair trial, and their right to an effective remedy (Arts. 8, 6 and 13 ECHR). Two specific interferences were at stake:

- The initial collection of data;
- The transfer of the data, with the applicants arguing that the large-scale transmission of data to the United Kingdom constituted a separate violation of their fundamental rights.

The ECtHR declared the application inadmissible, however, and did not examine the merits of the case because domestic remedies had not yet been exhausted (principle of subsidiarity). The Court accepted the French government's argument that the applicants should have used the effective remedies available to them in France before bringing their case to Strasbourg. Notably, reference was made to Article 694-41 CPC, which provides that remedies must be available in France against measures executed pursuant to an EIO whenever similar remedies exist in domestic law for comparable internal measures. In the case at hand, the reference point was the transfer of data already collected from one case file to another, as also highlighted by the ECJ and labelled above as the "transfer-EIO". Although the French criminal procedure code does not expressly provide for a remedy against data transfers, the Court of Cassation has recognised the possibility of an annulment claim (*recours en nullité*) against data transfers between national criminal proceedings within France.[33]

The ECtHR's reasoning is open to two criticisms. The first concerns the accessibility of the remedy: It is far from evident that foreign applicants could reasonably be expected to identify the procedural avenues available under French law without assistance or notification of the collection of their EncroChat data. Secondly, even if such information were accessible, it is uncertain whether the French courts would recognise the applicants' claims, given that they were not directly involved in any criminal proceedings in France. It should be noted that the legal question of access to such remedies is currently being debated in the SkyECC proceedings, another cryptophone case (see Section VI.).

By accepting the inadmissibility argument, the ECtHR missed an opportunity to analyse a measure of legal hacking for the first time. Yet, as the Court itself highlights in para. 102 of the decision, the analysis and use of bulk data as evidence, whether resulting directly from legal hacking or from a transfer of the collected data, qualify as "undoubtedly being the most intrusive [steps] in the process"[34] but these acts were "not among those brought before the Court."[35] Therefore, there is hope that the Strasbourg Court will have the opportunity to revisit the fundamental rights issues in substance, particularly the right to privacy, the proportionality of analysing bulk data in view of the limited safeguards regarding legal hacking (in France), and the proportionality of the data transfer to many other countries.

V. New Complaints on the EncroChat Hacking in France (2025)

Following the ECJ's and ECtHR's decisions, the Court of Cassation issued four decisions related to the EncroChat data capture during the first quarter of 2025.

In January 2025, the Court reaffirmed that circumventing EncroChat's "infrastructure protection system" had allowed investigators to access "the data itself, which was readable in plain text within the files." [36] This means that the data collected was never encrypted and later decrypted by the investigators, as had been already stressed by the Court in its May 2023 decision (see above, section III.5). The Court also reiterated that judicial authorisations concerning the installation of technical measures do not require a time limit, and are not subject to "specific technical requirements." This position in effect excludes judicial authorisations for future data capture from the enhanced safeguards applicable to technical means protected by national defence secrecy.

Despite this limitation, the Court proceeded to assess the proportionality of the data capture operation in light of the ECJ's case law on indiscriminate data retention and access.[37] It concluded that the operation was sufficiently targeted, as authorisation had to be obtained for specific automated data processing systems, such as servers identified by their IP addresses and the terminals and peripherals connected to them. As the measure was limited to EncroChat users (even if all of them), the Court held that it did not constitute mass surveillance. In our view, the Court's analysis reflects a narrow interpretation of the ECJ's data retention case law, which cannot be fully explored in this article. At least, the Court acknowledged a technical safeguard by requiring installation reports for the capture devices to be included in the case file. Importantly, in this context, it clarified that it is the responsibility of the investigating judge, rather than the defendant, to request these reports.

