COMPARATIVE EXPERIENCES AND
RECOMMENDATIONS FOR MONTENEGRO

CeMI
CENTRE FOR MONITORING AND RESEARCH

ADMISSIBILITY OF THE USE OF ENCRYPTED COMMUNICATIONS AS EVIDENCE IN CRIMINAL PROCEEDINGS

ADMISSIBILITY OF THE USE OF ENCRYPTED COMMUNICATIONS AS EVIDENCE IN CRIMINAL PROCEEDINGS

COMPARATIVE EXPERIENCES AND RECOMMENDATIONS FOR MONTENEGRO

Publisher:
Center for Monitoring and Research (CeMI)
Bul. Svetog Petra Cetinjskog 96, VI/12
E-mail: info@cemi.org.me
www.cemi.org.me

Editor:
Zlatko Vujovic

Author:
Vladimir Simonovic

Print:
SmartPrint

Circulation:
100

Year of Issue:
2023

INTRODUCTION

As technology advances, so does the way the judiciary deals with evidence in criminal proceedings. Electronic evidence, which includes data stored or transmitted in digital form, has become a crucial part of many criminal investigations. Messages from mobile phones, emails, digital records, and similar are now routinely used as evidence in courtrooms. However, while electronic evidence provides new opportunities for conducting investigations and prosecuting crimes, it also poses a set of new challenges, including issues related to privacy, data security, and the legality of collecting and using such evidence. The use of evidence collected through intrusions into encrypted applications, such as EncroChat, Sky ECC, Anom, and others, serves as examples illustrating these complex problems.

In this Policy Brief, our main focus will be on cases related to EncroChat, considering that some of the most prominent legal proceedings in European countries have taken place precisely in the context of using this application. Despite public statements suggesting differences between these two platforms, they are not significant for the admissibility of data from the Sky ECC application as evidence in legal proceedings. However, given that individuals facing criminal proceedings in Montenegro used the Sky ECC platform, we cannot neglect its importance.

After a retrospective summarizing these platforms and describing how the discovery unfolded, resulting in actions against organized criminal groups across Europe, the key topic addressed in this Policy Brief pertains to the legality of using evidence obtained through "hacking" into secure communication platforms in court. This is particularly relevant in the broader context of the right to privacy in the digital age and the right to a fair trial. It is essential to clarify whether, when, and how these electronic pieces of evidence can be used in criminal proceedings, following rules on evidence and fair trial requirements. To achieve this, the document provides a comparative analysis of various European countries that have dealt with this issue, hoping that their experience will facilitate a better understanding of different jurisdictions' approaches and identify possible models for implementation in other countries, including Montenegro. The Policy Brief offers insights into the legal perspectives and court decisions in France, Germany, Norway, the Netherlands and Italy, regarding the legality of using encripted communication as evidence in court and potential repercussions in the context of human rights protection. These countries were selected due to

their relevance and significant legal proceedings that occurred in the context of using such evidence.

In conclusion, based on our research, the Policy Brief includes conclusions and recommendations for further steps, emphasizing the need to find a balance between the necessity for the effective administration of justice and the protection of fundamental human rights.

I. ENCROCHAT AND SKY ECC: RETROSPECTIVE

EncroChat and Sky ECC are encrypted communication platforms designed to protect user messages from unauthorized access through advanced encryption algorithms. Encrypted communication refers to the process of encoding information or messages so that only authorized parties can understand them. The basic idea is to transform information from its original, readable format into certain unreadable forms, using algorithms and keys for encryption and decryption. This method is often used to protect sensitive data from unauthorized access and reduce the risk of message interception by third parties.

1.1. EncroChat

EncroChat is a platform that utilizes Android devices with two operating systems: one standard Android and the other an EncroChat system for encrypted messages, voice calls, and financial transactions. On the company's website, which is still functional at this time, there is a list of services and functionalities that EncroChat provides to its users.[1]

France initiated an investigation into EncroChat in 2017 after law enforcement officers repeatedly found phones with this application in operations against organized criminal groups. Thanks to technical analysis, French authorities managed to breach the encryption and access user communication. As EncroChat was widely used among criminal networks, in 2019, French authorities opened the case to Eurojust. The investigation allowed the processing of collected data under French legislation and with judicial authorization, within the framework of international judicial and police cooperation.[2]

1 https://encrophone.com/en/
2 Europol/Eurojust (2020), "Dismantling of an encrypted network sends shockwaves through organized crime

This was possible thanks to Article 706-102-1 of the French Code of Criminal Procedure[3], which allows the installation of technical devices for accessing, recording, storing, and transmitting computer data without the consent of the parties concerned, for the purpose of more effectively conducting investigations in criminal cases involving organized crime.

