European Journal of Risk Regulation (2025), 1–13
doi:10.1017/err.2025.10047

CAMBRIDGE UNIVERSITY PRESS

CASE NOTES

The CJEU Ruled that the EncroChat Data can be Admissible Evidence in the EU

Andi Hoxhaj

Lecturer in Law, The Dickson Poon School of Law, King's College London, UK
Email: andi.hoxhaj@kcl.ac.uk

Abstract

The Court of Justice of the European Union ruled, in Case C-670/22 *Staatsanwaltschaft Berlin* v *M.N. (EncroChat),* that a public prosecutor's office may also request a European Investigation Order without a court order to obtain encrypted data from another EU Member State, and use it as evidence in cross-border crimes and criminal cases. The decision resolved a dispute between German courts regarding the compatibility and legality of gathering and using data from an encrypted communication network named "EncroChat," in a drug trafficking and cybercrime investigation by the French authorities as evidence in criminal cases. The case note analyses how the CJEU interprets the European Investigation Directive regarding the admissibility of evidence in court and assesses whether the ruling adequately safeguards the defendant's rights and provides a fair trial under EU law. The case note analyses the implications of *C-670/22-M.N. (EncroChat)* for cross-border crime prosecution and judicial cooperation across the EU, and it discusses how it could lead to the establishment of new modality for evidence admissibility under the European Investigation Directive.

1. Introduction

The French law enforcement agency, La Gendarmerie Nationale, discovered in 2017 that organised crime networks involved in cybercrime and illegal drug trafficking used a modified mobile phone and online network called EncroChat, which came with four pre-installed apps for untraceable encrypted messaging, internet-based voice calls, e-mail messages, and notetaking.[1] EncroChat mobiles could be purchased on the black market for about EUR 1000 each, with a six-month online global subscription for EUR 1500. The law enforcement agency found the EncroChat network used a French-based internet service provider called "OVHcloud." Its servers were also based in France, and allowed users all around the world to communicate using their encrypted mobile phones.[2] France initially shared the information with the Netherlands, and with the assistance of Eurojust and Europol, the two countries formed a joint investigation team (JIT). French and Dutch law enforcement investigators were able to hack the EncroChat server, by inserting Trojan

[1] J J Oerlemans, and D A G van Toor, "Legal Aspects of the EncroChat Operation: A Human Rights Perspective", (2022) 30(3-4) European Journal of Crime, Criminal Law and Criminal Justice 309–328.

[2] G Sagittae, "On the lawfulness of the EncroChat and Sky ECC-operations", (2023) 14(3) New Journal of European Criminal Law 269–72.

software which then uploaded all the communications of EncroChat users to the JIT – who were thus able to read the user chat messages and phone conversations in real time.[3]

In 2020, the JIT found that EncroChat was one of Europe's largest encrypted digital communication platforms, with most of its members allegedly engaging in illegal activities. The Europol's Internet Organised Crime Threat Report 2021 describes EncroChat as a "grey infrastructure that, provided optimally, conceals offenders from law enforcement authorities."[4] In 2023, the JIT presented an initial assessment of the results of the investigation. Based on the information collected from EncroChat data, investigators were able to intercept, share and to analyse over 120 million EncroChat messages and phone calls sent by over 60,000 users in more than 120 countries worldwide, as well as avert violent attacks, attempted murders, corruption and large-scale drug transports.[5] Europol also exchanged information with law enforcement agencies in other countries based on EncroChat users' geographic locations. According to Europol, EncroChat data has so far led to nearly 6500 arrests, the confiscation of almost EUR 900 million in criminal finances, and 7134 years in prison for offenders.[6]

However, in several EU and non-EU Member States, courts are debating whether EncroChat dates can be considered lawful and acceptable evidence, as it has proven difficult for the defence to obtain information about how the evidence was collected by JIT, and how it was shared with EU and non-EU Member States, as well as effectively verifying some of the EncroChat users because they were not registered under any name, and determining which investigatory powers were used to collect these data. In April 2022, the German Federal Court of Justice *(Bundesgerichtshof),* the country's highest court for civil and criminal actions, ruled that the EncroChat data provided by French authorities was lawful and acceptable evidence.[7] However, the Regional Court of Berlin disagreed with the Federal Court of Justice's decision. The Berlin Court argued that data could not be used as evidence, because only a court, not a public prosecutor, can issue a European Investigation Order (EIO) under the Directive, and obtain data from French authorities, and that there were some infringements on the right to privacy of telecommunications and the right to a fair trial.[8] The Berlin Court requested a preliminary opinion from the CJEU on whether the German Public Prosecutor's Office breached EU law by accessing EncroChat data, how any such breach affects how the data could be used in criminal proceedings, and whether a public prosecutor's office can issue an EIO without a court order.[9]

The case note will begin with a summary of the facts (II), followed by the Advocate General's opinion (III) and the CJEU's decision (IV). The case note will then go into greater detail on the CJEU's interpretation of the EIO (V), and how the court appears to enable those that favour the usability of the data from the EncroChat hacking operation without a

[3] 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 510–20.

[4] Europol, "Internet Organised Crime Threat Assessment," 19 December 2023, <https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021>.

