Volume XXI, Issue (1) (2025) 551-561

International May Conference on Strategic Management

DOI: 10.5937/IMCSM25551M *Original Research*

THE SIGNIFICANCE OF THE COURT OF JUSTICE OF THE EUROPEAN UNION JUDGMENT OF 30 APRIL 2024 IN CASE C-670/22 ("ENCROCHAT") FOR THE ADMISSIBILITY OF EVIDENCE IN CRIMINAL PROCEEDINGS

Remigijus Merkevičius*

Vilnius University, Faculty of Law, Lithuania

Abstract: This article analyses the judgment delivered by the Court of Justice of the European Union (CJEU) on 30 April 2024 in Case C-670/22 ("EncroChat") and its implications for the admissibility of evidence in national criminal proceedings. According to the CJEU, a European Investigation Order (EIO) requesting evidence already held by the executing Member State may only be issued by a competent authority as defined by the issuing State's national law. When issuing such an EIO, the issuing authority must assess its compliance with (i) the classic principles of *necessity* and *proportionality* as set out in Article 6(1)(a) of the Directive and (ii) all "material conditions" prescribed by national law for the sharing of evidence in domestic proceedings. This includes, *inter alia*, evaluating the effect of the executing State's refusal to disclose the technical features of the tools used to infiltrate the encrypted telecommunications system, comparing the categories of investigated criminal offences, and the coercive procedural measures used to obtain the data in question. The ability of the issuing State to use such evidence depends directly on (i) the conditions and procedures of its collection in the executing State and (ii) the defendant's awareness and ability to effectively challenge it. Where the defendant cannot meaningfully dispute the authenticity, legality or reliability of the evidence, such evidence must be excluded. In addition, if, *in concreto*, such a coercive measure would not be permissible under the issuing State's domestic law, the exclusion of that evidence is also governed by Article 31(1) and (3) of the Directive.

Keywords: Admissibility of evidence, Court of Justice of the European Union, EncroChat, Encrypted communication, European Investigation Order.

1. INTRODUCTION

Eurojust, Europol, and national law enforcement authorities almost annually report successful infiltrations into encrypted telecommunications systems used by organised criminal groups for conspiratorial purposes. These operations have yielded substantial incriminating

* *Corresponding author: remigijus.merkevicius@tf.vu.lt*

Remigijus Merkevičius, ORCID: 0009-0009-4555-0018

evidence and led to severe blows against organised crime. For instance, in July 2020, it was announced that French and Dutch law enforcement authorities had jointly "cracked" the encrypted telecommunications system EncroChat, which had around 60,000 users. Notably, the infiltration was carried out without regard to the users' territorial location or the jurisdiction in which they were situated. In March 2021, an even greater success was reported: through the joint efforts of French, Dutch, and Belgian law enforcement authorities, the encrypted communications system SKY ECC, used by more than 170,000 individuals, was intercepted, and over 20 million messages and other information transmitted via this covert channel were seized. In June 2021, it was revealed that the US Federal Bureau of Investigation had created and administered its own encrypted network, ANOM, which it monitored, controlled, and recorded *ab initio*, using the obtained data to initiate criminal prosecutions. One of the most recent developments came in December 2024, when the takeover of data from the encrypted telecommunications system MATRIX was publicly announced. Thus, covert law enforcement infiltrations into encrypted telecommunications systems represent the new reality of criminal justice. Sommer (2023) has referred to this as "the direction in which the criminal process of the future is developing – a digitalised and, above all, Europeanised criminal process" (Sommer, 2023). On the one hand, we can indeed commend law enforcement for its ability to respond effectively and pragmatically to criminal behaviour shaped by modern technologies. On the other hand, however, the use of such data in criminal proceedings can determine the fate of many individuals and is therefore permissible only if it is lawful. It is no coincidence that Strate (2022) opens his analysis with the vivid expression: "The road to hell is paved with good intentions" (Strate, 2022).