In two subsequent decisions issued in February 2025,[38] the Court of Cassation addressed the procedural safeguards and remedies available to defendants in the context of data capture. As a general rule, individuals may challenge the legality of investigative measures taken prior to their formal indictment within six months of being notified of the indictment (Article 173-1 CPC). This time limit does not apply, however, if the contested operations were not already included in the case file. In the EncroChat proceedings, the data capture was only added to the case file after the defendants had been charged. Against this backdrop, the Court held that it would be unlawful to refuse judicial review of the measure in such cases. Instead, the six-month time limit for contesting the legality of the operation must begin from the date of the defendant's interrogation after the addition of the data capture reports to the case file.

Finally, in March 2025,[39] the Court of Cassation revisited the principle of the right against self-incrimination. In the case at hand, the investigating chamber rejected an appeal challenging the legality of the data capture on the basis that the defendant had denied being an EncroChat user. However, the Court of Cassation over-

turned this reasoning, reaffirming its 2023 case law: A defendant is not required to admit ownership or use of the cryptophone in order to access remedies. Conversely, it is the responsibility of the courts to establish whether the individual is connected to the device under investigation. If the prosecution establishes such a connection, the defendant must be granted access to legal remedy in order to challenge the legality of the data capture.

VI. Potential Next Steps

Although the EncroChat case has attracted considerable attention, the French and European litigation concerning the measures implemented in France remain unsatisfactory in several respects. In particular, the French courts have not fully examined whether legal hacking was necessary and proportionate. This shortcoming may be due to several factors: the novelty, complexity, and sensitivity of the case; as well as procedural choices shifting the debate towards highly technical matters to the detriment of fundamental questions.

At the European level, neither the ECJ nor the ECtHR has yet addressed the substance of the proportionality of the legal hacking carried out in France. They also have not dealt with the implications of these measures for criminal proceedings abroad. Several applications are pending before the ECtHR, which will likely offer the opportunity to revisit the matter. However, as these applications are not directed against France as the "collecting country", the Court in Strasbourg is not going to discuss the proportionality of legal hacking.[40]

Ultimately, EncroChat is no longer an isolated case. Similar questions have emerged in other cryptophone proceedings, most notably in the SkyECC case. This case extends the debate to the crucial issue of whether individuals whose data were collected on French territory but used against them abroad can access remedies in France (see above, section IV.2). Under current French law, such individuals may be denied redress and therefore have no access to domestic remedies. In the SkyECC case, the French Court of Cassation has refused to refer this issue to the Constitutional Council,[41] but instead requested a preliminary ruling from the ECJ.[42] This situation has already given rise to numerous issues concerning the admissibility of evidence in various European countries, which will need to be addressed separately. This is a different story to tell.

Pending these legal and technical challenges, the judicial chronology of data-driven investigations is still unfolding.

---

1. J.-J. Oerlemans and S. Royer, "The future of data driven investigations in light of the Sky ECC operation", (2023) 14(4) *New Journal of European Criminal Law*, 434-458.↩
2. Europol Press Release of 3 December 2024, "International operation takes down another encrypted messaging service used by criminals –<https://www.europol.europa.eu/media-press/newsroom/news/international-operation-takes-down-another-encrypted-messaging-service-used-criminals>. All hyperlinks in this article were last accessed on 8 April 2026. See also C. Riehle and T. Wahl, "Trojan-Encrypted Device Reveals Criminal Activities", (2021) *eucrim*, 106.↩
3. The *Cour de cassation* (Court of cassation) is the highest court in the French judiciary. It has jurisdiction to hear cases in civil, commercial, social or criminal matters. The Court only reviews questions of law (but not questions of fact) and bears ultimate responsibility for a uniform interpretation and application of statutory law throughout France. It also filters out appeals challenging the constitutionality of statutes before forwarding them to the *Conseil constitutionnel* (Constitutional Council).↩
4. This chronology is based on dates extracted from the following documents: C. Thorfinn, "L'enquête EncroChat en France - Genèse du dossier et chronologie de la procédure EncroChat", *Policy Commons*, 2 July 2020, <https://policycommons.net/artifacts/1918483/lenquete-encrochat-en-france/2670254/> ; ECtHR, 24 September 2024, *A.L. et E.J. v. France (dec.)*, Appl. nos. 44715/20 and 47930/21; ECJ, 30 April 2024, Case C-670/22 , *Criminal proceedings against M.N. [Encrochat]*; Eurojust, *Annual Report 2020: Criminal justice across borders in the EU*, 23 March 2021, <https://www.eurojust.europa.eu/sites/default/files/assets/2021_04_14_eurojust_annual_report_2020_final.pdf>; Europol, *Internet organised crime threat assessment (IOCTA) 2020*, <https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf>; Cour de cassation, Chambre criminelle, 14 February 2023, 22-84.288.↩
5. Eurojust Press Release of 27 June 2023, "Dismantling encrypted criminal EncroChat communications leads to over 6 500 arrests and close to EUR 900 million seized", , <https://www.eurojust.europa.eu/news/dismantling-encrypted-criminal-encrochat-communications-6-500-arrests-900-eur-seized>; see also C. Riehle, "Results of EncroChat Take-Down", (2023) *eucrim*, 163-164.↩
6. Law no. 2011-267 of 14 March 2011 on guidelines and planning for internal security performance (*loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure*).↩