[5] Europol, "Dismantling encrypted criminal EncroChat communications leads to over 6500 arrests and close to EUR 900 million seized, 27 June 2023, <https://www.europol.europa.eu/media-press/newsroom/news/dismantling-encrypted-criminal-encrochat-communications-leads-to-over-6-500-arrests-and-close-to-eur-900-million-seized>.

[6] Europol, "Operation Emma: Dismantling EncroChat, an encrypted phone network widely used by criminal networks," 29 June 2023, <https://www.europol.europa.eu/operations-services-and-innovation/operations/operation-emma>.

[7] T Wahl, "Germany: Federal Court of Justice Confirms Use of Evidence in EncroChat Cases", (2021) The European Criminal Law Associations' Forum (eucrim), <https://eucrim.eu/news/germany-federal-court-of-justice-confirms-use-of-evidence-in-encrochat-cases>.

[8] Case C-670/22 *Staatsanwaltschaft Berlin* v *M.N.*, (EncroChat) (2024) ECLI:EU:C:2024:372.

[9] Ibid, § 29.

court order. The case note will discuss how the CJEU assessed the criteria under the EIO to obtain existing information, and decided that these criteria should be lower than in cases where an EIO was authorised to start the collection of evidence. The case note also discusses concerns raised by defence lawyers, NGOs, and academics about whether the CJEU's decision has made it more difficult for defence lawyers to defend clients against whom criminal proceedings were initiated as a result of the surveillance, and if it has had an adverse effect on ensuring a fair trial under EU law. The case note observes that the CJEU appears to favour the EU's strategy to combat organised crime within the Union – prioritising the interpretation of EU law in favour of the police and prosecution using EncroChat data during criminal investigations – over concerns expressed by defence lawyers, NGOs, and academics about meeting the human rights standard on the right to a fair trial.

2. Facts of the case

In early 2020, the JIT informed several EU Member State law enforcement agencies that it had decrypted the EncroChat network, finding that 63.7 per cent of the conversations and data was used for criminal purposes, while 36.3 per cent was either partially inactive or had not been fully evaluated.[10] After examining initial data, JIT surveillance discovered that EncroChat users were based in more than 120 countries, including several EU and non-EU Member States, and the alleged crimes were of a cross-border nature. Many states enquired about the EncroChat data. This included Germany, where there were approximately 4600 users, and the German Public Prosecutor's Office requested the transmission of intercepted data from the French investigators through European Investigation Orders (EIOs) – under Directive 2014/41 (EIO Directive) in 2020 for pre-trial proceeding.[11] An EIO is a judicial order from one EU Member State to another to share or transfer evidence.[12] Subsequently, Frankfurt's General Public Prosecutor launched an investigation into "unknown persons."[13]

In June 2020, a French judge granted the EIO request to send EncroChat data related to Germany for use in criminal investigations. The data proved useful as information for the prosecution, as encrypted messages and phone conversations exchanged by suspects using the EncroChat network to arrange drug trafficking and other illegal operations revealed new insights and filled in gaps in some of the suspects' investigations. After receiving the data, the German authorities opened over 2250 investigations and arrested over 750 EncroChat users for illegal activities, and several German courts convicted offenders by using EncroChat data as lawful and acceptable evidence in criminal procedures.[14] In a case heard by the Higher Regional Court of Hamburg in March 2021, a defendant appealed the conviction of five years in prison for drug trafficking and the confiscation of proceeds

[10] G Sagittae, "On the lawfulness of the EncroChat and Sky ECC-operations", (2023) 14(3) New Journal of European Criminal Law 269–72.

[11] T Wahl, "Dismantled Encryption Networks: German Courts Confirmed Use of Evidence from EncroChat Surveillance," (2021) The European Criminal Law Associations' Forum (eucrim) <https://eucrim.eu/news/dismantled-encryption-networks-german-courts-confirmed-use-of-evidence-from-encrochat-surveillance/>.

[12] A I Szabo, "The European investigation order – an instrument of cooperation for a stronger European union", (2019) Centre for European Studies Working Papers 3, <https://www.proquest.com/working-papers/european-investigation-order-instrument/docview/2313055463/se-2>.

[13] D Klein, "Germany Cracks Down on Organized Crime after EncroChat Bust," Organized Crime and Corruption Reporting Project, 3 October 2022, <https://www.occrp.org/en/news/germany-cracks-down-on-organized-crime-after-encrochat-bust>.