A second, equally evident, reality of contemporary criminal justice is the "free" – unrestrained and uncontrolled – sharing of covertly obtained information. U. Sommer aptly observes that the mutual "legal assistance" between democratic states and the mutual trust displayed towards investigating authorities serve as a kind of "magic hood" (Ger. *Tarnkappe*) used to cover and thereby conceal the quiet displacement of judicial transparency and foreseeability from legal processes, replacing them with a gateway to unlimited criminal prosecution (Sommer, 2024). For example, the results of secret operations by the French law enforcement authorities, which deeply intruded into individual privacy, were widely disseminated to counterparts in states that had not directly participated in those covert investigations. It is therefore unsurprising that mass arrests, searches, asset seizures, indictments and convictions followed across Europe based on this information. For instance, more than 2,000 preliminary investigations were launched in Germany alone on the basis of EncroChat data intercepted by French law enforcement authorities and transferred to Germany (Gebhard & Michalke, 2020; Kipker & Bruns, 2022; Lenk, 2024). Europol reports that, based on this information, more than 6,500 suspects were arrested, nearly €740 million in cash was confiscated, over 30 million tablets of synthetic drugs were seized, as well as more than 103 tonnes of cocaine. The scale is staggering.

Cooperation between law enforcement authorities and the sharing of information are, *per se*, undoubtedly a *conditio sine qua non* for effective criminal justice. Mutual trust is one of the core ideas uniting the Member States of the European Union (hereinafter – the EU). However, the problem that determines the relevance of this discussion lies in the fact that the "hacking" of an encrypted telecommunications system and the acquisition and use of a substantial amount of its content for incriminating purposes constitute a serious intrusion into individual privacy. Such intrusion cannot be justified merely by the popular slogan that "only or mostly criminals use encrypted communications." From a formal procedural perspective, the information covertly obtained through infiltration of encrypted telecommunications systems by France was shared with other EU Member States by means of legal cooperation instruments –

namely, European Investigation Orders (hereinafter – EIO) submitted by the requesting states to obtain evidence already in the possession of the French authorities, acting as the executing state. However, the legal basis for the use of coercive procedural measures that restrict privacy differs across EU Member States. In some respects, it is even questionable whether national law permits actions of the nature, scale and intensity actually carried out *in concreto* by the law enforcement authorities of France, the Netherlands, or other countries. Therefore, the aim of this discussion is not to limit the capabilities of law enforcement or to deprive them of effective tools, but rather to assess and ensure legality – without which the concept of the "rule of law" cannot exist.

A third significant aspect is that the French authorities have refused to disclose the technical means, methods, and tools by which they succeeded in intercepting the data transmitted via the encrypted telecommunications system in question, how the recipients of the communication (users or end devices) were identified, and so forth. In France, this has been classified as a matter of "national security secrecy" (Fr. *secret de la défense nationale*). In such a situation, during criminal proceedings taking place in different states, not only do the accused lose the opportunity to verify and assess the integrity, authenticity, and reliability of the covertly obtained data, but so does the court. This increases the risk of fatal error – the danger that an innocent person may be convicted – and raises serious concerns about the legitimacy of using such acquired and transferred data in national criminal proceedings. For instance, Zimmermann (2022) questions the entire process of obtaining and using these data: the installation of spyware on the EncroChat server, the transmission of the data collected by French authorities to authorities in other states, and the processing and use of those data for incrimination purposes (Zimmermann, 2022). Not only criminal procedural aspects are being debated, but also constitutional and personal data protection issues (Derin & Singelnstein, 2021).

Initially, individual nation states attempted to resolve these issues independently – each in their own way, as best they could (Škulić, 2024). Recognising the seriousness of the situation in terms of privacy protection and the need to assess the matter systematically, including in the context of legal cooperation within the EU, the Berlin Regional Court (Ger. *Landgericht Berlin*), in its decision of 19 October 2022 on a request for a preliminary ruling, referred five essential questions to the Court of Justice of the European Union (hereinafter – the CJEU). These questions concerned the interpretation of Articles 7, 8, and 11 of the Charter of Fundamental Rights of the European Union (hereinafter – the Charter), as well as Article 6(1) (in conjunction with point (c) of Article 2), and Articles 31(1) and (3) of Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (hereinafter – the Directive). These questions arose in the context of the use, in German criminal proceedings, of data obtained from France, which had been collected by French law enforcement authorities through covert infiltration of the encrypted telecommunications system EncroChat. The judgment in the case, registered as Case C-670/22, was delivered by the CJEU on 30 April 2024 (hereinafter – the CJEU judgment).