7. B. Roussel, *Les investigations numériques en procédure pénale*, PhD thesis, Université de Bordeaux, 7 July 2020, pp. 199-200, online <https://theses.hal.science/tel-02947825>; M. Quéméner, "Fasc. 1105 : La preuve numérique dans un cadre pénal", *JurisClasseur Communication*, Lexis-Nexis, 8 November 2022 ; E. De Marco, "La captation des données", in: K. Blay-Grabarczyk et al. (eds.), *Le nouveau cadre législatif de la lutte contre le terrorisme à l'épreuve des droits fondamentaux*, Institut Universitaire Varenne, Collection "Colloques & Essais", no. 44, 2017, p. 88.↩
8. CNIL, *Délibération portant avis sur un projet de décret modifiant le décret n°2015-1700 du 18 décembre 2015 relatif à la mise en œuvre de traitements de données informatiques captées en application de l'article 706-102-1 du code de procédure pénale*, September 2019, demande d'avis n°18004354.↩
9. The liberty and custody judge is a judicial authority responsible for authorising intrusive investigative measures during a preliminary investigation. They perform a role similar to that of an investigating judge (*juge d'instruction*), but specifically in the context of safeguarding individual liberties prior to the opening of a formal judicial inquiry (*instruction*).↩
10. The authority responsible for granting the authorisation will depend on the framework of the investigation.↩
11. Cour de cassation, Chambre criminelle, 1 February 2022, 21-85.148. The same issues reached the Court again in April 2022: Cour de cassation, Chambre criminelle, 5 April 2022, 21-85.763.↩
12. ECtHR, 23 November 2010, *Moulin v. France*, Appl. no. 37104/06.↩
13. Article 230-3 CPC whose crucial passage reads: « Sous réserve des obligations découlant du secret de la défense nationale, les résultats sont accompagnés des indications techniques utiles à la compréhension et à leur exploitation ainsi que d'une attestation visée par le responsable de l'organisme technique certifiant la sincérité des résultats transmis. »↩
14. Conseil constitutionnel, 4 April 2022, *M. Saïd Z.*, no. 2022-987 QPC.↩
15. However, the Constitutional Council did not address the meaning of the "sincerity" requirement. Indeed, the concept of "sincerity" is not used elsewhere in the legal framework, neither in the criminal procedure code nor in the Law no. 78-17 of 6 January 1978 "on information technology, files and civil liberties" (*Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*.). The latter was, *inter alia*, amended to transpose the EU's 2016 Law Enforcement Directive (Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, OJ L 119, 4.5.2016, 89). On the one hand, the concept could mean that the results, i.e., the selection from the raw data, must be certified sincerely, as not to exclude exculpatory evidence. On the other hand, and on a different note, "sincerity of the results" could refer to the integrity or authenticity of the data from a forensic perspective.↩
16. For an analysis in the French literature, see J. Pidoux, "Nullités en matière de captation de données informatiques : précision et rappel sur la qualité à agir du requérant Crim. 25 oct. 2022, FS-B, n° 21-85.763", *Dalloz Actualité*, Dalloz, 15 November 2022 ; J. Pidoux, "Premiers contrôles par la Cour de cassation de procédures ouvertes à la suite de l'opération dite « EncroChat » Crim. 11 oct. 2022, F-D, n° 21-85.148 Crim. 25 oct. 2022, FS-B, n° 21-85.763", *Dalloz Actualité*, Dalloz, 14 November 2022.↩
17. Cour de cassation, Chambre criminelle, 11 October 2022, 21-85148.↩
18. Cour de cassation, Chambre criminelle, 25 October 2022, 21-85.763.↩