[14] D Brombacher, "Challenge accepted? Germany steps up against organized crime," Global Initiative Against Transitional Organized Crime, 22 May 2024, <https://globalinitiative.net/analysis/germany-organized-crime-cocaine-trade/>.

exceeding EUR 70,000. The defendant argued that the German authorities should not have used the EncroChat data as evidence, because it was illegally gathered and transferred from France to Germany. The case reached the Federal Court of Justice, which issued the first Supreme Court decision on the propriety of using EncroChat data as lawful and acceptable evidence in criminal proceedings.[15]

Based on previous rulings, the Federal Court of Justice (FCJ) stated that Section 261 of the German Code of Criminal Procedure allows authorities to evaluate evidence obtained through mutual legal assistance, and that making use of evidence collected abroad is legal under German law.[16] The FCJ went on to suggest that Germany might have approved the same EncroChat surveillance as France had, if it had reasonable suspicion about illegal activities taking place in Germany.[17] Furthermore, there were no violations of fundamental human rights, fundamental constitutional rights, or EU law, and the EIO request was legal. The Court explained that if the use of EncroChat data might involve an encroachment on the secrecy of telecommunications, as protected by Art. 10 of Basic Law, the principle of proportionality must be applied. This principle – recognised under the German Constitution, the Code of Criminal Procedure, and the Narcotics Act – allows the use of personal data, including an online search or acoustic surveillance, if there is reasonable suspicion about illegal activities taking place in the country.[18] The FCJ therefore ruled that EncroChat data could be used as evidence in criminal proceedings.

The Regional Court of Berlin disagreed with the FCJ's ruling, arguing that only a court, not a public prosecutor (without a court order or approval), could issue an EIO – and therefore, the EncroChat data should not be used as evidence.[19] Unlike other German regional courts, Berlin suspended a drug trafficking prosecution in October 2022, by referring various questions to the Court of Justice of the European Union (CJEU). The judges in Berlin asked the CJEU 14 questions, which can be summarised as follows within three categories: (a) EIO admissibility under Article 6(1) EIO Directive; (b) interpretation of Article 31 EIO Directive, which governs telecommunications surveillance without technical assistance; and (c) potential EU law infringement and national criminal proceedings.[20]

The Berlin Regional Court argued that the evidence violated the EU criteria for effectiveness and equivalence, which limit EU Member States' procedural jurisdiction over evidence.[21] Furthermore, the Court argued that the law enforcement agencies lacked transparency surrounding the gathering of the EncroChat data, because France's technical methods were not fully disclosed, making it unable to evaluate the integrity of the data and its use as acceptable evidence in court.[22] Moreover, the Court argued that the EU and German law enforcement agencies did not allow full access to the EncroChat data by the defence counsel, thereby limiting fact-finding by the defence lawyers[23] – thereby undermining a fair trial.

Similarly, a number of non-governmental organisations (NGOs), defence lawyers, and academics expressed misgivings about the rule of law and a breach of the right to a fair

[15] T Wahl, "Germany: Federal Court of Justice Confirms Use of Evidence in EncroChat Cases," (2021) The European Criminal Law Associations' Forum (eucrim), <https://eucrim.eu/news/germany-federal-court-of-justice-confirms-use-of-evidence-in-encrochat-cases/>.

[16] Ibid, § 36.

[17] Ibid, § 36.

[18] Ibid, § 37.

[19] A Sachoulidou, note 3.

[20] Case C-670/22 Opinion of Advocate General Tamara Ćapeta: *Staatsanwaltschaft Berlin* v *M.N.*, (EncroChat) (2023) ECLI:EU:C:2023:817.

[21] T Wahl, "EncroChat Turns into a Case for the CJEU," (2022) The European Criminal Law Associations' Forum (eucrim), <https://eucrim.eu/news/encrochat-turns-into-a-case-for-the-cjeu/>.

[22] Ibid, §§ 197–8.

[23] Ibid, §§ 197–8.

trial in Germany, echoing many of the Berlin Court's concerns about the use of EncroChat data as acceptable and lawful evidence.[24] They voiced concern about the prosecution's potential misinterpretation of EncroChat as evidence, given the difficulty of identifying the users, and the particular difficulties in verifying the data's accuracy, credibility and reliability. Additionally, they noted that the data was collected in secret, and the French judges who authorised the hacking were not provided with the full information and technical issues involved in its broader recording.[25] The information provided by various law enforcement agencies during the prosecution was inconsistent, and in some cases, the prosecution refused to provide the full data. Finally, opponents expressed concern that the hacking of EncroChat violated the right to respect for private life, family life, the right to freedom of expression, and the right to personal data protection – the authorities hacked all users, and their fundamental rights were violated because not all users were engaged in criminal activity.

These concerns have been widely shared in the legal debate in over 120 countries indicted as using EncroChat, and their legality and integrity as evidence have become major points of contention.[26] In October 2023, Advocate General Tamara Ćapeta provided an opinion on a preliminary ruling in the much-anticipated EncroChat data case, which will be explained in the following section.

3. The advocate general's opinion

In October 2023, Advocate General (AG) Tamara Ćapeta presented an opinion and response to the Berlin court's enquiries. The AG's opinion does not address the legality of French interception procedures or the evidence-gathering methods any EU Member States, leaving countries to decide if EncroChat data can be used in court under their own domestic laws and practices.[27] However, the AG suggested that the opinion does advise EU Member States on how to transfer evidence between EU Member States in accordance with EIO Directive;[28] she also stated the importance of the principle of mutual recognition under EU law, requiring EU Member States to recognise that a French interception operation was legal, if it was granted by a French court.[29]

Advocate AG grouped the 14 questions into five sections, including the first (i) section on EIO requirements and evidence transfer by a competent authority.[30] The Berlin Court claimed that only courts can issue EIOs, not a public prosecutor. Under Article 6(1)(a) and (b) EIO Directive, the AG clarified that public prosecutors can issue EIOs and be considered competent authorities for evidence transfer, because EU legislation does not require a judge's order.[31] A judge, court, investigating magistrate, or public prosecutor qualified to handle the case are all considered "issuing judicial authorities" under

[24] A Kanakakis, "The EncroChat Judgment (Case C-670/22, MN): CJEU Steering a Bold Course through the Symplegades of Evidence Admissibility," UK Association for European Law, 1 July 2024, <https://ukael.org/2024/07/01/the-encrochat-judgment-case-c-670-22-mn-cjeu-steering-a-bold-course-through-the-symplegades-of-evidence-admissibility/>.