This naturally raises the question of whether, and if so to what extent, the judgment of the CJEU affects the legitimacy of data (evidence) used in national criminal proceedings, where such data have been collected through covert infiltration of an encrypted telecommunications system by one EU Member State and subsequently transferred to another under a European Investigation Order. Although the CJEU judgment examined and assessed only the use of data obtained through covert infiltration of encrypted communications via the EncroChat devices and system (undoubtedly taking into account the specific nature of the infiltration in that particular case), it can nevertheless be argued that, provided the essential factual and legal circumstances described in the judgment remain unchanged (lot. *mutatis mutandis*), the legal conclusions and value-based directions articulated by the CJEU regarding the admissibility of

data (evidence) should apply irrespective of the name of the encrypted communication system in question (Lödden & Mania, 2025).

2. LITERATURE REVIEW

Less than a year has passed since the CJEU delivered its judgment, and it has therefore not yet attracted extensive attention in criminal procedure law scholarship. The key academic debate took place prior to the publication of the CJEU judgment. This article does not focus on the legal framework of any single Member State but rather seeks to offer broader insights. As the initiator of the judicial proceedings before the CJEU, Germany has shown a clear interest in obtaining a well-founded doctrinal justification for the legality of using such data (evidence). Accordingly, the scientific analysis in this article is based primarily on selected works by prominent German legal scholars, including R. Michalke, M. Lenk, U. Sommer, G. Strate, F. Zimmermann, among others.

3. METHODOLOGY

In conducting the research and formulating conclusions, classical scientific research methods typical and essential for legal analysis were employed. These included the logical-systematic method, legal document analysis, comparative method, as well as other methods of legal interpretation and application.

4. RESULTS AND DISCUSSION

Given, on the one hand, the rather superficial, formal, and prosecutorial approach taken by many states towards the use of encrypted telecommunications data covertly obtained by France in their national criminal proceedings, and, on the other hand, the profound consequences that the use of such data has had on the lives of numerous individuals, various stakeholders placed vastly different hopes in the CJEU judgment. It appears that, due to its considerable level of abstraction, somewhat convoluted rhetoric, and an evidently deliberate intention to limit itself to matters related to the issuance of the EIO, the CJEU judgment somewhat disappointed all sides. It is therefore not surprising that the judgment has been met with ambivalence in public discourse: some praised the CJEU in celebratory tones, welcoming its contribution to the effectiveness of criminal prosecution in the most serious offences; others, disappointed, questioned whether the judgment had effectively given a green light to forum shopping in criminal proceedings – that is, strategic manipulation of criminal jurisdiction (Gebhard & Michalke, 2020). It is still too early to state definitively what significance the CJEU judgment will ultimately have. In its essential part – the admissibility of evidence in the criminal proceedings of the issuing state – the judgment is formulated in terms that are far too abstract. Its actual significance will depend on how it is interpreted and applied by national courts. The first signals have already emerged. For example, by its decision of 1 November 2024 in case no. 2 BvR 684/22, the German Federal Constitutional Court declared inadmissible a constitutional complaint that raised questions regarding the inadmissibility of EncroChat data obtained from France in German criminal proceedings. Without delving into the reasoning of this decision, it seems that key legal aspects highlighted in the CJEU judgment continue to be overlooked (Meyer-Mews, 2025). This is cause for concern and calls for a more thorough discussion of the judgment, which not only directly answers questions related to the issuance of an EIO for evidence already in possession of the executing state but also sets out a clear

value-based direction for assessing the legitimacy of using such data in the criminal proceedings of the issuing state.

4.1. Who Can Issue an EIO to Obtain Evidence Already in the Possession of the Executing State, and Under What Conditions?