The interception of messages through EncroChat concluded on June 13, 2020, when the company warned users that authorities had infiltrated the platform and advised them to immediately discard their devices.[4] The initiation of the investigation was not only prompted by finding encrypted devices with criminals during police operations but also by the way the devices were advertised to users. This included the option of a so-called panic mode for deleting all data in case of being compromised, the inability to identify the company's owner, the high price of the devices, and the option to purchase them with cryptocurrencies, indicating to authorities that these devices were used to conceal criminal activities. Following the breach of EncroChat's encryption, actions were taken against organized criminal groups in several European countries. In some of these cases, we already have initial court rulings where EncroChat communication was used as evidence in court. It is noteworthy that between 90 and 100% of EncroChat application users were reportedly linked to organized criminal groups.[5]

1.2. Sky ECC

Similarly to EncroChat, Sky ECC uses its own encrypted platform for sending secure messages, emails, and files, with additional security features. Both systems provide a high level of privacy and security. However, the use of devices with this type of protection is associated with criminal activities.
SKY ECC provided some additional functionalities and layers of protection that were not available on the EncroChat platform. For example, SKY ECC used two-key encryption, while EncroChat used a single key. Two-key encryption typically refers to asymmetric encryption, where a key pair is used: a public key for encrypting data and a private key for decrypting. In this context,

groups across Europe", Europol, July 2, 2020 https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe
3 Possible situations may arise where the use of technical means is resorted to, aiming to have access, record, store, and transmit computer data anywhere without the consent of the person whose data is used. The State Prosecutor or the investigating judge can appoint any authorized natural or legal person registered on one of the lists provided for performing technical operations that enable the realization of the technical device mentioned in the first paragraph of this article. The State Prosecutor or the investigating judge can also prescribe the use of state means subject to national defense secrecy in forms provided for in Chapter I of Title IV of the Criminal Procedure Code.
4 Europol/Eurojust, op.cit.
5 https://www.france24.com/en/20200702-european-police-shut-criminal-phone-network-used-to-plan-murders

asymmetric encryption provides a higher level of security because even if someone manages to intercept the public key, they won't be able to decrypt the message without the corresponding private key. On the other hand, single-key encryption usually refers to symmetric encryption. In symmetric encryption, the same key is used for both encrypting and decrypting a message. While secure, this poses a problem if the key is compromised because then an attacker could decrypt all messages encrypted with that key. Additionally, Sky ECC offered various mechanisms to protect against abuse, such as panic buttons that allow users to quickly and discreetly erase all sensitive information. The higher level of privacy protection also meant a higher device cost, with a six-month subscription to the Sky ECC platform ranging between 950-2,600 EUR, while the EncroChat platform subscription cost between 1,000-1,500 EUR.

According to Eurojust, Sky Global, known as the Sky ECC platform, attracted a significant number of users from organized criminal groups after the fall of EncroChat.[6] In March 2021, Belgium, France, and the Netherlands launched an operation against Sky ECC following an investigation into criminal networks using this platform. Belgian police claims suggest that Sky ECC was used to coordinate illegal activities, including drug and weapon trafficking.[7] VAuthorities successfully breached Sky ECC encryption, leading to numerous arrests and asset seizures in Europe. Sky Global's CEO, Jean-Francois Eap, and former Sky Global device distributor, Thomas Herdman, are indicted in the U.S. for participating in criminal activities enabling the import and distribution of narcotics through the sale of encrypted devices.[8] The indictment alleges that Sky Global devices were designed to thwart the monitoring of criminal organizations' communications, and the company profited significantly by facilitating their criminal activities and shielding them from law enforcement, using digital currencies to facilitate illegal transactions.[9]

