BRILL
NIJHOFF

EUROPEAN JOURNAL OF CRIME, CRIMINAL LAW AND
CRIMINAL JUSTICE 33 (2025) 235–262

European Journal of
Crime, Criminal Law
and Criminal Justice
brill.com/eccl

Encrochat and Sky ECC Data as Evidence in Criminal Proceedings in Light of the CJEU Decision

Vanja Bajović | ORCID: 0000-0002-7781-725X
Associate professor of Criminal Procedure, University of Belgrade Faculty of Law, Belgrade, Serbia
bajovic@ius.bg.ac.rs

Vesna Ćorić | ORCID: 0000-0003-4240-7469
Senior Research Associate, Institute of Comparative Law, Belgrade, Serbia
v.coric@iup.rs

Received 29 June 2024 | Accepted 24 October 2024 |
Published online 2 September 2025

Abstract

On April 30, 2024, the CJEU passed a decision in the case M.N. (EncroChat), clarifying some provisions of the Directive 2014/41/EU and indirectly imposing some conditions for the use of EncroChat material as evidence in criminal proceedings before national courts. This ruling is of particular importance as it represents the first ruling by a supranational judicial body related to the EncroChat communication platform. However, it has raised numerous dilemmas regarding its scope, implementation, and effects. The primary aim of this paper is to analyse the conditions imposed by the CJEU, with the goal of demonstrating that they embody fundamental values that should be upheld not only by EU Member States but also by candidate countries, which remain outside the European Investigation Order (EIO) system. Special attention is given to the case law of the European Court of Human Rights (ECtHR), given that in matters of criminal law and justice, the EU has historically relied on Council of Europe standards. This paper also seeks to provide legal proposals and practical guidelines for addressing the complex legal issues arising from the widespread use of encrypted communication platforms.

Published with license by Koninklijke Brill BV | DOI:10.1163/15718174-BJA10062
 | ISSN: 0928-9569 (print) 1571-8174 (online)

Keywords

EncroChat – Sky ECC – CJEU – rule of law – national sovereignty – fair trial

1 Introduction

The validity of evidence obtained by the interception of encrypted communication platforms EncroChat and Sky ECC was a subject of salient debate in academic literature and legal practice across Europe, before the Court of Justice of the European Union (CJEU), passed a decision clarifying some issues that were disputable in front of national courts (CJEU EncroChat decision).[1] Although the decision formally concerns the interpretation of certain provisions of the Directive 2014/41/EU (the EIO Directive), it essentially sets some rules regarding the use of EncroChat material as evidence in national criminal proceedings, clarifying that:

1. Not only judges, but public prosecutors as well, are competent to order the transmission of evidence already in the possession of the competent authorities of the executing state.
2. Investigative measures used to intercept telecommunications of all the users of EncroChat phones could have been ordered under the same condition in a similar domestic case.
3. The Member State on whose territory the subject of interception is located must be notified about the interception of telecommunications.
4. The rights of users affected by interception must be protected.
5. In criminal proceedings, national courts must disregard information and evidence if the defendant is not in a position to comment on that information/evidence and if said information/evidence is likely to have a preponderant influence on the findings of fact.

This decision is particularly important as it represents the first ruling by a supranational judicial body related to the EncroChat communication platform. However, it has raised numerous dilemmas in both legal theory and practice regarding its scope, implementation, and effects, leaving ongoing uncertainties about the use of this material as evidence in criminal proceedings worldwide. Since the decision imposes certain limitations on the use of EncroChat and Sky ECC evidence, it is not seen as favourable by prosecutors. Consequently,

1 CJEU 30 April 2024, Case 670/22 (M.N.-EncroChat).

a thesis has emerged in the public discourse of some EU candidate countries, suggesting that it applies only to EU Member States, not to countries outside the EIO system, and that it pertains exclusively to EncroChat data, rather than Sky ECC data.[2]

Contrary to this view, our starting hypothesis is that the conditions outlined in the CJEU EncroChat decision should also apply to Sky ECC data, and that these conditions should be respected not only by EU candidate countries but by all countries committed to upholding the rule of law and safeguarding their sovereignty.

Firstly, we draw upon the definition of data-driven criminal investigations offered by Oerlamans and Royer, which describes such investigations as being driven by the collected data, leading to new criminal investigations.[3] The use of both EncroChat and Sky ECC falls under this definition. Following this approach, we argue that the outcome of the EncroChat decision is equally relevant for the use of both EncroChat and Sky ECC data, warranting the application of the same rules. Both platforms involve mobile phones equipped with special software and hardware that enable end-to-end encrypted communication, and it is interesting coincidence that in both cases, data collection was based on orders from the same court in Lille, France.

Secondly, we aim to demonstrate that the conditions established by the CJEU EncroChat decision should be respected by courts in EU candidate countries and in all other countries dedicated to upholding the rule of law and national sovereignty. In this context, we explain that the CJEU's requirement for the possibility of obtaining this material through 'domestic' investigative measures reflects the principle of legal certainty, a core element of the rule of law, while the notification requirement reflects the necessity of protecting national sovereignty and individual rights.

This leads to the key research question of this paper: How does the CJEU EncroChat decision impact the principles of the rule of law, privacy and fair trial in both EU Member States and candidate countries, particularly in the context of cross-border mass surveillance, and the admissibility of evidence obtained abroad through investigative measures unrecognized in domestic law?

2 This thesis is prevalent in Serbian and Montenegrin public discourse and has frequently been referenced in jurisprudence as well. See, for example: N. B. Šaranović, Presuda Suda Evropske Unije u predmetu "M.N. EncroChat": Granice tumačenja, *Vijesti,* 09 May 2024, available at: https://www.vijesti.me/kolumne/706133/presuda-suda-evropske-unije-u-predmetu-m-n-enchrochat-granice-tumacenja.

3 J. Oerlemans, S. Royer, 'The future of data driven investigations in light of the Sky ECC operation', *New Journal of European Criminal Law*, Vol. 14(4), (2023), p. 440.

We will address this main research question through four sub-questions, explored in four sections:

Section 2 discusses the challenges of using evidence obtained in a foreign country, analysing how the principle of legal certainty conflicts with the use of evidence gathered through investigative measures that are not permitted under domestic law.

Section 3 addresses the complexities introduced by the global nature of electronic communication in the context of surveillance and criminal investigations. With the rise of the internet and digital technologies, it has become possible for states to conduct investigative measures beyond their territorial borders, raising concerns about national sovereignty. The question is: How does the use of bulk interception in the EncroChat and Sky ECC cases align with the legal standards set by the ECtHR, and what are the implications for national sovereignty?

Section 4 focuses on two critical issues concerning the use of EncroChat data in national courts: How do the principles of the right to privacy and the right to a fair trial interact in cases where bulk interception, such as that used in the EncroChat and Sky ECC cases, is employed to gather evidence?

Section 5 examines the implications of the CJEU EncroChat Decision, particularly its application to EU Member States and candidate countries. In this section, we aim to challenge the perspective that the CJEU decision applies solely to EU Member States. We argue that the principles established by the CJEU EncroChat decision, including those related to the rule of law and the right to a fair trial, should also be respected by candidate countries, even though they are not yet part of the EIO framework.

The CJEU's condition related to the national authority for issuing and transmitting an EIO is left out of this analysis, as it is a formal condition tied exclusively to the EIO, not to the evidential value of data collected from mobile phones equipped with the EncroChat application. Instead, we focus more on contentious issues, such as the legitimacy of bulk interception in light of the ECtHR case law and the protection of defendants' rights, which is crucial for ensuring equality of arms between individuals and the state.

2 Diversity of Investigative Measures in Different Countries and Admissibility of Evidence Obtained Abroad

Investigative measures and the rules concerning evidence differ significantly at the national level, even within the EU Member States. This diversity complicates efforts to create 'an area of free movement of criminal evidence'

although the EIO Directive aimed to improve cooperation in cross-border evidence gathering.