In its judgment, the CJEU stated that the authority entitled to issue an EIO and the conditions under which an EIO may be issued to obtain evidence already in the possession of the executing state are determined by the criminal procedure law of the issuing state. An EIO for the transfer of evidence already held by the executing state "does not necessarily have to be issued by a court, where, under the law of the issuing state, the initial collection of such evidence in a purely domestic procedure would have required a court order, but the public prosecutor is competent to request the transfer of such evidence" [§ 77]. However, "where under the law of the issuing state the public prosecutor does not have the competence to order the transmission of evidence already held by the competent national authorities <...>, the prosecutor cannot be regarded as a competent issuing authority within the meaning of this provision" [§ 75]. Thus, when assessing the issuing of an EIO aimed at obtaining evidence already in the possession of the executing state, it is not decisive whether, had the same evidence been collected within the issuing state, a judicial decision (authorisation) would have been required. An EIO may be issued by a prosecutor, provided that, under the law of the issuing state, the prosecutor is authorised to determine the "sharing" of such evidence in domestic criminal proceedings. Therefore, in evaluating the legitimacy of issuing an EIO, the decisive criterion is not the conditions for *obtaining* the evidence, but the authority, legal basis, and procedure for the *transfer* of such evidence under the law of the issuing state.

The CJEU's interpretation was welcomed with great enthusiasm by prosecuting authorities. Although a position that excludes judicial oversight *a priori* – at the initial stage of evidence collection – significantly weakens the effectiveness of human rights protection, this interpretation must nevertheless be approached with due caution. The CJEU equated the "sharing of evidence" between EU Member States with the "sharing of evidence" within a single Member State (a position that is not without controversy, though it will not be assessed in the present context). At the same time, however, the CJEU imposed a strict obligation on the issuing state to comply fully with the procedural conditions and rules laid down in its own national law. In simple terms, the judgment does not justify an unconditional or purely formal conclusion that "the public prosecutor is always competent."

4.2. Can an EIO Seeking to Obtain Evidence Already in the Possession of the Executing State Be Issued Only If Such Evidence Was Obtained in Accordance With the Conditions Laid Down in the Law of the Issuing State?

The CJEU essentially rejected a direct link between the *collection* of evidence and the *transmission* of evidence, and, more specifically, the notion that the lawfulness of the *transmission* depends on whether the evidence was obtained *in accordance with the law* of the issuing state. This conclusion by the CJEU once again generated enthusiasm among prosecuting authorities. However, even in this legal context, the CJEU's reasoning must be considered in a systematic manner: although the lawfulness of the *transmission* of evidence under an EIO does not directly depend on whether such evidence could have been lawfully obtained under the law of the issuing state, the lawfulness of the *transmission per se*, by means of an EIO, does not *ipso facto* create or guarantee the issuing state's procedural freedom to use the evidence without limitation in its own criminal proceedings.

In its judgment, the CJEU pointed out that Article 6(1)(a) of the Directive:

(i) does not require that the issuance of an EIO seeking to obtain evidence already held by the executing state necessarily depend on the existence, at the time of issuance, of a specific factual suspicion that a serious offence has been committed by each individual concerned, provided that such a requirement is not imposed by the law of the issuing state; and

(ii) does not preclude the issuance of an EIO where the integrity of the data obtained by means of the investigative measure applied in the executing state cannot be verified due to the non-disclosure of the technical basis enabling the use of that measure – again, on the condition that the right to a fair trial will be ensured in the subsequent criminal proceedings [§§ 89–90].

Thus, the CJEU clearly distinguishes, on the one hand, the initial process – the *transmission* of evidence under an EIO – from, on the other hand, the final stage – the *assessment of evidence obtained* via the EIO. Moreover, in both legal aspects concerning the use of evidence under an EIO, the CJEU's reasoning is conditional – and such conditions may, *in concreto*, prove to be decisive.

From the perspective of "material conditions," Article 6(1)(b) of the Directive is linked solely to the requirements laid down in the law of the issuing state [§§ 91–94]. Therefore, if, under the law of the issuing state, the transmission of evidence (within that state) is permitted only in the presence of specific facts relating to serious offences committed by the accused, or if only under such conditions may evidence containing the data in question be assessed, the issuance of an EIO is dependent on the fulfilment of all such conditions [§ 95]. In this regard, the CJEU rightly highlighted a broader value-based orientation: Article 6(1)(b) of the Directive aims to prevent the circumvention of the rules and safeguards established under the national law of the issuing state [§ 97].