[25] See, "EnroChat Letter of Concern," Fair Trials, 18 February, <https://www.fairtrials.org/app/uploads/2022/02/EnroChat_LetterofConcern.pdf>.

[26] J J Oerlemans, and DAG van Toor, "Legal Aspects of the EncroChat Operation: A Human Rights Perspective", (2022) 30(3-4) European Journal of Crime, Criminal Law and Criminal Justice 309-328.

[27] Case C-670/22 Opinion of Advocate General Tamara Ćapeta: Staatsanwaltschaft Berlin v M.N., (EncroChat) (2023) ECLI:EU:C:2023:817.

[28] Ibid, § 5.

[29] Ibid, § 24.

[30] Ibid, § 23.

[31] Ibid, § 67.

Article 2(c)(1) of the EIO Directive – therefore, the public prosecutor can request evidence transfers using an EIO.[32]

In the second (ii) section of the opinion, the AG took a more nuanced approach to need and proportionality, arguing that under Article 6(1)(a) EIO Directive, national authorities must review and decide on the sort of investigation methods and surveillance used to monitor a suspect.[33] The AG went on to explain that any serious interference with fundamental rights and freedoms, such as requests for access to a network service provider and telecommunications data, must be justified by a significant public interest, which can only be determined by a national court. Referring to *C-746/18 – Prokuratuur* case, the AG explained that a French court granted permission to intercept EncroChat data;[34] therefore, the proportionality criteria had already been evaluated by an impartial and independent body.

Relating to the third (iii) section, over the lawfulness of using the EncroChat data collected by the French authority in a criminal proceeding in another EU Member State, the AG suggested that that any EU Member States court may not contest the lawfulness of the French authority's investigation methods if their domestic court have approved it. The AG strongly argued that questioning another EU Member State's judicial process in criminal proceeding would undermine respect for the principle of mutual recognition, which is long established under EU law and practice[35] – but added that it remains a matter for Germany whether or not it uses these data as evidence in court.

In the fourth (iv) section, the AG evaluated the questions over the application of Article 31 of the EIO Directive, and explained that the French authorities had an obligation to notify Germany of EncroChat communications as potential evidence,[36] given the cross-border nature of criminality that its users were allegedly committing. According to AG, France was required under Article 31 to alert German authorities, after identifying a high number of EncroChat users in Germany who were engaging in criminal activity. According to the AG, the EIO Directive does not indicate which body to notify (courts, prosecutor or police).[37] However, France was required to notify the authorities of offences in other EU Member States, and it was then for German authorities to decide whether the courts or prosecution or police would submit the EIO, based on their domestic laws and practices.

In the last (v) section, the AG suggested that the acceptance and validity of EIO-obtained evidence in criminal proceedings should be decided in accordance with the domestic laws of each EU Member State, being responsible for their own criminal processes and strategies, and ensuring a fair trial based on long-standing ECtHR case law.[38] The AG concluded that each EU Member State must safeguard the right to a fair trial and respect for citizens' fundamental rights and liberties in criminal procedures, as they are bound to do by Article 14(7), sentence II of the EIO Directive[39] to protect defence rights and promote procedural fairness in criminal proceedings.[40] In other words, to guarantee a fair process, the EncroChat data must be fully shared with the defence counsel.

The AG's opinions are not legally binding, but this interpretation indicates that EU law regards the EIO as an important tool which supports the facilitation of judicial cooperation in criminal matters at the EU level. The AG also recommends that no court or law enforcement agency in an EU Member State should impose any new restrictions on the use

[32] Ibid, § 36.
[33] Ibid, § 28.
[34] Ibid, § 92.
[35] Ibid, § 49.
[36] Ibid, § 104.
[37] Ibid, § 112.
[38] Ibid, § 123.
[39] Ibid, § 119.
[40] Ibid, § 123.

of EIO, as the transfer of information could be beneficial for verifying or establishing evidence in criminal cases. The AG also noted that ensuring the right to a fair trial is crucial, and, if approval has been received from a court in an EU Member State, disagreements between different judicial bodies regarding investigative procedures should not undermine any investigation by another EU Member State. The next section explains the CJEU's decision, which followed the AG's opinion.