In accordance with Article 6(1)(b) of the EIO Directive, the issuing authority must check whether the investigative measure(s) indicated in the EIO could have been ordered under the same conditions in a similar domestic case. In the EncroChat case, the CJEU gives the further explanation of this provision clarifying that:

> Through the use of the words 'under the same conditions' and 'in a similar domestic case', Article 6(1)(b) of Directive 2014/41 makes the determination of the precise conditions required in order for an EIO to be issued dependent on the national law of the issuing State alone.[4]

The CJEU also clarified that Article 6(1)(b) of the EIO Directive does not require that the issuance of an EIO for the transmission of evidence already in the possession of the competent authorities of the executing State should be subject to the same substantive conditions as those that apply in the issuing State in relation to the gathering of that evidence.[5] Instead, this article seeks to ensure that the rules and guarantees provided for by the national law of the issuing State are not circumvented.[6]

The challenge in many countries is that EncroChat and Sky ECC data could not have been obtained using their available technology and investigative measures, such as wiretapping or data production orders.[7] These data were obtained in France, under Article 706-102-1 of the French Criminal Procedure Code (CPC), which regulates the capturing of computer data through the installation of technical devices, essentially referring to hacking a computer or server.

According to the joint report of Europol and Eurojust, only a few of European countries have specific regulations regarding secret access to and decoding of encrypted electronic communications (e.g., online surveillance, intrusion into a computer system or the use of technical means to access digital evidence).[8]

---

4 CJEU EncroChat decision, para. 92.

5 CJEU EncroChat decision, para. 96.

6 CJEU EncroChat decision, para. 97.

7 "End-to-end encryption (E2EE) is a system that allows mobile phone users to communicate with each other without anyone else eavesdropping. So, the police cannot listen in either, even if they are authorized to tap the communication." See: Hartel, P., & van Wegberg, R. 'Going dark? Analysing the impact of end-to-end encryption on the outcome of Dutch criminal court cases' *Crime Science*, 12(1) (2023), https://doi.org/10.1186/s40163-023-00185-4.

8 Only Denmark, France, Germany, Poland, Sweden, Switzerland and The Netherlands have provisions that specifically address the use by law enforcement authorities of technical

Such measures typically involve the covert installation of special software in devices, either physically if the investigative authorities have access to the device or remotely, by inserting viruses or Trojans, which copy all content from the device and forward it to the police or prosecutor.[9] This basically refers to hacking, although this term is not used in criminal procedure codes. However, there is still no general consensus on the acceptance of such measures, primarily due to fears that they would represent an excessive intrusion into the rights of individuals.[10]

Therefore, the question is whether EncroChat (and Sky ECC) data may be used as evidence in countries that do not have equivalent investigative measures capable of obtaining such data. An affirmative answer would open the door to numerous manipulations, enabling a country, whose legal framework lacks such investigative measures, to deliberately seek their implementation from another country, thereby circumventing domestic evidentiary rules. This would enable countries to obtain surveillance material concerning their own citizens that would otherwise be inaccessible under their own legal framework.

Such a practice could potentially encourage so-called *forum shopping*, where law enforcement authorities intentionally request an investigative measure in a country with significantly lower standards for the protection of the fundamental rights, knowing that the results will be accepted.[11] For example, if the investigative authorities of state A are unable to obtain a warrant for

---

tools to attack encryption. Italian courts also have accepted the use of Trojan software which, after being "inserted" into the device, allows access to all the data contained within it. The Italian Supreme Court of Cassation has taken the position that the application of this measure is possible only in criminal proceedings for the most serious crimes, such as terrorism, organised crime, etc. See: Europol & Eurojust, *Third Report of the Observatory Function on Encryption*, (European Union, 2021), 11–13.

9 P. Hartel and R. van Wegberg explain that, with the permission of the examining magistrate, the police may install key logger malware on a smartphone. The key logger reports the passcode without the suspect knowing. Hartel, P., van Wegberg, R. *op.cit*., p. 3.

10 The Constitutional Court of Austria, for example, declared unconstitutional a CPC provision that regulated the installation of a special program (Federal Trojan) in a computer system to monitor and record encrypted messages. The court argued that such provisions were incompatible with Art. 8 ECHR, as their widespread use could allow law enforcement authorities to draw comprehensive conclusions about a person's preferences, inclinations, orientation, attitudes and lifestyle. It also emphasized that there are no guarantees that the measure can be limited only to detecting and proving the most serious forms of crime, as it gives the competent authorities the opportunity to monitor the entire Internet communication. See: Constitutional Court of Austria, AUT-2019-3-003, https ://www.vfgh.gv.at/downloads/Bulletin_2019-3_AUT-2019-3-003_G_72-74_2019__ua.pdf.

11 See: Z. Burić, M. Engelhart, A. Novokmet, S. Roksandić, 'Upotrebljivost rezultata masovnog nadzora komunikacija kao dokaza u hrvatskom kaznenom postupku-slučaj SKY ECC', *Hrvatski ljetopis za kaznene znanosti i praksu* (Zagreb), vol. 30, broj 2/2023, p. 266.

intrusion into a computer system because these measures are not permitted under domestic law, they could request state B to implement such measure on citizens of state A. In this way domestic rules are circumvented, and the rule of law is compromised, particularly legal certainty as one of its crucial elements.[12]

Legal certainty requires that laws must be easily accessible and foreseeable, meaning they should be promulgated in advance of their implementation and their effect must be predictable.[13] Investigative measures, by their nature, restrict fundamental rights and any such restriction must be "provided" or "prescribed" by law. The ECtHR has held that the phrase "prescribed by law" means the contested measure must have a legal basis in domestic law and that the law in question must be of sufficient quality- accessible to the person concerned and foreseeable in its effects.[14] If an investigative measure is not prescribed by domestic law, this principle is undermined, as foreign law is neither sufficiently accessible nor formulated with the necessary precision for domestic citizens.

Furthermore, the rule of law requires that all public authorities must operate within legal constraints that uphold democratic values and respect fundamental rights.[15] The law must clearly define the scope of discretion granted to the executive and the manner in which it can be exercised.[16] Otherwise, countries could obtain surveillance material concerning their citizens, that would be unattainable under their domestic legal framework, thereby nullifying legal certainty.

For this reason, Article 6(1)(b) of the EIO Directive seeks to ensure that the rules and guarantees provided by the national law of the issuing state are not evaded, requiring that the investigative measure(s) indicated in the EIO could have been ordered under the same conditions in a similar domestic

12 The rule of law is specifically mentioned in Article 2 of the Treaty of European Union (TEU) as one of a fundamental value on which the EU is founded. According to the definition provided by the European Commission it requires legality, legal certainty; prohibition of arbitrariness of the executive powers; independent and impartial courts; effective judicial review including respect for fundamental rights; and equality before the law. See: European Commission, Communication: A New EU Framework to Strengthen the Rule of Law, COM (2014) 158 Final, Brussels, 11.3.2024., p. 4.

13 Report on the rule of law-Adopted by the Venice Commission at its 86th plenary session (Venice, 25–26 March 2011), para. 44.

14 İzzettin Doğan and Others v. Turkey, App. no. 62649/10 (ECtHR 26 April 2016), para. 99, Hamidović v. Bosnia and Hercegovina, App. No. 57792/15, (ECtHR 5 December 2017), para. 32.

15 See more on the core meaning of the rule of law (as determined by the EU and Venice Commission): L. Pech, 'The Rule of Law as a Well Established and Well Defined Principle of EU Law', *Hague Journal on the Rule of Law,* Vol. 14, (2022), pp. 122–123.