According to the CJEU judgment, the issuing authority must *ab initio* – that is, at the moment of issuing the EIO – verify and assess whether the request to obtain evidence already in the possession of the executing state complies with: (i) the classical principles of *necessity* and *proportionality as laid down* in Article 6(1)(a) of the Directive; and (ii) all the "material conditions" that, under the law of the issuing state, govern the possibility of "sharing evidence" in domestic criminal proceedings. Although different Member States apply different national conditions for the internal "sharing of evidence" in criminal proceedings, issuing authorities must, as a general rule, prior to issuing an EIO seeking to obtain evidence already held by the executing state, first answer the question of whether, without knowledge of the technical characteristics of the measures used by the executing state's law enforcement authorities to covertly infiltrate the encrypted telecommunications system and extract its data, it is possible to fulfil all the "material conditions" required under the issuing state's national law for the internal sharing of such data. Even *in abstracto*, that is often not feasible.

On the other hand, when defining the legal possibility of "sharing evidence" in domestic criminal proceedings, the law of the issuing state often requires a comparison not only of the offences under investigation in different cases, but also of the specific coercive measures by which the requested data were obtained. A comparison of coercive measures first and foremost requires an assessment of whether, under the law of the issuing state, there is any legal basis at all for conducting investigative actions of the nature, scale, and intensity actually carried out *in concreto* by authorities from France, the Netherlands, or other states when infiltrating encrypted telecommunications systems. In some EU Member States, such as Lithuania, the criminal procedure law does not contain specific coercive measures that would legitimise remote access to a closed information system and the control of all data flows within it. However, even in those Member States whose criminal procedure laws provide for the use of certain covert measures targeting information systems, legal scholarship still questions whether the existing

legal framework can justify investigative actions of the type, scope, and intensity conducted by French and Dutch officials.

For instance, section 100b of the German Code of Criminal Procedure (Ger. *Strafprozessordnung*) provides for a special coercive measure known as *Online-Durchsuchung* (online or remote search and seizure), which allows covert (without the knowledge of the data subject) access to an IT system used by the individual and the extraction of data from it using technical means. However, even with such specific legal provisions aimed at legitimising intrusions into fundamental rights, German criminal procedure scholarship questions whether the actions and measures taken by the French authorities could be considered equivalent to and justified under section 100b of the German Code of Criminal Procedure (Gebhard & Michalke, 2020; Derin & Singelnstein, 2021; Löffelmann, 2022; Schmidt, 2022; Strate, 2022; Lödden & Makepeace, 2023; Sommer, 2023; Meyer-Mews, 2024). Ultimately, the comparison of coercive measures inevitably presupposes an analysis of the essential conditions under which such measures may be applied, one of which is usually the existence of a justified *in personam* suspicion (Gebhard & Michalke, 2020; Meyer-Mews, 2024; Meyer-Mews, 2025). Without knowing the technical method by which the data were obtained, it is not even possible to conduct a rational comparison between the actions and measures taken by the authorities of France, the Netherlands, or other states and those that could hypothetically be carried out lawfully under the law of the issuing state (Schmidt, 2022). Strate (2022) also notes that, *in concreto*, both sides – German and French – knew that the Directive does not, in principle, provide a legal basis for using a "Trojan" to take over a server and access all stored mobile communication content; therefore, such use of a Trojan could not, in any case, have been the subject of an EIO (Strate, 2022).

4.3. Under What Conditions May Evidence Collected by the Executing State and Transferred to the Issuing State Under an EIO Be Used in the Issuing State's Criminal Proceedings?

In this respect, the CJEU judgment rightly points out, first of all, that the principle of mutual recognition of judicial decisions does not grant the issuing authority seeking, by means of an EIO, to obtain evidence already held by the executing state, the right to examine the lawfulness of the proceedings in which that evidence was collected by the executing state [§§ 99–100]. At the same time, however, it emphasises that individuals affected by certain investigative measures are entitled to judicial protection of their fundamental rights under the Directive [§ 101]. Article 14(1) of the Directive requires Member States to ensure that remedies are available in respect of investigative measures requested in an EIO, and that such remedies must be equivalent to those that would be available in a comparable domestic (national) case [§ 102]. If the transmission of evidence already in the possession of the executing state to the issuing state appears disproportionate in relation to the objectives of the criminal proceedings being conducted in the issuing state against the person concerned – e.g. because it constitutes a serious infringement of that person's fundamental rights, or because the investigative measure was carried out in breach of the legal provisions that would apply in a similar domestic case – then the court examining a complaint against the EIO requesting the transfer of such evidence would be obliged to draw the conclusions required under the applicable national law of the issuing state.