6 https://www.europol.europa.eu/media-press/newsroom/news/new-major-interventions-to-block-encrypted-communications-of-criminal-networks
7 Ibidem
8 Meghan E. Heesch and Joshua C. Mellor (2021), 'Sky Global Executive and Associate Indicted for Providing Encrypted Communication Devices to Help International Drug Traffickers Avoid Law Enforcement,' Office of the U.S. Attorney, Southern District of California, March 12, 2021. https://www.justice.gov/usao-sdca/pr/sky-global-executive-and-associate-indicted-providing-encrypted-communication-devices
9 Ibidem

II. COMPARATIVE ANALYSIS: LEGAL RESPONSES TO ENCRYPTED COMMUNICATION IN EUROPE

International investigations conducted by the French police, concerning the EncroChat and Sky ECC platforms, consistently raise dilemmas about the application of foreign investigative methods in national judicial processes. On one hand, questions arise about the solidity of the investigation results and their susceptibility to review by defense lawyers and the adjudicating court. On the other hand, their legality is scrutinized in terms of compliance with fundamental principles of fair trial.

Within numerous European jurisdictions, we are already witnessing the first convictions based on evidence collected through the surveillance of devices using the previously described secure communication applications. However, there have also been contradictory decisions where courts took the position that the content of communications collected through encrypted communication surveillance cannot be used as evidence in a legal proceeding. In this chapter, we will analyze how different European states have approached the legality of using evidence obtained by states conducting surveillance on the platforms we discussed in the previous chapter. Our focus will be on the arguments of opposing sides, legal dilemmas, and judgments arising in connection with this complex issue, highlighting the impact of diverse legal frameworks on the treatment of such evidence, as well as the practices of the European Court of Human Rights (ECHR) in the context of the right to a fair trial.

2.1. France

In the case conducted before French courts, where evidence was collected from the EncroChat platform, the defense expressed doubts about the authenticity and reliability of such evidence. These doubts arose from the lack of transparency regarding the methods through which French authorities accessed this information. The prosecution, on the other hand, refrained from providing details about the investigation, citing the protection of national security as the primary reason. After the Court of Appeal in Nancy ruled the use of EncroChat evidence lawful, the defense appealed to the Supreme Court.

In the Supreme Court's case, three central arguments related to the legality of collecting data from secure communication devices were considered.[10]

As the first argument, the defense highlighted that the data interception procedure is unlawful because it violates the right to privacy and that the modifications to the EncroChat network are inconsistent with the French Code of Criminal Procedure. The court rejected this point of appeal, considering the modifications necessary and lawful technical operations for data collection.[11]

In the second argument, the defense highlighted that the omission of documentation from the proceedings before the court in Lille, which was competent for the EncroChat investigation, violated the principle of judicial oversight of prosecution procedures. Additionally, they claimed a breach of Article 6 of the European Convention on Human Rights, which guarantees the right to a fair trial. The court dismissed this argument as well, stating that the relevant documentation from the proceedings in Lille was accessible to the accused and investigating judges, allowing for an assessment of the fairness of the collected evidence.[12]

The third argument pertained to the secrecy of the operation against EncroChat and the inability to establish the authenticity and reliability of the evidence. The defense argued that the secrecy of the investigation contradicted the right of the accused to equality of arms and an effective legal remedy. They also contended that the French Criminal Code required authorities to provide details about the data collection operation, including a certificate of authenticity confirming the accuracy and authenticity of the evidence used. The Supreme Court partially agreed with this argument, noting the absence of technical information about the data collection process and the lack of a certificate of data authenticity. As a result, the Supreme Court overturned the decision of the Court of Appeals in Nancy and referred the case for a retrial to the Court of Appeals in Metz.[13] OThis court determined that considering the messages collected by the French police were not encrypted, there was no need for a certificate confirming their authenticity. As expected, the defense appealed this decision by the Court of Appeals, but the Supreme Court rejected it, thereby ultimately confirming the legality of using the specific EncroChat evidence in this trial.[14]

---

10 Bill Goodwin (2022), French Supreme Court rejects EncroChat verdict after lawyers question secrecy over hacking operation, ComputerWeekly.com, 12. oktobar 2022. godine. https://www.computerweekly.com/news/252525971/French-Supreme-Court-rejects-EncroChat-evidence-after-lawyers-question-defence-secrecy