16 Hasan and Chaush v. Bulgaria, App. no. 30985/96 (ECtHR 26 October 2000), par. 84, Maestri v. Italy, App. no. 39748/98 (ECtHR 17 February 2004), para. 30.

case. This means that the requesting country must be capable, through its own investigative measures, to obtain the EncroChat communication. Accordingly, German courts, when deciding on the admissibility of EncroChat data, compared the measure used to obtain the evidence in France with online surveillance as regulated by Article 100b of German CPC,[17] but there are still doubts about whether this measure can be equated with the one applied in France.[18] Similarly, in the Netherlands, the measure is compared with those described in Article 126 of the Duch CPC, such as reading and analysing confiscated smartphones, placing telephone or internet taps, obtaining cell tower data from a telecom provider to trace the location of a mobile phone, or hacking the computer or another device of the offender.[19]

In countries that do not regulate investigative measures analogous to the one implemented in France the investigative measure indicated in the EIO could not have been issued at all. Therefore, it is pointless to examine whether it could be issued "under the same conditions, in a similar domestic case".[20] The principle of legal certainty requires that in these countries, material obtained by capturing EncroChat data through the installation of technical devices cannot be used as evidence.

3 Interception of Telecommunications on the Territory of Another State and Legitimacy of Bulk Interception

Each country is authorized to carry out investigative measures on its own territory. Just a few decades ago, conducting investigative measures on the territory of one state without the knowledge and consent of another state

17 Hanseatisches Oberlandesgericht Hamburg 1. Strafsenat, 1 Ws 2/21, 1 Ws 2/21—7 OBL 3/21, 29.01.2021, para. 93, available at: https://www.landesrecht-hamburg.de/bsha/document/NJRE001454728.

18 However, on 19 April 2024, the Regional Court in Berlin officially registered the second reference for a preliminary ruling in the EncroChat case: Case C-675/23 (Staatsanwaltschaft Berlin II). This request seeks clarification on whether the requirements under Article 6 of the EIO Directive (specifically, the condition that an EIO can only be issued under the same conditions in a similar domestic case) have been met. The Berlin court contends that a corresponding measure—an online search as regulated by the German Code of Criminal Procedure—would never have been permissible if the server had been infiltrated within German territory. See: T. Wahl, *Second Reference for Preliminary Ruling in EncroChat Case*, 13 August 2024, available at: https://eucrim.eu/news/second-reference-for-preliminary-ruling-in-encrochat-case/.

19 P. Hartel, P., R. van Wegberg, *op. cit.,* p. 2.

20 Burić et al. also point out that it is an aggravating circumstance for accepting Sky ECC evidence that the Croatian judicial body requested the transmission of evidence that cannot be obtained under Croatian law at all. See: Z. Burić, M. Engelhart, A. Novokmet, S. Roksandić, *op. cit.,* p. 261.

was unthinkable. With the development of the internet, this has become possible, given that communication takes place through servers and internet service providers located in different countries. Crime today is also difficult to limit territorially, especially with the growing importance of digital evidence, which may not be physically present in the state where the crime occurred. Consequently, electronic evidence introduces a cross-border element in almost every criminal investigation and procedure.[21]

Efficiently fighting crime requires effective international cooperation, but the question arises whether State A can monitor the communication of individuals located on the territory of State B, without the knowledge and consent of State B? An affirmative answer would challenge the principle of national sovereignty. It would, in effect, grant states with mass surveillance technologies the power to monitor the entire world, including not only criminals but also politicians, journalists, NGO activists, and others. This would be a significant step toward global totalitarianism, or a so-called Orwellian society.

On the other hand, modern crime, terrorism, and other threats to national security are not confined to the borders of a single state. As a result, protecting the state and its citizens often requires the implementation of certain measures beyond territorial borders. This phenomenon is not new- espionage activities have always taken place abroad. However, the internet offers unprecedented opportunities, not only to criminals but also to states equipped with mass surveillance and data processing technologies. In recent years, there has been a shift from targeted surveillance of specific individuals to random, or bulk interception, raising the question of which category the EncroChat and Sky ECC interceptions fall into.

3.1 *Bulk Interception in the Case-Law of the ECtHR*

In its earlier case law, the ECtHR primarily focused on issues of mass surveillance of communications confined within the borders of a single state.[22] However, with the advent of the Internet and digital technologies, this form of surveillance has expanded to a nearly global scope. The bulk interception of communication of persons outside a state's territorial jurisdiction was

21 European Law Institute, *ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings* (2023) 11.

22 See, for example: Klass and Others v. Germany, App. 5029/71 (ECtHR 06 September 1978); Weber and Saravia v. Germany, App. 54934/00 (ECtHR 29 june 2006); Liberty and Others v. the United Kingdom, App. 58243/00, (ECtHR 01 July 2008); Kennedy v. the United Kingdom, App. 26839/05, (ECtHR 18 May 2010); Roman Zakharov v. Russia, App. 47143/06 (ECtHR 04 December 2015); Szabo and Vissy v. Hungary, App. 37138/14 (ECtHR 12 January 2016).

examined in the cases Big Brother Watch and Others v. The United Kingdom"[23] and Centrum for Rattvisa v. Sweden.[24] In both cases, the ECtHR addressed bulk interception regimes established for national security purposes and inter-state intelligence sharing.

According to ECtHR estimation, at least seven Council of Europe Member States (Finland, France, Germany, the Netherlands, Sweden, Switzerland and the United Kingdom) officially operate bulk interception regimes over cables and/or the airways, while in Norway a draft law authorising bulk interception is being debated.[25] Following that, Judge Pinto de Albuquerque reasonably concludes that non-targeted bulk interception is explicitly or implicitly prohibited in twenty-three European states.[26]

In the cases Big Brother and Centrum for Rattvisa, the ECtHR made clear distinctions between different types of interceptions:

1. Bulk interception is generally directed at international communication, that physically cross state borders, while targeted interception is directed at internal communication of specific individuals within the state's borders. Although bulk interception may include the communications of individuals within the surveilling state, its primary purpose is often to monitor communications of individuals outside the state's territorial jurisdiction- communication that cannot be captured through other forms of surveillance.[27]
2. Targeted interception is primarily used for investigating specific serious crimes, while the bulk interception regime is primarily used for foreign intelligence gathering. However, bulk interception can also be applied to the early detection and investigation of certain crimes, such as cyberattacks, counterespionage, and counterterrorism.[28]
3. Targeted interception is directed against specific individuals, while bulk interception captures communications of all users of the internet or particular communication platforms. Even when bulk interception

23 Big Brother Watch and Others v. The United Kingdom, App. 58170/3, 62322/14 and 24960/15 (ECtHR 25 May 2021).

24 Centrum for Rattvisa v. Sweden, App. 35252/08 (ECtHR 25 May 2021).

25 ECtHR, Big Brother Watch, paras. 242, 243.

26 It is explicitly or implicitly prohibited in Albania, Andorra, Austria, Belgium, Bosnia and Herzegovina, Croatia, the Czech Republic, Greece, Ireland, Iceland, Italy, Liechtenstein, Moldova, Monaco, Montenegro, North Macedonia, Poland, Portugal, Romania, San Marino, Serbia, Turkey and Ukraine. See: Judge Pinto de Albuquerque, *Partly Concurring and Partly Dissenting Opinion of Judge Pinto de Albuquerque in Big Brother Case*, para. 11.

27 ECtHR, Big Brother Watch, para.344, ECtHR, Centrum for Rattvisa, para. 258.

28 ECtHR, Big Brother Watch, para. 345, ECtHR, Centrum for Rattvisa, para. 259.

> is used to target specified individuals, it does not monitor their devices directly; instead, it "targets" them by applying strong selectors to the communications.[29]

According to available data, the surveillance of EncroChat devices was initially authorized in a criminal case against the EncroChat company. However, this authorization resulted in the interception of communications from thousands of users worldwide, leading to the initiation of numerous criminal proceedings. The method used in the operation closely resembles bulk interception rather than targeted interception, as it focused on the communication carriers (all EncroChat and Sky ECC phones) rather than specific devices of specific users. In the Big Brother Watch case, the European Court of Human Rights (ECtHR) described bulk interception as "in the absence of any limit on the number of communications which could have been intercepted, it would appear that all packets of communications flowing across the targeted bearers while the warrant was in force were intercepted."[30] This description is fully applicable to the EncroChat and Sky ECC cases.