4. The CJEU's judgment

The CJEU mostly followed the AG's opinion,[41] with some slightly different interpretations on the right to a fair trial, and answered the Berlin Court's[42] questions as follows:

4.1. Is it required for a judge to issue the EIO?

To answer question (i), the CJEU agreed with the AG that a public prosecutor may order the transmission of evidence by using EIO Proceedings (paras. 69–77).[43] The CJEU held that the EIO Directive Arts. 2(c) and 6(1) may also include public prosecutors, under the meaning of "judicial authority," similar to a judge or court, who may authorise EIOs and can do so without a court order, if it is to request a transmission of evidence from another EU Member State.[44]

4.2. Under which conditions could the EIO be issued?

The CJEU answered questions (ii) and (iii) together, noting that the necessity and proportionality test of an EIO hinges on national law. The CJEU says that Article 6(1)(b) of the EIO Directive does not stipulate that the measures undertaken in the executing state need to meet the same substantive conditions as similar measures in the issuing state.[45] As a result, the body that issued the EIO cannot challenge the legality of the methods used to collect EncroChat data, because that would violate the EU principle of mutual recognition in criminal proceedings.[46] Against this backdrop, the CJEU 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 with respect to each person concerned exists if no such requirement arises under the national law;[47]

Given that the subsequent criminal proceedings guarantee the right to a fair trial, the inability to verify the integrity of the data gathered by the interception measure is irrelevant.[48]

In other words, the CJEU suggested that France gathered evidence on its territory and adhered to its own laws and procedures. Germany's questioning of the French authorities' methods and procedures for gathering the EncroChat data is irrelevant, as it undermines the EU principle of mutual recognition in judicial cooperation in criminal matters. However, the CJEU said that legal remedies against the EIO shall be available (Article 14 EIO Directive).[49] It also said that if a national court finds that a party cannot appropriately

[41] Case C-670/22 *Staatsanwaltschaft Berlin* v *M.N.*, (EncroChat) [2024] ECLI:EU:C:2024:372.
[42] Ibid, § 59.
[43] Ibid, § 69.
[44] Ibid, § 88.
[45] Ibid, § 84.
[46] Ibid, § 99.
[47] Ibid, § 87.
[48] Ibid, § 90.
[49] Ibid, § 102.

comment on a relevant piece of evidence sent through an EIO – thus, identifying an infringement of the right to a fair trial – it can discard that evidence to stop the infringement.[50] Thus, the CJEU held that the EIO Directive allows national courts to assess respect for the parties' fundamental rights to ensure the right to a fair trial, but it is up to the national courts to make that decision.

4.3. Who must be notified under EIO Directive Article 31?

In its response to question (iv), the CJEU agreed with the AG, albeit with slightly broader reasoning over the notification process, and clarifying whether an internet-based communication service such as EncroChat constitutes an "interception of telecommunications" within the meaning and objective of Article 31 of the Directive, and if so, whether the interception must be authorised by a court.[51]

The CJEU interpreted that the concept of "telecommunications" in Article 31 can also include internet-based communication services such as EncroChat or another similar network, and therefore, infiltration for the purpose of data collection does fall under the meaning of "interception of telecommunication." The CJEU went on to clarify that the authorities in the EU Member State executing the interception must have authorised the wording of Article 31(1) (competent authority).[52] However, the Court leaves it up to EU Member States to notify their counterparts about the evidence as they see fit – if, for example, France cannot identify the competent authority in Germany (prosecutor, office, or courts).

4.4. Does EU law require the exclusion of unlawfully obtained evidence?

The CJEU slightly varied with the AG in its response to question (v). While recognising that domestic law usually regulates evidence admissibility in criminal proceedings, the CJEU stated that Article 14(7) of the EIO Directive requires Member States to ensure fair trial rights in EIO related procedures.[53] The CJEU based this reasoning on its previous rulings in *C-746/18 – Prokuratuur* and joined cases *C-511/18, C-512/18 and C-520/18 – La Quadrature du Net and Others*.[54] However, the CJEU went on to explain that the principle of procedural autonomy (that empowers EU Member States to safeguard the right to a fair trial and respect for citizens' fundamental rights and liberties in criminal procedures) derives from EU law and ECtHR case law. However, this rule has two primary limitations:

The principle of equivalence states that national laws should not be less favourable than those governing equivalent domestic actions.

In addition, the principle of effectiveness states that national rules should not make exercising rights granted by EU law impossible or difficult.

In other words, if an EU Member State court finds that a party is unable to effectively comment on an important piece of evidence obtained through an EIO, the court may consider it as a violation of the right to a fair trial, and exclude the evidence to prevent such a breach.[55] The CJEU examined this further, explaining that under EIO Directive Article 14(7) concerning criminal proceedings against a person suspected of committing a criminal offence, EU Member States courts can disregard evidence if defence counsel is

[50] Ibid, § 106.
[51] Ibid, § 108.
[52] Ibid, § 115.
[53] Ibid, § 115.
[54] Ibid, § 129.
[55] Ibid, § 130.

unable to comment sufficiently for the purpose of defence (e.g., without full access to EncroChat data likely to have a preponderant influence on the outcome of the case).[56]

5. Comment

The first impression of CJEU ruling in *C-670/22 – M.N. (EncroChat)* seem to be supportive of the hacking of EncroChat data and their use in court; Advocate General Ćapeta's opinion suggests that the justifications against their use owing to EU law violations are weak.[57] However, the AG and the CJEU reformulated the main question of the Berlin Court, and focused on whether a prosecution office may issue an EIO to transfer evidence without a judge's approval. In short, it made the case about the interpretation of the EIO and tried to clarify its application – avoiding the questions over the legality of the EncroChat data, whether there were any procedure violations, and how these might impact their admissibility in court as legitimate evidence.