11 Ibid

12 Ibid

13 Ibid

14 Bill Goodwin (2023), French supreme court dismisses legal challenge to EncroChat cryptophone evidence, ComputerWeekly.com, 6. septembar 2023. godine. https://www.computerweekly.com/news/366551078/

The provisions of the French Code of Criminal Procedure that allowed law enforcement agencies to collect controversial evidence were also subject to the decision of the Constitutional Court. According to the Constitutional Court's opinion, elaborated in the decision of April 22, 2022,[15] the provisions of the French Code of Criminal Procedure regulating the acquisition and processing of data in investigations are in line with the Constitution of France. This is based on several reasons. Firstly, the provisions of the Code of Criminal Procedure provide complex mechanisms that allow state authorities to access encrypted or otherwise protected information, but under strict conditions and the supervision of the court. Secondly, there is a clear procedure for engaging experts to decrypt data, subject to oaths and ethical standards. Thirdly, specific protocols and deadlines have been introduced for the use of state resources that are part of national defense secrecy, with the possibility of actions being suspended by authorized authorities. The Constitutional Court concluded that these mechanisms enable effective investigations while simultaneously ensuring the protection of individuals' rights and preserving national interests, thus striking a balance between efficiency in criminal proceedings and civil liberties, and are therefore in accordance with the Constitution of France.

2.2. Germany

One of the significant cases where EncroChat communication was accepted as evidence comes from Germany.

Specifically, the Federal Court of Justice rejected the appeal against the judgment of the Regional Court in Hamburg from 2021, where the defendant was sentenced to five years in prison for drug trafficking. In this case, the accused challenged the legality of using EncroChat communication as evidence in the proceedings against him. This communication had been provided to the German Federal Criminal Police through Europol. The data indicated numerous serious crimes committed within the territory of Germany. In light of these findings, the Central Office for Combating Internet Crime at the General Public Prosecutor's Office in Frankfurt initiated investigations against several unknown individuals. During the investigative phase, a European Investigation Order (EIO) was sent to the French authorities, covering a request for the transfer of all EncroChat data related to Germany and permission for their use in German criminal proceedings. The French court approved both requests, allowing for further investigation.[16]

French-supreme-court-dismisses-legal-challenge-to-EncroChat-cryptophone-evidence

15 Decision of the Constitutional Court of France No. 2022-987 QPC, available at: https://www.conseil-constitutionnel.fr/decision/2022/2022987QPC.htm

16 Decision of the Federal Supreme Court of the Federal Republic of Germany No. 5 StR 457/21 dated March 1, 2022. Available at: https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2022&nr=127966&linked=bes&Blank=1&file=dokument.pdf

To determine whether it is possible to use this data as evidence in a court proceeding, the Federal Court had to answer three questions: 1) whether there has been a violation of procedural law, 2) whether this law, if violated, protects the rights of the suspect, and 3) whether the interest of the suspect outweighs the prosecutor's interest.

The court did not find a violation of procedural rights that would affect the legality of using this data as evidence in court. Firstly, it did not consider it necessary to assess the legality of how the French authorities obtained the data, as this would violate the principle of mutual trust governing cooperation between EU member states. The court also did not find a violation of the principle of proportionality, given the serious nature of the crime targeted by the communication interception measure. From the perspective of procedural assumptions and the application of Article 31 of the EIO Directive, the court found a violation in this part. It concluded that there was a violation because French authorities were obliged to inform German authorities that an investigation was ongoing against individuals on their territory.[17] However, this violation could not affect the (il)legality of using EncroChat communication in the judicial process, as the purpose of Article 31 EIO is not to protect the rights of the suspect but to safeguard the sovereignty of the state conducting the investigation.

The court particularly appreciated the admissibility of evidence from the perspective of Article 6 EIO, which requires that the order must be proportional and that one country cannot request from another what it could not do based on its own legislation. Regarding the first requirement, the court found nothing indicating disproportionality. As for the second requirement, it's worth noting that the German prosecution did not ask the French investigative authorities to carry out covert surveillance measures; they only requested the transmission of the investigation results. According to the Federal Court, there is no condition that French investigative measures must be allowed under German law for the transmitted data to be admissible in German courts.