On the other hand, Article 14(7) of the Directive obliges Member States to ensure that, in criminal proceedings taking place in the issuing state, the evaluation of evidence obtained through an EIO guarantees the rights of the defence and safeguards the fairness of those proceedings (the right to a fair trial) [§§ 103–104]. If it is established that a party to the

proceedings is unable to properly and effectively present their position regarding evidence that may have a significant impact on the assessment of the facts, the court must find a violation of the right to a fair trial and exclude that evidence from the proceedings [§§ 105, 130–131]. According to Meyer-Mews (2024, 2025), the CJEU judgment articulates "an absolute exclusionary rule that is not subject to balancing against other competing values in the specific case" (Ger. *ein abwägungsfestes absolutes Beweisverbot*) (Meyer-Mews, 2024; Meyer-Mews, 2025).

Thus, when assessing the CJEU's reasoning as a whole, it becomes clear that the Court separated the conditions for *issuing* an EIO from the criteria that govern how evidence obtained through such an order must be *assessed* in the issuing state. As previously mentioned, the lawfulness of issuing an EIO does not grant the issuing state the freedom to use the evidence obtained under it without limitation in its domestic criminal proceedings. The admissibility of evidence obtained under an EIO – namely, evidence already in the possession of the executing state and shared with the issuing state – depends directly on (i) the conditions and procedures under which the evidence was collected in the executing state, and (ii) whether the accused was aware of those circumstances and had the opportunity to effectively comment on them. If the accused's knowledge of the evidence transmitted to the issuing state under the EIO does not enable them to properly and effectively express their position regarding its lawfulness, reliability, accuracy, authenticity, and other essential characteristics, such evidence – without denying or undermining the *principle of mutual recognition of judicial decisions* – cannot be used in the evidentiary process conducted in the issuing state. It is evident that knowledge of the technical details regarding how the tools used to intercept encrypted telecommunications content were designed and operated constitutes one of the *conditio sine qua non* for an effective defence.

In the context of the admissibility of evidence collected by the authorities of the executing state and subsequently transferred to the issuing state under an EIO for use in the issuing state's criminal proceedings, the CJEU also referred to Article 31(1) and (3) of the Directive, which, among other things, aim to protect the rights of individuals (mobile network users) affected by telecommunications interception measures [§ 125]. Article 31 of the Directive is intended to safeguard not only the sovereignty of the state to which notification is given, but also the level of protection afforded under that state's law concerning the lawfulness of telecommunications surveillance (information interception), ensuring that it is not diminished in comparison to what would apply in a purely domestic procedure. Since telecommunications surveillance (interception of information) constitutes an interference with the right to respect for private life and the confidentiality of communications enshrined in Article 7 of the Charter, Article 31 of the Directive also seeks to protect the rights of persons subjected to such measures. This objective includes safeguarding those rights in relation to the use of the intercepted data for the purposes of criminal prosecution in the notified state [§ 124].

Articles 31(1) and (3) of the Directive essentially imply that if both the intercepting state and the notified state properly fulfil their obligations under these provisions, the competent authorities of the intercepting state cannot carry out telecommunications surveillance (interception of information) on the territory of the notified state if such action would not be permitted under the national law of that state. Gebhard and Michalke (2020) rightly observe that this is not an obligation that a Member State may choose to disregard (Gebhard & Michalke, 2020). If either of the states concerned fails to properly or timely fulfil its obligations under Article 31(1) or (3) of the Directive – be it the intercepting state failing to inform the other state of the measures being implemented on its territory, or the notified state failing to prevent the unlawful interception of information (i.e. in violation of its own national law) – then

permitting the use of such evidence in the issuing state's criminal proceedings would amount to circumventing the rules and safeguards laid down in the Directive (Schmidt, 2022).