19. The ECtHR relied particularly on this decision when assessing the existence of a remedy in France against legal hacking (see Section III.2), ECtHR, *A.L. et E.J. v. France (dec.)*, *op. cit.* (n. 4), § 141.↩
20. Cour de cassation, Chambre criminelle, 14 February 2023, *op. cit.* (n. 4).↩
21. Cour de cassation, Chambre criminelle, 10 May 2023, 22-84.475.↩
22. C. Ascione Le Dréau, "QPC dans l'affaire EncroChat : des jours heureux pour Big Brother ? Décision rendue par Conseil constitutionnel", *Actualité juridique Pénal*, Dalloz, 2022, p. 376 ; X. Laurent, "Captation de données numériques : une étape significative dans la consolidation du régime de l'article 706-102-1 du code de procédure pénale", *Dalloz IP/IT*, Dalloz, 2022, p. 578 ; M. Lassalle, "L'affaire EncroChat", *Recueil Dalloz*, Dalloz, 2023, p. 1833 ; L. Saenko, "Captation de données informatiques et secret-défense : une arme sans contrôle ?", *Lexbase pénal*, 2022, no. 48.↩
23. M. Lassalle, "L'affaire EncroChat", *op. cit.* (n. 22), p. 1833.↩
24. See T. Wahl, "EncroChat Turns into a Case for the CJEU", (2022) *eucrim*, 197-198. In this part on the EncroChat case before the ECJ, we exclude the following ECJ order from our analysis, as it does not concern the French procedure: ECJ, 4 July 2024, Case C-288/24, *Criminal proceedings against M.R.* For this decision, see T. Wahl, "Berlin Regional Court's EncroChat Battle – Third Round, (2024) *eucrim*, 86-87.↩
25. Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014, 1.↩
26. For a summary of this decision in English, see T. Wahl, "Germany: Federal Court of Justice Confirms Use of Evidence in EncroChat Cases", (2022) *eucrim*, 36-37.↩
27. T. Wahl, (2022) *eucrim*, *op. cit.* (n. 24), 197-198.↩
28. ECJ, *Criminal proceedings against M.N. [Encrochat]*, *op. cit.* (n. 4). For the summary of this judgment in eucrim: T. Wahl, "ECJ Ruled in EncroChat Case", (2024) *eucrim*, 40-43.↩
29. ECJ, *Criminal proceedings against M.N. [Encrochat]*, *op. cit.* (n. 4), para. 103.↩
30. ECJ, *Criminal proceedings against M.N. [Encrochat]*, *op. cit.* (n. 4), paras. 104-105. On this aspect, the ECJ relied on its previous case law, ECJ, 2 March 2021, Case C-746/18, *Criminal proceedings against H K vs Prokuratuur*.↩
31. See L. Bachmaier Winter, "The fight for fair trial rights and the paradigm shift in evidence: from liberalism to mass surveillance in criminal proceedings in Europe", (2025) 11(1) *Revista Brasileira de Direito Processual Penal*; S. Steinborn and D. Swieczkowski, "Verification in the Issuing State of Evidence Obtained on the Basis of the European Investigation Order", (2023) 54 *Rev. Eur. & Comp. L.*, 169-194 ; A. Sachoulidou, "The Court of Justice in *Staatsanwaltschaft Berlin v. M.N.* (EncroChat): From cross-border, data-driven police investigations to evidence admissibility", (2024) 31(4) *Maastricht Journal of European and Comparative Law*, 510-520; M. Nicolas-Gréciano, "Affaire EncroChat devant la CJUE : premiers accrocs aux droits fondamentaux", *La Gazette du Palais*, 9 July 2024, vol. 23, 18-21 ; M. Lassalle, "La phase supranationale de l'affaire EncroChat", *Recueil Dalloz*, 3 July 2025, p. 1194 ; A. Hoxhaj, "The CJEU Ruled that the EncroChat Data can be Admissible Evidence in the EU", (2025) 16 *European Journal of Risk Regulation,* 1567-1579; A. Caiola, "Un arrêt fondateur entre efficacité et protection des droits. La décision d'enquête européenne en matière pénale et quelques précisions jurisprudentielles sur la transmission et l'utilisation de preuves", (2024)(2) *Law & European Affairs*, 341-352;