However, there are dissenting opinions. The Regional Court in Berlin disagreed with the Federal Court's stance and submitted a request for an

17 Article 31 states: "Where several Member States are in a position to provide the necessary technical assistance, an EIO should be sent only to one of them and priority should be given to the Member State where the person concerned is located. Member States where the subject of the interception is located and from which no technical assistance is needed to carry out the interception should be notified thereof in accordance with this Directive. However, where the technical assistance may not be received from merely one Member State, an EIO may be transmitted to more than one executing State " https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0041&from=EN

interpretation of the relevant law to the European Court of Justice,[18] posing a series of questions. The most significant among them are the following three:

The first question pertains to the legality of the EIO issued by the German authorities, i.e., whether the order was correctly issued in the context of Article 6(1)(b) of the EIO Directive, which requires that an EIO can be issued only if the investigative measures specified in the order could have been imposed under the same conditions in a similar domestic case. The Regional Court in Berlin expressed doubts about whether an EIO could be used to transfer data if the surveillance methods used by France were impermissible under German law in a similar domestic case.

The second question concerns the legality of using evidence potentially obtained in violation of EU laws. The court raises the question of whether such evidence should be excluded from criminal proceedings in line with the principle of effectiveness and the principle of equivalence. The question is particularly directed at the fact **that the secrecy of French surveillance measures prevents independent verification of the accuracy and reliability of the data, which is central to an effective defense**.[19]

The Berlin court also inquired whether, in accordance with EU law, specifically the principle of effectiveness, it is permissible to use evidence collected unlawfully if the offense is serious, even if this seriousness was not known when the evidence was first obtained. The court emphasizes that, according to the basic principle of effectiveness, national laws should protect the rights of the accused so that they do not suffer unfair disadvantages during criminal proceedings due to illegally obtained evidence. It suggests that this protection can be achieved in two ways: either by excluding illegally obtained evidence from the proceedings or by taking into account, during the assessment of evidence, the fact that it was collected unlawfully. The court favors excluding the evidence.

According to the opinion of the Advocate General of the European Court of Justice, dated October 26, 2023,[20] the evidence was obtained in accordance with the law. However, the Advocate General did not express an opinion on whether the evidence is admissible in criminal proceedings in Germany or other EU member states. This is because EU law does not contain norms

18 Decision of the Regional Court in Berlin on Referral to the European Court of Justice, dated October 19, 2022 – (525 KLs) 279 Js 30/22 (8/22), para. 31. https://www.burhoff.de/asp_weitere_beschluesse/inhalte/7384.htm
19 Ibid, para. 71
20 Find more: https://curia.europa.eu/juris/document/document.jsf;jsessionid=4667734026567B77078D-65D21E14FC73?text=&docid=279144&pageIndex=0&doclang=en&mode=req&dir=&occ=-first&part=1&cid=3556492

regarding the admissibility of evidence,[21] rather, this is a matter for national legislation, as indicated by the practice of the European Court of Human Rights.[22] On the other hand, the opinion emphasizes that member states are **bound by the principle of mutual recognition**, which requires them to accept the legality of the French interception operation approved by French courts unless those measures would be illegal in French legal proceedings.[23]

2.3. Norway

In Norway, the Supreme Court ruled on the appeal of three individuals convicted of trading large quantities of narcotics as part of the activities of an organized criminal group.[24]

In March 2020, the Norwegian National Criminal Investigation Service (Kripos) was granted access to data from Norwegian users of EncroChat. Based on this data, several phone users were identified, and grounds for suspicion against multiple individuals were established. Subsequently, Kripos obtained permission from the Regional Court in Oslo to monitor communication, including that of the three defendants in the case that reached the Supreme Court of Norway. In June 2020, after the Oslo police received the data from Kripos, the prosecution obtained consent from French authorities to use this data as evidence in the criminal proceedings.

One of the key defense arguments was that the evidence should be excluded because the foreign authorities actually obtained it in Norway, not in France, and that they were obligated to act in accordance with Article 216 of the Norwegian Criminal Procedure Code. According to Article 216, when there is reasonable suspicion of an attempted or committed criminal offense, the police must obtain a court permit to access computer data that is not publicly available. However, the Supreme Court rejected such claims, affirming the judgments of the trial and appellate courts, and in its ruling, it referred to existing precedents.