Furthermore, the majority of intercepted communications were "international," crossing French borders, and were initially used not for specific investigations but for the early detection of certain crimes. In most cases, criminal proceedings were initiated only after France submitted EncroChat and Sky ECC data to other countries. Considering these factors, the interception of EncroChat and Sky ECC communications constituted bulk interception, targeting not only specific individuals but all users of these platforms, both within France and globally.

3.2 *Legitimacy of the Bulk Interception in the Case-Law of the ECtHR*

The ECtHR did not take a clear position about the legitimacy of bulk interception, focusing instead on whether the domestic legal framework of the surveilling state (more precisely the United Kingdom in the *Big Brother Watch* case) contains sufficient guarantees against abuses. The Court held that Article 8 of the European Convention on Human Rights (ECHR) does not in principle prohibit the use of bulk interception to protect national security and other essential national interests against serious external threats. However, when operating such a system, the margin of appreciation afforded to states must be narrower, and a number of safeguards must be in place to prevent potential abuse.[31]

29 ECtHR, Big Brother Watch, para. 346, ECtHR, Centrum for Rattvisa, para. 260.
30 ECtHR, Big Brother Watch, para. 372.
31 ECtHR, Big Brother Watch, para. 347.

By taking this stance, the ECtHR deviated from its earlier jurisprudence, which generally deemed bulk interception and indiscriminate surveillance of communications as incompatible with the ECHR.[32] This shift is justified by technological advancements that have significantly altered the way people communicate. Today, the vast majority of communications "take digital form and are transported across global telecommunications networks using a combination of the quickest and cheapest paths without any meaningful reference to national borders."[33] In light of these changes, it becomes essential to assess whether the domestic legal framework of the intercepting state provides adequate safeguards against abuse. Consequently, this framework must clearly define:

1. The grounds on which bulk interception may be authorised,
2. The circumstances in which an individual's communications may be intercepted
3. The procedure for selecting, examining, using and storing the obtained material
4. The precautions to be taken when communicating the material to other parties
5. The limits on the duration of interception and the circumstances in which such material must be erased and destroyed
6. The procedures for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance
7. The existence of notification mechanisms, and
8. The remedies provided for by national law.[34]

Applied to the EncroChat (and Sky ECC) cases, it should be determined whether these guarantees were respected by France, given that the interception measures were ordered by a French court. Since the collection of EncroChat

32 For instance, in Roman Zakharov v. Russia, the ECtHR found the practice of authorizing surveillance of all communications in the area where a crime was committed unacceptable, particularly when no specific person or phone number was identified for wiretapping (Roman Zakharov v. Russia, App. 47143/06, ECtHR, 4 December 2015, para. 265). In Mustafa Sezgin Tanrıkulu v. Turkey, the ECtHR criticized a Turkish decision that allowed the surveillance of electronic and telephone communications of anyone in Turkey, ostensibly to prevent the activities of criminal organizations (Mustafa Sezgin Tanrıkulu v. Turkey, App. 27473/06, ECtHR, 18 July 2017). In Szabó and Vissy v. Hungary, the ECtHR condemned the unlimited surveillance of a large number of citizens in the fight against terrorism (Szabo and Vissy v. Hungary, App. 37138/14, ECtHR, 12 January 2016, paras. 63, 67. Szabo and Vissy v. Hungary, App. 37138/14, ECtHR, 12 January 2016, paras. 63, 67).

33 ECtHR, Centrum for Rattvisa, para. 236.

34 ECtHR, Big Brother Watch para. 275.

data has been classified as a defence secret in France, it remains difficult to assess whether these minimum guaranties were respected, until the French government provides the responses requested by the ECtHR in 2021.[35]

What distinguishes the EncroChat and Sky ECC cases from the bulk interception cases previously approved by the ECtHR is that, in *Big Brother Watch* and *Centrum för Rättvisa*, the focus was on foreign intelligence gathering by intelligence agencies for national security purposes, whereas in the EncroChat and Sky ECC cases, bulk interception was used to gather evidence for criminal proceedings. Although the ECtHR did not rule out the use of bulk interception for investigating serious crimes in *Big Brother Watch*, it did not specify the criteria under which prosecution authorities could conduct bulk interception of communications from individuals outside the state's territorial jurisdiction for criminal investigations.

Generally, intelligence is not gathered under the same evidentiary rules as criminal evidence because it serves a distinctly different purpose. While evidence is specifically collected for criminal investigations, intelligence is primarily gathered for national security purposes. Shared intelligence remains the property of the originating agency and cannot be further disclosed or used by the receiving agency without explicit written consent. Some scholars argue that the data gathered from hacking should be treated as intelligence to guide the course of an investigation and should not be presented in court as evidence.[36] Similarly, Stoykova suggests that, given the large number of suspects and data collection, it is more likely that the EncroChat operation can be classified as a criminal intelligence operation aimed at collecting, processing, and analysing information about crime or criminal activities.[37]

35 Following the petition filed by two British nationals whose EncroChat communication were accepted as evidence in British courts, the ECtHR requested that the French government provide the following details: How many devices were involved in the data capture? What was the nature of the data collected? What guarantees against arbitrariness and abuse were provided at the stage of: a. the examination, selection, use, and storage of the captured data? b. the transmission of this data to third parties? c. the timely destruction of the captured data and related analysis and judicial documents? Did individuals suspecting surveillance of their data have the right to access data concerning them or to be informed of the existence of such measures? Was a mechanism for subsequent notification provided? Were remedies available through an independent body or courts in case of abuse? See: A.L. v. France (no. 44715/20) and E.J. v. France (no. 47930/21), European Court of Human Rights- Press Unit, *Mass surveillance* (June 2024), available at: https://www.echr.coe.int/documents/d/echr/fs_mass_surveillance_eng.

36 P. Sommer, 'Evidence from hacking: A few tiresome problems', *Forensic Science International: Digital Investigation 40* (2022) 301333.

37 R. Stoykova,'Encrochat: The hacker with a warrant and fair trials?', *Forensic Science International: Digital Investigation 46* (2023), p.3. https://doi.org/10.1016/j.fsidi.2023.301602.

Given the secrecy surrounding the entire operation, we cannot rule out the possibility that EncroChat and Sky ECC data were technically obtained through measures authorized under the 2015 French Intelligence Act,[38] which permits highly invasive surveillance techniques such as network exploitation, computer hacking, and the use of "black boxes" to scan internet content for suspicious URLs.[39] However, analysing such speculations is beyond the scope of this paper. In any case, labelling the acquisition of EncroChat data as a "defence secret" and selectively sharing this material with other countries raises suspicions about the legal nature of EncroChat and Sky ECC data. If treated as evidence, the question arises whether such data could be lawfully collected through bulk interception of communications outside of French territorial jurisdiction. Conversely, if treated as intelligence, the issue is whether it can be legitimately used as evidence in criminal proceedings.

3.3 *Surveillance of Communication in Foreign Territories and Notification Criteria*

The CJEU did not examine how the data was obtained in France, nor did it address the legitimacy of bulk interception. Instead, it relied on the principle of mutual trust and the presumption that the procedure by which France gathered the evidence was lawful. It was stated that when the issuing authority seeks, via an EIO, the transmission of evidence already in the possession of the competent authorities of the executing State, the issuing authority is not permitted to review the lawfulness of the separate procedure by which the executing Member State gathered the evidence. The CJEU further explained that any other interpretation of Article 6(1) of the directive would result, in practice, in a more complicated and less effective system, which would undermine the objective of that directive."[40] Instead, the CJEU focused on whether EU Member States must be notified about the interception of communications on their territory.