V. Bajović and V. Ćorić, "Encrochat and SkyECC Data as Evidence in Criminal Proceedings in Light of the CJEU Decision", (2025) 33 *European Journal of Crime, Criminal Law and Criminal Justice*, 235-262.↩

32. ECtHR, *A.L. et E.J. c. France (dec.)*, *op. cit.* (n. 4).↩
33. ECtHR, *A.L. et E.J. c. France (dec.)*, *op. cit.* (n. 4), para. 82. Cour de cassation, Chambre criminelle, 25 octobre 2022, 21-85.763.↩
34. Referring to ECtHR, 25 May 2021, *Big Brother Watch and Others v. the United Kingdom*, Appl. nos. 58170/13, 62322/14, 24960/15.↩
35. The translation is made by the authors from the official French text of the decision.↩
36. Cour de cassation, Chambre criminelle, 7 January 2025, 24-82.908.↩
37. See for instance: ECJ, 8 April 2014, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*; ECJ, 6 October 2020, Joined Cases C-511/18, C-512/18, and C-520/18, *La Quadrature du Net and Others*; ECJ, 5 April 2022, Case C-140/20, *G.D. v. Commissioner of An Garda Síochána*; ECJ, 20 September 2022, Joined Cases C-793/19 and C-794/19, *Bundesrepublik Deutschland v SpaceNet AG and Telekom Deutschland GmbH*; ECJ, 30 April 2024, Case C-470/21, *La Quadrature du Net and Others v Premier ministre and Ministère de la Culture*.↩
38. Cour de cassation, Chambre criminelle, 4 February 2025, 24-80.567; Cour de cassation, Chambre criminelle, 4 February 2025, 24-80.411.↩
39. Cour de cassation, Chambre criminelle, 26 March 2025, 21-83.122 & 23-87.113.↩
40. Joint Defense Team, "Update 2025: EncroChat and SkyECC Legal Developments Across Europe"30 October 2025, <https://www.joint-defense-team.com/post/encrochat-skyecc-legal-update-2025>.↩
41. Cour de cassation, Chambre criminelle, 3 June 2025, 25-80.792 ; Cour de cassation, Chambre criminelle, 3 June 2025, 25-80.497. See also Cour de cassation, Chambre criminelle, 18 November 2025, 25-82.065 ; Cour de cassation, Chambre criminelle, 31 March 2026, 25-82.068.↩
42. Cour de cassation, Chambre criminelle, 16 September 2025, 24-84.262 (referenced at the ECJ as Case C-625/25, "*Prudniez*").↩

About eucrim

eucrim is the leading journal serving as a European forum for insight and debate on criminal and "criministrative" law. For over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU's financial interests – a key driver of European integration in "criministrative" justice policy.
Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of legal and policy developments across Europe.
All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.
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