The CJEU explained that granting an EIO to legally seek and transfer evidence from another EU Member State is a simpler procedure than initiating proof-gathering in another EU Member State; this is a valuable clarification in understanding how a country's judicial authority can make use of the EIO. It is particularly helpful in clarifying the interpretation of an EIO, and as such, whether the prosecution office can also issue an EIO without a judge's approval – although it should be noted that this is only when asking to transfer evidence already in possession of another EU Member States, and not to initiate proof-gathering in another EU Member State, which would require a judge's approval.

However, on closer assessment, *C-670/22 – M.N. (EncroChat)* could be argued to stand out as a contribution in the area of EU judicial cooperation in criminal matters for a variety of reasons. First, as a way to address the defence rights concerns raised over the use of the EncroChat data as evidence, here the CJEU has developed a new framework for EU Member States on evidence admissibility and ensuring that the right to a fair trial is protected. For instance, the CJEU ruling established a framework and conditions that EU Member States must adhere to when deciding whether to accept evidence: (i) a trial is considered fair only if the defendant is able to "comment effectively" on the evidence against them, particularly if it is likely to have a significant impact on the case's facts and outcome; (ii) if the defendant fails to comment effectively on such important evidence, a breach of the right to a fair trial occurs; (iii) as a result of this breach, the evidence in question "should be excluded" to prevent an infringement of the right to a fair trial.[58]

This CJEU framework and conditions are based on Article 47 of the EU Charter of Fundamental Rights, with the view of strengthening the Charter's application to EIO Directive evidence.[59] Therefore, the CJEU's ruling attempted to emphasise the protection of fair trial rights when using EncroChat data in court – a right that courts in EU Member States must uphold when evaluating such data use in a criminal proceeding. However, there are some questions marks over whether the CJEU has truly addressed the concerns raised by NGOs, defence lawyers, and academics over the potential breach of the right to a fair trial in Germany.[60] This is because the CJEU did not rely on ECtHR case law on

[56] Ibid, § 131.

[57] Case C-670/22 Opinion of Advocate General Tamara Ćapeta: Staatsanwaltschaft Berlin v M.N., (EncroChat) (2023) ECLI:EU:C:2023:817.

[58] Case C-670/22 Staatsanwaltschaft Berlin v M.N., (EncroChat) (2024) ECLI:EU:C:2024:372.

[59] I Szijártó, "The Interplay Between the European Investigation Order and the Principle of Mutual Recognition", (2023) 8(3) European Papers 1575–97.

[60] A Kanakakis, "The EncroChat Judgment (Case C-670/22, MN): CJEU Steering a Bold Course through the Symplegades of Evidence Admissibility", UK Association for European Law, 1 July 2024, <https://ukael.org/2024/07/01/the-encrochat-judgment-case-c-670-22-mn-cjeu-steering-a-bold-course-through-the-symplegades-of-evidence-admissibility/>.

evidentiary admissibility, even though Budak and Yüksel Yalçinkaya used the same approach,[61] to offer wider protection. The lack of reference by the CJEU to the ECtHR's case law can be understood as aligned to the desire to reaffirm the EU's autonomy in this field, building on its previous case law in *C-470/21 – La Quadrature du Net and Others*.[62] Yet, it also seems that the CJEU wanted to be supportive of the investigation, because the EncroChat data has been invaluable in gaining a better understanding of current operations of organised crime, and the types of criminal activities in which it is involved.[63] The prosecution considered the EncroChat data a goldmine of information, allowing them to solve a number of ongoing investigations, and shedding new light on the evolution of organised crime in Europe – notwithstanding some serious questions as to the reliability and accuracy of the data. For example, the Italian Supreme Court made a ruling in a similar case about encrypted communications from a network known as Sky ECC;[64] in pre-trial hearing the court did not consider this data sufficient and admissible evidence.

Similarly, in France, lawyers have pushed back against the use of encrypted data in the case of EncroChat on the basis of (i) the French Gendarmerie's refusal to disclose technical details of the interception operation; (ii) the authorisation of far-reaching measures not being covered by their legal bases; (iii) "massive and indiscriminate" interception; and (iv) the absence of a time limit on interception measures in court orders. The French Court of Cassation (Supreme Court) ruled on two EncroChat cases after asking the Conseil Constitutionnel (Constitutional Court) whether Articles 706-102-1 and 230-1 of the French Code of Criminal Procedure are constitutional.[65] On 8 April 2022, the Conseil Constitutionnel ruled 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, privacy, freedom of expression, or any other constitutional right.[66] However, it suggested that all of the data gathered in the hacking must be shared with the defence, to ensure a fair trial.