Article 31 of the EIO Directive requires the intercepting Member State to notify the competent authority of the notified Member State, from which no technical assistance is needed, regarding the interception. Notification may occur before, during or after the interception. Logically, prior notification can only occur if the competent authority is aware, at the time of ordering the

38 For more information about the French Intelligence Act of 2015 see: Wanda Mastor, 'The French Intelligence Act: "The French Surveillance State?": A comparison with the USA PATRIOT Act and FREEDOM Act' *European Public Law,* 2017, vol.23 (no. 4), pp. 707–722.

39 V. Bajović, 'EncroChat i Sky ECC komunikacija kao dokaz u krivičnom postupku', *Crimen* 2/2022, (2022) pp. 167–169.

40 CJEU EncroChat decision, para. 100.

measure, that the subject of the interception is, or will be, on the territory of the notified Member State. In other cases, foreign countries should be notified during or after the interception, as soon as the intercepting country becomes aware that the subject of interception is located within another state's territory. According to the CJEU's interpretation, Article 31 of the EIO Directive is intended not only to guarantee respect for the sovereignty of the notified Member State but also to ensure that the guaranteed level of protection in that Member State is not undermined.[41]

This implies that France was obliged to notify other countries about the interception if the subjects of interception were located on their territory. It is reasonable to assume that France could not have known, prior to the EncroChat and Sky ECC interception, where individuals using these phones would be located. Rather, the question is whether other countries were notified about the interception immediately after France became aware that the subjects were within their jurisdiction. To assess this, it is crucial to establish when France obtained data related to the subject of the interception and when the competent authority of another state was notified about it, what is extremely difficult to prove. Given that the exact method of obtaining that data is classified as a 'defence secrets', it will be challenging to determine when France came into possession of the data and decrypted the communications relating to a specific person.

The 'notification' criteria remain highly controversial in national laws as well. In many countries, individuals may remain unaware that their communications have been intercepted unless criminal proceedings are initiated and the intercepted data is used as evidence, or unless this information is leaked through other means.[42] However, in cases of the bulk interception, the notification requirement has little practical effect, as such surveillance is often used for foreign intelligence gathering and primarily targets the communications of individuals outside the state's territorial jurisdiction.[43]

If we assume that the EncroChat (and Sky ECC) interception constituted bulk interception of these platforms, it is logical to conclude that the communications of all individuals using EncroChat or Sky ECC devices were intercepted. In the absence of a notification requirement for bulk interception, the ECtHR has emphasized the importance of domestic legal systems to establish an independent body capable of examining, through an adversarial process, the remedies available to all individuals who suspect their communications

41 CJEU EncroChat decision, para. 124.
42 ECtHR, Roman Zakharov, para. 289.
43 ECtHR, Big Brother Watch, para. 358.

have been intercepted.[44] For example, in the United Kingdom, any person who suspects he or she were under surveillance can appeal to the Investigatory Powers Tribunal, which does not require prior notification of surveillance for its jurisdiction to apply. This mechanism upholds the right to an effective remedy as stipulated in Article 13 of the ECHR.

On the other hand, the "notification" requirement outlined in Article 31 of the EIO Directive were designed not only to protect the individual's right to an effective remedy but also to safeguard national sovereignty.[45] Consequently, any breach of the notification requirement under Article 31 of the EIO Directive is both a legal and a political issue, as the principle of mutual trust could be jeopardized if one Member State intercepts the communications of citizens in another Member State without notifying its competent authority.

4 Integrity of the Data and Right to a Fair Trial

The integrity of the data and the right to a fair trial are crucial considerations when dealing with EncroChat and Sky ECC material in national courts. Particularly, questions arise regarding whether its use and the methods of its acquisition are in accordance with the right to a fair trial and the right to privacy. The right to privacy is primarily considered from the perspective of those EncroChat and Sky ECC users, who were not involved in criminal activities.

4.1 *Right to Privacy*

Article 8 of the ECHR guarantees the right to respect for private and family life, home, and correspondence. It stipulates that public authorities shall not interfere with the exercise of this right except in accordance with the law and when necessary, in a democratic society, in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

It is indisputable that the interception of communication platforms EncroChat and Sky ECC has contributed to the detection and prevention of many criminal acts, which, in accordance with paragraph 2 of Article 8 of the ECHR, justifies the intrusion by public authorities into individuals' right to privacy. The surveillance measures clearly served legitimate aims, such

44 ECtHR, Big Brother Watch, para. 359.

45 CJEU EncroChat decision, para. 124.

as protecting national and public safety, preventing disorder and crime, and safeguarding the rights and freedoms of others. However, what remains debatable is whether this "intrusion" was conducted in accordance with the law and the standards set by the ECtHR, particularly given that the measures did not exclusively target the communication of "criminals" but affected all users of EncroChat and Sky ECC devices. These devices were not illegal, their possession and use were lawful, and the platforms had thousands of users worldwide,[46] many of whom, logically, were not part of the "criminal milieu."

In one of the first decisions related to EncroChat, the Higher Regional Court of Hamburg noted that, according to data from French authorities, the interception affected 32,477 users across 121 countries. Of these, 380 users were located entirely or partially within French territory, and according to French authorities, at least 242 individuals—over 60%—were using the encrypted communication system for criminal purposes.[47] It has been also emphasized in theory that a significant number of individuals were using the service for legitimate purposes—to protect their privacy, confidential information, intellectual property, etc.[48]

Through the interception, the French authorities gained access to the communication and data of all its users, i.e., the entire communication that took place through these platforms. A similar situation would arise, for example, if the authorities were to monitor all communication on platforms like Viber or WhatsApp. This type of surveillance raises concerns about communication that enjoys special protection. For instance, it is conceivable that lawyers used these devices to communicate with clients, or that journalists or politicians used them to exchange confidential information. Furthermore, such operations rise concerns about the privacy of users of "ordinary" mobile phones, which are generally far less secure than EncroChat or Sky ECC devices, but still contain significant personal data—such as personal documents, bank accounts, private photos, and more.

---

46 In accordance with some estimations, in the EncroChat operation, French law enforcement authorities collected over 120 million messages from 60.000 EncroChat users, while in the Sky ECC operation they collected approximately 1 billion messages from 70,000 phones all over the world. J.J. Oerlemans, S. Royer, *op.cit.,* p. 435.

47 Hanseatisches Oberlandesgericht Hamburg 1. Strafsenat, decision of 29.01.2021.- 1 Ws 2/21, 1 Ws 2/21—7 OBL 3/21, para. 8. It was further stated in the same decision that the remaining 40% of users were either inactive or had not yet been analysed at that time. However, it has not been disclosed whether this 40% has since been analysed. Therefore, it is reasonable to assume that these data remain relevant, based on the presumption that if all users had been found to be involved in criminal activities, France would have disclosed this to justify the scale of the surveillance.

48 R. Stoykova, *op. cit.,* p. 6.

The unconditional use of EncroChat and Sky ECC evidence could be defended by arguing that the fight against crime is justified by the fact that France, for instance, provided other countries only with data related to the activities of criminal groups within their territories, not those related to the communication of law-abiding citizens, politicians, journalists, civic activists and the like. Additionally, the receiving state will not submit a formal request if it does not plan to initiate criminal proceedings against certain individuals.