The fundamental question in this case is identical to the one raised in Germany – whether data collected by foreign authorities can be used as evidence in a Norwegian criminal proceeding. Although Norwegian law does not regulate the use of such data, some precedents allow for the use of evidence legally

21 Ibid, para. 117
22 Ibid, para. 123
23 Ibid, para. 48
24 The decision of the Supreme Court of Norway on appeal No. HR-2022-1314-A, (case No. 22-027874STR-HRET), (case No. 22-027879STR-HRET), and (case No. 22-027883STR-HRET), is available at: https://www.domstol.no/globalassets/upload/hret/decisions-in-english-translation/hr-2022-1314-a.pdf

obtained in other countries, even if such access would not be legal in Norway.

This principle was first confirmed in the case of wiretapping a Norwegian citizen in Spain. The ruling states that if an individual chooses to live in a country with different communication control restrictions than those in Norway, that person cannot expect information obtained through legal communication control in that country to be unacceptable as evidence in Norway. If the information is acquired in line with Norwegian values and used as evidence for a criminal offense in the relevant country, it should be admissible as evidence in Norway, **provided that the accused has access to this information**.[25] In another case cited by the Supreme Court, it is noted that requiring foreign police and judicial institutions to apply Norwegian procedural laws in criminal cases would hinder international cooperation in the fight against transnational crime, which would not be acceptable.[26]

2.4. The Netherlands

The need for the accused to have access to the evidence used against them is a cornerstone of any defense. In Dutch proceedings related to EncroChat evidence, the defense argued that every piece of data collected through monitoring of the EncroChat platform should be made available to the defense.

Specifically, Article 6 of the European Convention on Human Rights (ECHR) requires the prosecution to provide the defense with access to all relevant evidence, ensuring the accused has adequate time and means to prepare their defense. However, the relevance of evidence can be questioned, and the accused must provide valid reasons for requesting access to the evidence. Although there is an obligation in a system where the prosecution considers facts for and against the suspect to ensure fairness, the prosecution's assessment of the relevance of evidence may be inconsistent with the requirements of Article 6(1) ECHR. Nevertheless, it is important to emphasize that the right to disclosure of relevant evidence is not absolute. In criminal proceedings, there are conflicting interests (such as national security or the protection of witnesses) that must be balanced with the rights of the accused.[27]

25 Ibidem
26 Ibidem
28 European Court of Human Rights, Guide on Article 6 of the European Convention on Human Rights - Right to a Fair Trial (Criminal Aspect), 2022, page 37/130 https://www.echr.coe.int/documents/guide_art_6_criminal_eng.pdf

In some situations, i**t is necessary to withhold certain evidence from the defense to preserve the fundamental rights of others or protect the public interest**. However, **such limitations on the right of defense are allowed only if absolutely necessary**, with the existence of appropriate measures to offset potential difficulties for the defense.[28]

In cases before Dutch courts, defense attorneys insisted on reviewing the evidence held by the prosecution to verify its integrity and reliability, as well as to search for potential evidence that could be in favor of their clients.[29] The defense was partially granted access to the requested data. According to the practice of Dutch courts, the defense had the right to access EncroChat data, but only to the extent that the data was relevant to the specific case, i.e., not including data from other criminal investigations. The defense could analyze this data at the Dutch Forensic Institute, using the same analytical software as the prosecution, and obtain a copy of the relevant EncroChat data. The Supreme Court of the Netherlands considers this approach lawful and in line with the principle of equality of arms.[30]

Despite defense arguments questioning the integrity and reliability of the evidence against their clients, the defense failed to challenge the reliability of EncroChat data, often coming from multiple sources. As a result, no data from the EncroChat operation proposed by the prosecution was excluded from Dutch criminal cases.[31] Similarly to Germany and Norway, the criminal court in the Netherlands believes it is not its role to verify the adequacy of the legal basis for investigative actions conducted by another state. The court emphasizes that its task is limited to ensuring that the use of results from a foreign investigation in a criminal proceeding does not violate the right to a fair trial.[32]

The use of EncroChat and Sky ECC evidence before Dutch courts has also been the subject of consideration by the Supreme Court of the Netherlands. At the request of two district courts, the Supreme Court was called upon to answer two preliminary questions. The first question concerned the principle of mutual trust between states in the context of joint investigations, particularly whether data collected by the French police using unknown techniques