In recognising EncroChat's data as evidence, even though some experts and national courts question its reliability,[67] the CJEU's ruling has not adequately safeguarded the right to a fair trial, failing to provide a strong framework for the defence to argue against the EncroChat data's integrity and reliability.[68] The decision has made it difficult for defence counsel arguments on the grounds that they cannot "comment effectively" on the content of the chat, even though the court has acknowledged that the data can make it difficult to identify the person using EncroChat.

[61] T Emre and YA ByLock, "Prosecutions and the Right to Fair Trial in Turkey: The ECtHR Grand Chamber's Ruling in Yüksel Yalçınkaya v Türkiye", Statewatch, 30 March, 2024, <https://ssrn.com/abstract=4778618>.

[62] X Groussot and A Engel, "Op-Ed: The Devil is in the (Procedural) Details – the Court's Judgment in La Quadrature du Net", EU Law Live, 13 May 2024, <https://eulawlive.com/op-ed-the-devil-is-in-the-procedural-details-the-courts-judgment-in-la-quadrature-du-net-by-xavier-groussot-and-annegret-engel/>.

[63] J J Oerlemans, and D A G van Toor, "Legal Aspects of the EncroChat Operation: A Human Rights Perspective", (2022) 30(3-4) European Journal of Crime, Criminal Law and Criminal Justice 309–28.

G Sagittae, "On the lawfulness of the EncroChat and Sky ECC-operations", (2023) 14(3) New Journal of European Criminal Law, 273–93. <https://doi.org/10.1177/20322844231159576>.

[64] See, "Italian criminal procedure allows Encrochat and Sky-Ecc encrypted messaging without algorithm (Cass. 23999/23)", canestriniLex, 6 June 2023, <https://canestrinilex.com/en/readings/italian-criminal-procedure-allows-encrochat-and-sky-ecc-encrypted-messaging-without-algorithm-cass-2399923>.

[65] H Mildebrath, "EncroChat's path to Europe's highest courts," European Parliamentary Research Service, 16 December 2022, <https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2022)739268>.

[66] Ibid, §§ 1–2.

[67] G Sagittae, "On the lawfulness of the EncroChat and Sky ECC-operations," (2023) 14(3) New Journal of European Criminal Law 269–72.

[68] L Bernardini, "Op-Ed: On Encrypted Messages and Clear Verdicts – the EncroChat Case before the Court of Justice (Case C-670/22, MN)", EU Law Live, 21 May 2024, <https://eulawlive.com/op-ed-on-encrypted-messages-and-clear-verdicts-the-encrochat-case-before-the-court-of-justice-case-c-670-22-mn-by-lorenzo-bernardini/>.

The decision of the CJEU appears to be influenced by the new EU strategy to combat organised crime, which has seen Member State law enforcement authorities agencies focusing on equipping their state prosecution bodies with the necessary legal tools and protections to uncover organised crime groups operating within the EU and to gain a clearer understanding of the evolution of organised crime and its current state.[69] The EncroChat data have provided a new understanding into the operations of organised crime within the Union – and in this decision to classify the data as legal, the CJEU has chosen to support this approach, despite legitimate questions over the data's integrity.[70]

Thus, the right to a fair trial in cases involving EncroChat data cannot be fully guaranteed. As a result, the defence should rely on the principle of proportionality, which requires that any decisions made against their client are carefully evaluated and weighed against the alleged crime, ensuring that the penalties imposed are appropriate and proportionate.

To help further develop the EU law's procedural approach on this matter, given that many EncroChat users may argue that the French authorities' data collection, interception, and assessment violated their domestic law and procedures, in October 2024, the EU adopted a new regulation on the transfer of proceedings in criminal matters. The intention was to develop a common legal procedure for transferring evidence and criteria, to improve respect for the fundamental rights of suspects or those accused during the process of transferring criminal proceedings from one country to another.[71]

Also in October 2024, the CJEU and the ECtHR heard a case on encrypted communication via EncroChat and SKY ECC networks. The *A.L. and E.J.* v *France* ruling was that the collecting authorities in France obtained evidence legally.[72] Along similar lines to the CJEU, the ECtHR found that the evidence was gathered in accordance with French law, and the UK Crown Prosecution Service asked for the French authorities' evidence to be transferred to the UK for a criminal case only (not to intercept and gather further evidence).[73] This built on the *C-670/22 – M.N. (EncroChat)* ruling, wherein the prosecution acquiring encrypted data to initiate a new investigation (not just as evidence in an existing case) would have to be done in accordance with states' domestic laws.

However, unlike the CJEU, the ECtHR stated that there are remedies available to applicants in France who believe the data was gathered illegally, such as challenging the data transfer measures taken, according to the EIO in the ECtHR case issued by the UK authorities, as well as the data retrieval measure used. This was aimed at giving the defence a remedy in case of a breach. Furthermore, the ECtHR noted that, under Article 694-41 of the French Code of Criminal Procedure, applicants could have applied for the exclusion of evidence collected through enforcement in France.[74] Although one could also rely on EU law for remedies, as in *C-746/18 – Prokuratuur*, the CJEU said that access to data and retention of electronic communications must be confined to serious crimes.[75]

[69] European Commission, "EU roadmap to fight drug trafficking and organised crime," 18 October 2023, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023DC0641/>.