However, both arguments are open to criticism. First, if France provided only selected data (primarily related to criminal groups), it suggests that the surveillance state (France) retains all the data and can share it selectively, according to its own interests. Secon, if national authorities were given access to all the data, but they chose to initiate criminal proceedings against only certain individuals, it indicates that the national authorities are also acting selectively, potentially driven by political interests. In both scenarios, selective justice is at play, and the principles of equality before the law are seriously undermined.[49]

In any case, even if the ECtHR finds that Article 8 of the ECHR has been violated, it is unlikely to have a significant impact on the criminal proceedings and judgments of national courts that have used EncroChat data as evidence.[50] Starting with the case of Schenk v. Switzerland,[51] the ECtHR has consistently held that using evidence obtained in violation of Article 8 does not make the proceedings unfair, as long as the illegal surveillance is not the sole basis for conviction. The Court also assesses the quality of the evidence, particularly whether the conditions of its acquisition cast doubt on its accuracy or reliability.[52] A violation of Article 8, however, will not overturn a conviction

49 For example, there has been a lot of speculation in the Serbian public about the identity of a certain "Oscar," who is mentioned in the correspondence of many criminals. Opposition politicians have even claimed that "Oscar" is the President of the Republic. Such speculations have never been clarified, as the correspondence involving "Oscar" has never been disclosed, the prosecution has not established who is behind that nickname, nor has any procedure been initiated to determine it. This arouses public distrust in the work of institutions. See: Radar: Why did Vučić keep silent about the connections between officials and criminals revealed by SKY (March, 2024) https://en.vijesti.me/world/balkan/700200/radar%2C-what-vucic-kept-silent-about-the-connections-between-officials-and-criminals-revealed-by-sky.

50 J.J. Oerlemans, S. Royer, *op. cit.,* p. 456.

51 Schenk v. Switzerland, App. 10862/84 (ECtHR 12 July 1988).

52 Khan v. the United Kingdom, App. 35394/97 (ECtHR 12 May 2000) para. 34–40; P.G. and J.H. v. the United Kingdom, App. 44787/98 (ECtHR 25 September 2001) para. 76–81; Bykov v. Russia, App. 4378/02 (ECtHR 10 March 2009), para. 90; Hambardzumyan v. Armenia, App. 43487/11 (ECtHR 5 December 2019), para. 79.

but will entitle the applicant to compensation for both pecuniary and non-pecuniary damages. An exception arises when the violation of Article 8 also constitutes a breach of Article 6 of the ECHR. In such cases, a retrial or reopening of the case may be required.

4.2 *Right to Fair Trial*

Unlike a violation of the right to privacy, a breach of Article 6 of the ECHR in criminal cases could have more serious consequences for domestic criminal proceedings. When an individual has been convicted in proceedings that violated the requirements of Article 6, the ECtHR may indicate that a retrial or reopening of the case, if requested, is generally an appropriate remedy and often the most suitable one.[53] In assessing the overall fairness of the proceedings, it is crucial to examine the rights of the defence, particularly whether the applicant was given the opportunity to challenge the authenticity of the evidence and to oppose its use.

France obtained the EncroChat data by invoking Article 706-102-1 of the French CPC, which regulates capturing computer data through the installation of technical devices. However, from a technical standpoint, the exact method of obtaining this data remains unknown due to the 'defence secrets' classification imposed by French authorities. Keeping the operation secret raises concerns about the right to a fair trial under Article 6 of the ECHR, as the defence must understand how evidence was obtained in order to challenge its authenticity and reliability during the trial.

Oerlemans and van Toor reasonably argued that information about how evidence was collected should be available to the defence, as this enables them to challenge the legality of the operation and possible abuse of power by law enforcement authorities.[54] Sommers explains that if hacked material is used as evidence, they must be open to scrutiny in court and subject to the same scientific and technical standards as any other form of non-testimonial evidence.[55] The Italian Supreme Court also emphasized that it is essential for the defence to know the methods and procedures used by investigators, and that prosecutors and police should disclose how intercepted messages from the Sky ECC cryptophone network were obtained.[56]

53 Verein gegen Tierfabriken Schweiz (VgT) v. Switzerland, App. 32772/02 (ECtHR 30 June 2009), par. 89, Moreira Ferreira v. Portugal, App. 19867/12 (ECtHR 11 July 2017), paras. 49 and 52.

54 J.J. Oerlemans, D.A.G. van Toor, *op.cit.,* p. 315.

55 P. Sommer, *op.cit.*, p. 1.

56 Italian Supreme Court (Cass., quarta sezione, n. 32915) of 15 July 2022.

On the other hand, the non-disclosure of technical methods used for evidence gathering is also reasonable in certain cases, as full transparency could enable criminals to evade such methods in the future. The ECtHR stands at the same position, acknowledging that in criminal proceedings there may be competing interests against disclosure. In some cases, it may be necessary to withhold certain evidence from the defence to protect the fundamental rights of others or to safeguard important public interest, such as national security, the protection of witnesses at risk of reprisals, or the need to keep police investigation methods confidential.[57] When assessing the overall fairness of the proceedings, consideration may be given to the balance between the public interest in investigating and punishing the offence and the individual's right to ensure that evidence is gathered lawfully.[58]

When the Berlin court referred the matter to the CJEU, it emphasized that due to the confidentiality of the technology underpinning the interception measure, the integrity of the data could not be verified. Consequently, the accused might not be able to comment effectively on that data in subsequent criminal proceedings. The CJEU did not examine the technical aspects of how the EncroChat material was obtained in France. Instead, it relied on the principle of mutual trust among EU Member States, assuming the lawfulness of France's actions.[59]

Similarly, Dutch and Belgian courts also have refrained from questioning the legitimacy of the evidence gathered by France, adhering to the principle of mutual trust. They argued that decisions made by French authorities must be respected, and national courts should not scrutinize the methods France used to obtain the EncroChat data.[60] The Hamburg Regional Court also noted that the German authorities cannot question the legality of evidence obtained in

57 Rowe and Davis v. The United Kingdom, App. 28901/95 (ECtHR, 16 February 2000), para. 61, Jasper v. The United Kingdom, App. No. 27052/95 (ECtHR, 16 February 2000), para. 52.

58 Hambardzumyan v. Armenia, App. 43478/11 (ECtHR 5 December 2019), paras. 75–76.

59 It is stressed that in accordance with the EIO Directive, the EIO issuing authority (Germany in concrete case) is not authorised to review the lawfulness of the separate procedure by which the executing Member State (France) gathered the evidence sought to be transmitted, bearing in mind that "any other interpretation of Article 6(1) of the Directive would result, in practice, in a more complicated and less effective system, which would undermine the objective of that directive." CJEU, EncroChat decision, para. 100.

60 Courts practice in Netherland is explained in: J.J. Oerlemans, D.A.G. van Toor, "Legal Aspects of the EncroChat Operations: A Human Rights Perspective", *European Journal of Crime, Criminal Law and Criminal justice* 30 (2022), pp. 309–328, and courts practice in Belgium in: J.J. Oerlemans, S. Royer, "The future of data-driven investigation in the light of the SKY ECC operation", *New Journal of European Criminal Law* 2023, Vol. 14(4) (2023), pp. 434–458.

another EU Member State, since it would undermine the principle of mutual trust.[61]

The CJEU focused solely on interpreting the EIO Directive and did not address whether the secrecy surrounding the acquisition of EncroChat data affects the rights of the defence. It stated that "the integrity of evidence transmitted can, in principle, be assessed only when the competent authorities actually have the evidence in question at their disposal and not at the earlier stage of the issuing of the EIO"[62] Thus, the CJEU effectively deferred to national courts the responsibility of determining whether the secrecy of the methods used to obtain the data affects the fairness of the proceedings. National courts are tasked with ensuring that the rights of the defence are respected and are required to disregard information and the evidence if the defence cannot effectively comment on them, and if such evidence is likely to have a preponderant influence on the findings of fact.[63]

Therefore, the CJEU provided guidelines with two key conditions that must be met in any criminal proceeding where EncroChat (and Sky ECC) material is used:

1. The defence must be given an opportunity to comment effectively on every piece of evidence including EncroChat (and Sky ECC) material.
2. EncroChat (and Sky ECC) material must not have a preponderant influence on the finding of facts.