29 J.J. Oerlmans i D.A.G. van Toor (2022), Pravni aspekti EncroChat operacije: perspektiva ljudskih prava, Evropski časopis za kriminal, krivično pravo i krivičnu pravdu, 30 (2022), 309–328. https://brill.com/view/journals/eccl/30/3-4/article-p309_006.xml?language=en

30 Ibid

31 Ibid

32 The decision of the District Court in Rotterdam dated June 25, 2021, paragraph 3.2.4. https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:RBROT:2021:6113

could be used as evidence in Dutch courts. The second question related to the relevance of EU Directives 2002/58/EC and 2016/680, addressing the processing of personal data and privacy.

The Supreme Court of the Netherlands, in its decision[33] concluded that Directive 2002/58/EC could not be applied because data from communication protection applications were not retained by service providers, as the directive required. The relevance of Directive 2016/680 was dismissed as irrelevant to resolving the preliminary questions.

With its decision, the Supreme Court limited the ability of Dutch courts to oversee the legality of foreign investigations, starting from the assumption that such investigations were conducted legitimately unless proven otherwise by a decision in a foreign country. Essentially, the Court's stance meant that investigations conducted by cooperating states, as long as they did not violate rights guaranteed by the ECHR, would be considered lawful and acceptable. The Court also emphasized that the right to challenge evidence is not absolute and can be balanced against conflicting interests, such as national security. It also limited the role of the national court in further examining evidence collection methods when those methods are protected as state secrets by another country.

2.5. Italy

Italy represents an exception to the previously mentioned countries where the use of evidence obtained by infiltrating secure communication applications has been accepted. In the case of Italy, it specifically involved communication obtained through the infiltration of the Sky ECC application. The case concerned the legality of detaining an individual accused of drug trafficking. In its decision dated July 15, 2022,[34] the Supreme Court of Italy emphasized that the accused cannot fully understand the investigation or the nature of the evidence against them without access to such materials. The court highlighted that details on how the evidence was collected, including the "capture and decryption of telematic flows" from Sky ECC, must be disclosed to the defense to ensure a fair trial, which was lacking in this case and was necessary for assessing the relevance, reliability, and value of the evidence.

As emphasized in the decision, at the core of criminal proceedings is the imperative that evidence must comply with the fundamental principles of

33 The decision of the Supreme Court of the Netherlands, dated June 13, 2023 https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:HR:2023:913

34 Cass, 32915/22, https://canestrinilex.com/en/readings/due-process-requires-transparency-of-evidence-gathering-in-sky-ecc-proceeding-cass-3291522

the Italian legal system, particularly the right to defense. Therefore, a careful assessment of how the evidence was collected is of utmost importance to ensure that the right to defense is not compromised. The ruling underscores that both parties must have the opportunity to comment not only on the collected evidence but also on the methods of collection. This assessment is crucial, even in situations where detention decisions are made, as was the case here. If the evidence influences the judge's decision on detention, the methods of collecting that evidence must be carefully considered. Specific focus is placed on evidence obtained from digital communications, such as electronic messages. In this regard, it is essential to verify whether the content of messages accurately corresponds to the originally sent and received messages and whether user accounts match the real senders and recipients of messages.

At first glance, the decision of the Supreme Court of Italy appears to be a significant deviation from the practices of courts in other EU member states. In all the previously mentioned countries, the courts respected the principle of mutual trust and did not question the legality of procedures carried out in other member states. However, the key distinction in the Italian case lies in the nature of the presented information. Unlike other EU countries where evidence is obtained directly from judicial authorities through mechanisms of international judicial cooperation, in Italy, the information was obtained from Europol as part of international police collaboration.

III. ADMISSIBILITY AND IMPACT OF ENCRYPTED COMMUNICATION AS EVIDENCE IN MONTENEGRIN JUDICIARY

For over a year, the Montenegrin public has had the opportunity, through the media, to become acquainted with (allegedly) part of the content of Sky ECC communications involving individuals who are suspects, some of whom were later charged with serious crimes related to organized crime. Lawyers argue that the data received by the Special State Prosecutor's Office (SDT) through Europol represent purely operational information that cannot be used as evidence in court. Some lawyers emphasize that this data was obtained through criminal activity, as investigative authorities of other countries allegedly gained access to the data through "hacking" and introducing a "virus," even though some countries, like France, which participated in this operation, allow such investigative actions.