Thus, the CJEU judgment also implies a legal conclusion that, if under the domestic law of the issuing state (which, in the legal context under discussion, is the notified state) a certain measure involving access to end-user telecommunications devices – for the purpose of intercepting the flow, location, and metadata of internet-based communications – could not *in concreto* be applied on its territory, then data obtained through such a measure by the intercepting state may not be used as incriminating evidence in the criminal proceedings of the issuing state. This conclusion must be drawn regardless of whether the measure applied was lawful and legitimate under the law of the intercepting (executing) state, and irrespective of whether the obligations set out in Article 31(1) and (3) of the Directive were formally fulfilled.

5. CONCLUSION

The Directive does not require that an EIO seeking to obtain evidence already held by the executing state be issued by a court. However, this does not automatically imply that such an EIO may be issued by a public prosecutor. The competent authority and the conditions under which an EIO of this kind may be issued are determined by the national law of the issuing state.

When issuing an EIO seeking to obtain evidence already held by the executing state, the issuing authority must assess whether the EIO complies with: (i) the classical principles of *necessity* and *proportionality* set out in Article 6(1)(a) of the Directive; and (ii) all the "material conditions" which, under the national law of the issuing state, define the possibility of "sharing evidence" in its domestic criminal proceedings. Specifically, the issuing authority must assess the impact and legal relevance of the fact that the executing state does not disclose the technical characteristics of the measures used to infiltrate the encrypted telecommunications system. It must also compare the categories of criminal offences under investigation, as well as the specific coercive measures by which the data to be "shared" were obtained. The lawfulness of issuing an EIO seeking to obtain evidence already held by the executing state does not grant the issuing state unrestricted freedom to use the evidence obtained through that EIO in its domestic criminal proceedings. The admissibility of such evidence – already in the possession of the executing state and subsequently shared with the issuing state – depends directly on: (i) the conditions and procedures under which the evidence was collected in the executing state; and (ii) the extent to which the accused was informed about those conditions and had the opportunity to effectively respond to them. If the accused's knowledge of the evidence is insufficient to enable them to properly and effectively express their views on its validity, lawfulness, authenticity, reliability, and other essential conditions and characteristics, such evidence may not be used in the evidentiary process conducted in the issuing state.

From the perspective of Article 31(1) and (3) of the Directive, if a specific measure – namely, one involving access to end-user telecommunications devices for the purpose of intercepting the flow, location, and metadata of internet-based communications – could not *in concreto* be applied on the territory of the issuing state under its national law, then the data obtained through such a measure by the intercepting (executing) state may not be used as incriminating evidence in the issuing state's criminal proceedings.

REFERENCES

Berlin Regional Court (Germany). (2022, October 19). Request for a preliminary ruling in the criminal case against M. N.

https://curia.europa.eu/juris/showPdf.jsf?text=&docid=268449&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=3474663 [accessed 29 March 2025].

Charter of Fundamental Rights of the European Union. (2016). OJ C 202/02, 389–405.

Court of Justice of the European Union. (2024, April 30). EncroChat, C-670/22. ECLI:EU:C:2024:372.

Derin, B., & Singelnstein, T. (2021). Use and exploitation of data from large-scale intrusions into information technology systems from abroad [Verwendung und Verwertung von Daten aus massenhaften Eingriffen in informationstechnische Systeme aus dem Ausland (EncroChat]. *Neue Zeitschrift für Strafrecht*, 449 - 454. (in German)

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, 1–36.

Federal Constitutional Court of Germany. (2024, November 1). Judgment in case No. 2 BvR 684/22. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2024/11/rk20241101_2bvr068422.html?nn=68080 [accessed 29 March 2025].