[70] European Commission, "Fight against organised crime: New 5-year strategy for boosting cooperation across the EU and for better use of digital tools for investigations," 14 April 2021, <https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1662>.

[71] Council of the European Union, "Regulation of the European Parliament and of the Council on the transfer of proceedings in criminal matters," 16 October 2024, <https://data.consilium.europa.eu/doc/document/PE-72-2024-INIT/en/pdf>.

[72] A.L. and E.J. v France, no. 44715/20 and 47930/21, ECHR 244 (2024), 17 October 2024.

[73] Ibid, §§ 1-4.

[74] Ibid, §§ 1-4.

[75] S Rovelli, "Case Prokuratuur: Proportionality and the Independence of Authorities in Data Retention", (2021) 6(1) European Papers 199–210.

In closing, the CJEU has established a tailored evidence admissibility threshold for evidence transfer in EIO proceedings. In particular, it has helped to ensure how EIOs are interpreted. However, it missed an opportunity to strengthen the EU Charter of Fundamental Rights on fair trials and defence rights in cross-border criminal cases. Furthermore, it failed to fulfil its potential to improve some EU procedural guarantees for defendants across Europe, as there are still major questions mark over the reliability and verification of the EncroChat data. The CJEU ruling can be understood to have been largely motivated by providing law enforcement agencies with an understanding of the status and evolution of organised crime, and thus, it mostly focused on clarifying the use of the EIO Directive, rather than on the legality of the data itself. Thereby, the CJEU made the work of defence lawyers more difficult, in their arguments against the use of EncroChat data as evidence in court. These defence lawyers, as well as NGOs and academics, echoed many of the Berlin Court's concerns about the use of EncroChat data as acceptable and lawful evidence, in their protestations that such use undermines the rule of law, and possible breaches of the right to a fair trial have not been fully assessed. Arguably, the CJEU hid behind the fact that France did the hacking according to its own laws, on the premise that Member States should not question other Member States' judicial procedures, bin order to uphold mutual trust within the Union. It would seem that the real reason for ducking this question is because the police and prosecution claim that the data has been so powerfully valuable as a source of information about organised crime in Europe – the CJEU's priority was to safeguard this source, despite the risks to the right to a fair trial in some cases.

6. Conclusion

The primary goal of the Berlin Regional Court's questions to the CJEU was to understand how the French authorities investigate and gather evidence, given the significant secrecy surrounding the hacking of the EncroChat network, and how both the courts and the defence can analyse the integrity of data when dealing with users facing criminal charges. The Berlin Court, NGOs and academics assert that infiltrating the EncroChat server on German territory would have violated the German Code of Criminal Procedure. However, the CJEU shied away from answering this question directly, reformulating it and focusing on interpreting the definition of EIOs. This can be understood as the CJEU prioritising the police and prosecution's ability to extract useful data from the EncroChat device in order to understand better the evolution of organised crime in Europe and to support the EU's strategy against organised crime, rather than adhering to the human rights standard that ensures the right to a fair trial and the defence's ability to effectively contest the evidence obtained from the EncroChat device.

Thus, the focus of the CJEU shifted, to establish that the public prosecution office can issue EIOs without approval by the courts under the EIO Directive, although solely to obtain evidence that another EU Member State has already gathered, not to launch an inquiry to gather evidence, which requires a court order. The CJEU ruling raised some questions as a result, and in response to the case, the EU passed a new regulation to enhance the transmission of evidence across the EU, including a framework and conditions set by the CJEU, to which EU Member States must adhere when assessing evidence to ensure a fair trial. The new regulations specify EU law and conditions under which a judicial authority or police may file an inquiry to transfer and access evidence, as well as when launching a new investigation to collect evidence from another EU Member State. Therefore, the case has revealed the limitations of EU law in this area.

In responding to the main question of the Berlin Regional Court, the CJEU found the French authority's methods of investigation were in line with domestic laws and regulations, and suggested that it is up to a state's national laws and procedures as to how

it initiates its investigations. Unlike in France, the EncroChat data would have been inadmissible in Germany were it sourced there, due to the hacking methods and data gathering for an investigation being illegal under German law. Both the CJEU and ECtHR noted that countries questioning the French authorities and judiciary's evidence-gathering methods undermines the principle of mutual recognition, a long-established practice under EU and ECtHR case law. However, they also both commented that countries retain the right to opt not to use such data, if the defence cannot comment effectively upon it, and if it fails to meet due process and fair trial requirements. Thereby, both courts went some way to recognising the concerns raised by the Berlin Court, NGOs, and academics over the legitimacy and reliability of the EncroChat data.

In closing, the EncroChat data has not provided key evidence incriminating those charged, but the information provided through the intercepted encrypted communications has assisted the prosecution and police in solving several criminal investigations – hence the CJEU's attempts to ensure that the EncroChat data are considered admissible by the court, in order to bridge the gaps in the understanding of the evolution of organised crime in the EU, and mapping criminal activity that has taken place across countries.

Cite this article: A Hoxhaj, "The CJEU Ruled that the EncroChat Data can be Admissible Evidence in the EU". *European Journal of Risk Regulation*. https://doi.org/10.1017/err.2025.10047