What does it mean for the defence to comment effectively on each piece of evidence? In Serbia, Sky ECC data is presented in Excel tables, classified by courts as documents obtained through international legal assistance. While the defence can formally comment on this data, their ability to do so effectively is limited, given that data in Excel tables can be easily manipulated, and the method of collecting this data remains unknown. For the defence's commentary to be meaningful, they must understand how the evidence was obtained in order to challenge its legality and address potential abuses by law enforcement authorities.[64]

Because of that, some national courts have provided explanations regarding how EncroChat evidence was gathered, despite it being classified as a defence secret in the country of origin. For example, the Court of Midden-Nederland

61 Higher Regional Court Hamburg, *op. cit.,* paras. 77–88.
62 CJEU EncroChat decision, para. 90.
63 CJEU EncroChat decision, para. 131.
64 J.J. Oerlemans, D.A.G. van Toor, *op. cit.,* p. 315.

revealed that a 'hacking tool' was uploaded as an update from a French server to connected EncroChat phones.[65] Similarly, the UK's Royal Court of Justice explained, following expert analysis, that the French Gendarmerie introduced a virus ("implant") into EncroChat devices via a fake software update message. Once users initiated the update, the virus was installed, allowing the transfer of data to the police.[66] Such explanations do not disclose the technical details of how the data was collected but clarify the process, providing essential information for the defence in criminal proceedings.

The second condition implies that such evidence must not have a preponderant influence on the findings of facts. Since judges rely on their free judicial conviction and evaluate all evidence presented, it can be challenging to assess whether a single piece of evidence had a decisive impact. Typically, evidence is corroborated by other materials, and decrypted messages are seldom the sole basis for convictions.[67] Additional investigative methods, such as data production orders directed at telecommunication providers to gather subscriber and location data, seizing a suspect's cryptophone, correlating suspect nicknames from other sources of evidence with Sky ECC messages, and obtaining testimonials or even confessions, are also commonly employed.[68] Multiple sources of evidence can validate each other and strengthen the case,[69] meaning that every piece of evidence is supported by others.

However, a problem may arise when EncroChat or Sky ECC messages are the only evidence available. In such cases, this material should be excluded, as it undoubtedly has a preponderant influence on the findings of fact, given that no other supporting evidence exists. This should not be seen as pardoning criminals, but rather as a sign that the investigative authorities did not do their job thoroughly if, despite having valuable EncroChat or Sky ECC data, they failed to gather supporting evidence.

5 The Legal Effects of the CJEU EncroChat Decision

The CJEU EncroChat Decision raised numerous dilemmas in both legal theory and practice regarding its scope, implementation, and effects. Considering

65 J.J. Oerlemans, D.A.G. van Toor, *op. cit*, p. 314.

66 Royal Courts of Justice Strand, London, WC2A 2LL, R v A and others [2021] EW CA Crim 128, 05.02.2021., par. 149., https://www.judiciary.uk/wp-content/uploads/2021/02/A-v-R.pdf.

67 J.J. Oerlemans, S. Royer, *op. cit.,* p. 453.

68 Court of Amsterdam 24 November 2022, ECLI:NL:RBAMS:2022:7082 and Court of Gelderland, 11 April 2023, ECLI:NL:RBGEL:2023:2011., See. J.J. Oerlemans, S. Royer, *op. cit.,* fn. 20.

69 J.J. Oerlemans, D.A.G. van Toor, *op. cit.,* p. 328.

that the request for a preliminary ruling was submitted by the Regional Court in Berlin, a thesis has emerged in Serbian legal circles that the rules outlined in the CJEU EncroChat decision apply only to Germany, and potentially to other EU Member States, but not to EU candidate countries, which are outside the EIO system. Such an argument is untenable, and it is important to clarify why the rules set forth in the CJEU EncroChat decision have an *erga omnes* effect for national authorities of Member States, should be respected by candidate countries, and could serve as valuable guidelines for all other countries that aspire to uphold democratic principles and adhere to the rule of law.

Firstly, it is important to recall a long-standing debate on the effects of the preliminary rulings issued by the CJEU for national authorities of Member States. The preliminary ruling procedure is often described as the most important mechanism that enables constitutionalizing of the EU legal system and development of EU law principles.[70] A national court of the Member State is entitled to requesting a preliminary ruling when it faces a dilemma regarding the interpretation or validity of EU law. The CJEU decisions are final and include the interpretation of the harmonization of national law with EU acquis, which national courts are obligated to apply within their national legal systems.[71] It seems undisputed in the legal doctrine that *erga omnes* means that the ruling binds not only the referring court but all the authorities of all the Member States, including domestic judges.[72]

Secondly, it is essential to examine the effects of CJEU preliminary rulings on EU candidate countries. These countries must align their legislation with the EU acquis, which includes not only treaties and directives but also CJEU case law. Harmonization with EU law is impossible without adhering to CJEU rulings, as they shape judicial standards and clarify the rule of law as a common value. Since 1993, the rule of law has been a key element of the Copenhagen criteria for EU membership,[73] and under the 2020 enlargement methodology,

70 Donnelly, Tom de la Mare and Catherine, 'Preliminary Rulings and EU Legal Integration: Evolution and Continuity', in Paul Craig, and Gráinne de Búrca (eds), *The Evolution of EU Law*, 3rd edn (Oxford, 2021; online edn, Oxford Academic, 21 Oct. 2021), pp. 363–393, https://doi.org/10.1093/oso/9780192846556.003.0008.

71 Harlow, C., 'Three phases in the evolution of EU administrative law', in: Paul Craig, and Gráinne de Búrca (eds), *The Evolution of EU Law*, 3rd edn. (Oxford, 2021), p. 455.

72 F. G. Nicola, C. Fasone, D. Gallo, Comparing the Procedures and Practice of Judicial Dialogue in the US and the EU: Effects of US Unconstitutionality and EU's Preliminary Interpretative Rulings, *European Journal of Legal Studies* CJEU Special Issue, No. 3 (2023), p. 164.

73 A. Knežević Bojović, V. Ćorić, 'Challenges of Rule of Law Conditionality in EU Accession', vol. 7, no.1, *Bratislava Law Review* (2023) https://doi.org/10.46282/blr.2023.7.1.327.

it plays an even more central role in accession negotiations.[74] Article 49 TEU requires candidate countries to respect and promote EU values, making it necessary for them to not only align their laws but also adhere to the rule of law as interpreted by CJEU decisions.

On the other hand, candidate countries remain outside the EIO system, meaning they are not bound by the provisions of EIO Directive, which could support the argument that the decision interpreting this Directive does not apply to them. However, this only means that EncroChat and Sky ECC data cannot be transmitted to them through the EIO and must instead be shared via traditional instruments of international legal assistance. The CJEU EncroChat decision, through its interpretation of the EIO Directive, upholds the principles of the rule of law and legal certainty, establishing specific requirements for accepting EncroChat material as evidence, and as such, it should also be respected by candidate countries.

The EIO was created as a judicial cooperation instrument based on the principle of mutual recognition within the EU, designed to simplify the classical framework of international legal aid. It was intended to strengthen mutual trust and facilitate the free flow of evidence.[75] However, candidate countries remain outside this framework, meaning they must still use more demanding traditional legal assistance mechanisms, with foreign judicial decisions subject to specific recognition procedures.

Despite this, Serbian courts have unconditionally accepted Sky ECC material as evidence, even though Serbian authorities were not notified about surveillance of their citizens and such interception could not have been authorized under Serbian law. Furthermore, hacking and infiltration of computer viruses is a criminal offense under article 300 of the Serbian Criminal Code. In the absence of an investigative measure comparable to capturing of computer data through the installation of technical devices, courts in Serbia treated Sky ECC data as written documents obtained through international legal assistance.[76] The basis for this was found in Serbian Criminal Code and

74 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Enhancing the accession process—A credible EU perspective for the Western Balkans, Brussels, 5.2.2020, COM (2020) 57 final, https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/enlargement-methodology_en.pdf.