Gebhard, A., & Michalke, R. (2020). The end does not justify the means – The EncroChat complex and the limits of the use of evidence in criminal proceedings [Der Zweck heiligt die Mittel nicht – Der EncroChat-Komplex und die Grenzen strafprozessualer Beweisverwertung]. *Neue Juristische Wochenschrift*, 655–659. (in German)

Kipker, D.-K., & Bruns, H. (2022). EncroChat und die „Chain of Custody“. Digitale Ermittlungen als Bewährungsprobe für ein Recht auf faires Verfahren? [EncroChat and the "chain of custody": Digital investigations as a test case for the right to a fair trial?] *Multimedia und Recht*, 363–368. (in German)

Lenk, M. (2024). The development of European evidence law in light of the "EncroChat proceedings [Die Entwicklung des europäischen Beweisrechts im Lichte der „EncroChat-Verfahren]. *Europarecht*, 51–76. (in German)

The Code of Criminal Procedure of the Republic of Lithuania [Lietuvos Respublikos baudžiamojo proceso kodeksas] (2002). Official Gazette [Valstybės žinios], 37–1341. (in Lithuanian)

Lödden, C., & Makepeace, J. (2023). Same same but different: SkyECC – or how European law enforcement agencies intercepted a billion messages over 21 months [Same same but different: SkyECC oder wie europäische Strafverfolgungsbehörden eine Milliarde Nachrichten über 21 Monate lang abgefangen haben]. *HRRS*, December, 384–391. (in German)

Lödden, C., & Mania, L. (2025). No 'fear' of rule-of-law consequences of the KCanG – The limitation on use and the EncroChat decision of the Federal Court of Justice (BGH). [Keine 'Angst' vor rechtsstaatlichen Folgen des KCanG – Die Verwendungsschranke und die EncroChat-Entscheidung des BGH]. *HRRS*, January, 11–19. (in German)

Löffelmann, M. (2022). Exclusionary rule for data transfers from abroad [Verwertungsverbot bei Datentransfer aus dem Ausland]. *Juristische Rundschau*, 9, 454–460. (in German)

Meyer-Mews, H. (2024). EncroChat: Game, set, and match for the Berlin Regional Court. Commentary on the CJEU judgment, HRRS 2024 [EncroChat: Spiel, Satz und Sieg für das LG Berlin. Anmerkung zum Urteil des EuGH HRRS 2024] Nr. 644. *HRRS*, June, 191–197. (in German)

Meyer-Mews, H. (2025). Some remarks on the EncroChat decision of the Federal Constitutional Court (BVerfG) [Einige Bemerkungen zum EncroChat-Beschluss des BVerfG] HRRS 2025 Nr. 1. *HRRS*, January, 19–24. (in German)

Schmidt, A. (2022). On the admissibility in criminal proceedings of data from the surveillance of encrypted mobile phones by another EU Member State [Zur strafprozessualen

Verwertbarkeit der Daten aus der Überwachung verschlüsselter Mobiltelefone durch einen anderen Mitgliedstaat der EU] *Juristische Rundschau*, 134(4), 982–1015. https://doi.org/10.1515/zstw-2022-0029 (in German)

Škulić, M. (2024). Evidentiary value of information from communication conducted via applications / modified encryption devices – such as SKY ECC and EncroChat. [Dokazni značaj informacija iz komunikacije ostvarene aplikacijama / modifikovanim uređajima za kriptovanke – kao što su SKY ECC i EncroChat]. *Crimen*, 15, 3–55. (in Serbian)

Sommer, U. (2023). Chat about EncroChat. *Strafverteidiger Forum*, 7, 250–259. (in German)

Sommer, U. (2024). ANOM, or: how the rule of law can produce injustice. [ANOM oder: wie der Rechtsstaat Unrecht produzieren kann]. HRRS, December, 394–401. (in German)

German Code of Criminal Procedure [Strafprozessordnung] (2025, March, 29) https://www.gesetze-im-internet.de/stpo/ (in German).

Strate, G. (2022). EncroChat – some additional thoughts [EncroChat – einige ergänzende Gedanken]. *HRRS*, January, 15–18. (in German)

Strate, G. (2024). The CJEU decision on EncroChat. [Die EuGH-Entscheidung zu EncroChat]. *HRRS*, July, 226–231. (in German)

Zimmermann, F. (2022). The admissibility of foreign evidence in light of the EncroChat investigations. [Die Verwertbarkeit von Auslandsbeweisen im Lichte der EncroChat-Ermittlungen]. *Zeitschrift für Internationale Strafrechtswissenschaft*, 2, 173–190. (in German)