75 Katja Šugman Stubbs, 'Assessment of evidence obtained abroad: theoretical problems and Slovenian court practice' in Z. Đurđević, E. Ivičević Karas (eds.), *European Criminal Procedure Law in Service of Protection of European Union Financial Interests: State of Play and Challenges*, (Zagreb: Croatian Association of European Criminal Law, 2016), p. 33.

76 Higher Court in Belgrade, K-P01 125/2023.

Code of Criminal Procedure which still equate computer data with documents, despite common sense and jurisprudence in other countries confirming that unmaterialized computer data, by its structure and form, cannot be regarded as traditional legal documents.

Defence lawyers' requests to determine how this data was obtained in France were rejected and the courts relied on the assumption that the evidence was obtained lawfully, referring to the "general principle of mutual trust in the legal system of another state, as a generally accepted rule of international law."[77] Nevertheless, the problem is that the principle of mutual trust is neither a general principle of international law nor enshrined in any provision of Serbian law. Instead, this is a cornerstone of EU criminal justice and applies only within the EU. While courts in the Netherlands,[78] Belgium, or Germany can invoke mutual trust, courts in Serbia or other candidate countries still do not have a legal basis to do so, until they become full EU members.

Finally, it is paradoxical that courts in candidate countries invoke mutual trust to unconditionally accept EncroChat or Sky ECC evidence while simultaneously claiming that the principles established by the CJEU EncroChat decision bind only EU Member States. It would be extremely illogical for the CJEU to impose these requirements solely on EU Member States and not on candidate countries, as this would imply that the EIO system is more stringent than the traditional system of international legal aid. Given that the principles outlined in the CJEU EncroChat decision uphold the rule of law (legal certainty), fair trial, and national sovereignty, they should serve as benchmarks not only for EU candidate countries but for all countries committed to democratic values and safeguarding their sovereignty, especially in today's era of mass surveillance.

Conclusion

The interception of encrypted communication platforms (EncroChat and Sky ECC) is undoubtedly a significant and ingenious achievement by the

77 Higher Court in Belgrade, 10 Kž2-Po124/23, Court of Appeals in Belgrade, Kž2-Po1 214/23.

78 In the Netherlands, Dutch defence lawyers debated a theory that the evidence was illegally obtained under Dutch law and should therefore be excluded, but Dutch courts disagreed. As a principle of mutual trust, the Dutch judiciary does not investigate the legitimacy of the evidence that has been gathered by foreign law enforcement authorities on foreign territory any further, unless it interferes with the right to a fair trial. See: J.J. Oerlemans, D.A.G. van Toor, *op.cit.*, p. 319.

investigative teams of France, the Netherlands and Belgium, as it was necessary to outsmart criminal groups that use all technological advantages in the same way. However, from a legal perspective, the unconditional use of this evidence opens a Pandora's box of procedural irregularities, potentially legitimizes mass surveillance, and challenging traditional democratic values and fair trial guarantees.

While awaiting the ECtHR decision, the CJEU's preliminary ruling remains the first and the only decision of one supranational judicial body addressing EncroChat data. Although the CJEU EncroChat decision formally analyses the EIO Directive, the rules set forth by it fundamentally serve to protect the rule of law, fair trial guarantees, and national sovereignty. Therefore, the principles set forth by this decision should be respected not only by EU Member States and EU candidate countries but could also serve as valuable guidelines for courts in all other states committed to protecting these values. Thus, the stance taken by courts in some EU candidate countries- unconditionally accepting Sky ECC evidence by invoking the principle of mutual trust while refusing to apply the rules from the CJEU EncroChat decision on the grounds that such decisions do not bind non-EU Member States- is even more unfounded. This creates a paradoxical situation where EU Member States, within the EIO system, impose certain conditions on the use of evidence coming from other EU Member States, while EU candidate countries, out of the EIO framework, apply no additional restrictions!

The requirement that the investigative measure(s) indicated in the EIO could have been ordered under the same conditions in a similar domestic case, serves to uphold the rule of law, particularly the principle of legal certainty. Any restriction of fundamental rights must be explicitly prescribed by law, and investigative measures, by their nature, restrict these rights. When a country's legislation does not provide for methods such as online surveillance, computer system intrusion, or similar techniques, its authorities cannot bypass domestic legal standards by accepting evidence obtained through such means from another country. This is because those investigative measures are not accessible or foreseeable in their effect for domestic citizens. Adopting the opposite approach would set a dangerous precedent, allowing domestic evidentiary rules and prohibitions to be circumvent by importing evidence from foreign jurisdictions, thereby undermining the rule of law. Therefore, the EncroChat (and Sky ECC) cases emphasize the need for all countries to regulate investigative measures analogous to hacking, such as system intrusion and other methods for accessing and decoding encrypted communications, given that traditional investigative methods are inadequate for addressing emerging forms of criminality.

The EncroChat and Sky ECC cases raise important questions about the legitimacy of using bulk interception to gather criminal evidence, as opposed to its use for intelligence gathering for national security purposes—an issue previously addressed by the ECtHR. Labelling the acquisition of EncroChat data as a "defence secret" raises suspicions about the legal nature of EncroChat data. If treated as evidence, the question arises whether such data could be lawfully collected through bulk interception of communications outside of French territorial jurisdiction. Conversely, if treated as intelligence, the issue is whether it can be legitimately used as evidence in criminal proceedings. While awaiting further clarification from the ECtHR, the CJEU emphasized, referring to Article 31 of the EIO Directive, that an intercepting EU Member State is obliged to notify the Member States where the subject of interception is located. This provision is intended to protect both national sovereignty and individual rights. Given the controversy surrounding the notification requirement in today's era of digital communications and mass surveillance, it would be advisable for all countries to establish specialized bodies, akin to the Investigatory Powers Tribunal in the United Kingdom. These bodies would be empowered to assess, through an adversarial process, the claims of individuals who suspect their communications have been intercepted, thus ensuring that proper remedies are available.

Bulk interception of communication inevitably affects the right to privacy, but according to the ECtHR, evidence obtained through a violation of this right alone, may not significantly impact criminal proceedings before national courts. As a result, these operations are often trivialized, with arguments that it is absurd to invoke privacy concerns when dealing with serious criminal offences such as brutal murders or drug trafficking. However, if such reasoning prevailed, landmark decisions like the famous *Miranda* ruling would never have been made—following the logic of, "what does it matter that the perpetrator wasn't informed of their rights if they already confessed to the crime?" The aim, therefore, is not to shield criminals by appealing to "privacy" but to set clear limits on the extent to which states can intrude upon individual rights.

Finally, the CJEU did not delve into the technical aspects of how the EncroChat material was gathered in France, assuming the lawfulness of France's actions in accordance with the principle of mutual trust. In any case, secrecy surrounding the methods of obtaining the data can undermine the defence's ability to challenge the evidence's authenticity and legality. The CJEU established two key conditions for using EncroChat evidence: the defence must be able to comment effectively on the evidence, and the evidence must not have a preponderant influence on the findings of fact. When these conditions are not met, the material should be excluded to ensure the fairness of the proceedings.

Ultimately, even if all EncroChat users were criminals (a claim that is unprovable), they are still entitled to the guarantees of a fair trial, including the right to know how the evidence against them was obtained so that they can challenge it in court. Ignoring procedural safeguards in these cases creates a dangerous precedent and threatens to undermine these protections in future cases, where innocent people or political opponents of certain regimes may be on the defendant's bench. Thus, while unconditionally accepting EncroChat and Sky ECC evidence may seem like a straightforward solution for convicting "criminals", the guarantees of a fair trial- as a cornerstone of democracy and a safeguard against abuse by governments and state authorities- must not be compromised for the sake of quick and easy convictions.