Despite the defenders' stance, the Higher Court in Podgorica has confirmed several indictments in which the Special State Prosecutor's Office (SDT) presented communication via the Sky ECC application as evidence,[35] In one of the indictments filed by the SDT on December 30, 2022, the legal basis for the use of this evidence can be seen. According to the indictment, the evidence was collected in accordance with the Law on International Legal Assistance in Criminal Matters, and the collection methods did not necessarily have to comply with the Criminal Code of Montenegro, provided they were not contrary to domestic legal principles and international law.

Namely, according to Article 45 of the Law on International Legal Assistance in Criminal Matters of Montenegro, a procedural action undertaken by the foreign judicial authority in accordance with its law shall be deemed equal to the relevant procedural action undertaken by a domestic judicial authority within the criminal proceedings, unless this is contrary to the principles of the domestic judicial system and generally accepted principles of the international law. Although not specified in the indictment, it should be noted that other international instruments of cooperation allow the exchange of data between investigative authorities. Specifically, one state's prosecutor's office can share data with other states through international judicial cooperation without the need for a prior formal request. This possibility is stipulated by Article 11 of the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters[36] and Article 26 of the Budapest Convention on Cybercrime.[37]

In the aforementioned indictment, it is further emphasized that the revision of foreign law is not a prerequisite for the transfer of evidence obtained by French

35 Indictment of the Special Prosecutor's Office, Kt-S No. 172/22

36 The competent authorities of one contracting party may, without prejudice to their own investigations or proceedings and a prior request, provide information to the competent authorities of another contracting party that they have obtained within the framework of their own investigations, if they believe that such information would assist the recipient in initiating or conducting investigations or proceedings or could lead to a request by that state, following the provisions of this Convention or its additional protocols. The contracting party that has provided the information may, under its legislation, determine the conditions under which the recipient may use the information provided. The contracting party that has received the information undertakes to respect the conditions set. Each contracting party may at any time, by a statement addressed to the Secretary-General of the Council of Europe, declare that it reserves the right not to adhere to the conditions set by the party that provided it with information, except when it has been previously informed of the nature of the information provided and agrees to its transmission.

37 A member state may, within the limits of its national law, without a prior request, transmit information to another member state that it has obtained in the course of its own investigations if it believes that the disclosure of such information could assist the receiving member state in initiating or conducting investigations or other procedures related to offenses established in accordance with this Convention or could lead to that member state making a request for mutual cooperation based on this chapter. Before transmitting such information, the member state providing it may request that it be kept confidential or used only under certain conditions. If the member state receiving the information cannot accept such a request, it must inform the member state providing the information, which will then decide whether to still transmit the information. If the member state accepts the information under certain conditions, those conditions will be binding for it.

authorities according to French law to Montenegro's criminal proceedings. The key is that the evidence was collected in accordance with the laws of the country where it was gathered, in this case, France. Based on the principles of mutual recognition and trust in international judicial cooperation, the evidence was transferred to Montenegrin authorities. The indictment also highlights that there is no legal dispute regarding the evidence collected through the Sky ECC application, neither by French courts nor by the European Court of Human Rights or the European Court of Justice. Therefore, there is no reason to assert the illegality or inadmissibility of this evidence before Montenegrin courts.

When it comes to the decisions of the Higher Court in Podgorica confirming indictments in which the prosecution proposed communication through the Sky ECC application as evidence, including the previously mentioned indictment[38] according to the current judicial practice in Montenegro, these pieces of evidence are admissible in the indictment review process and will be evaluated during the main trial. According to the president of the Higher Court in Podgorica, *the admissibility of evidence obtained through the SKY application can only be discussed based on a final judgment, and these pieces of evidence will be considered as such*.[39] t is not realistic to expect a change in judicial practice in this regard without a prior decision by the Supreme Court on these issues, or a decision by a relevant international body. Reasons for this situation can also be found in the short deadlines for reviewing the legality of evidence in the indictment review process, especially considering that in many cases, these are the main pieces of evidence. Taking into account that the defense has the option to propose new evidence, which could lead to the exclusion of evidence proposed by the prosecution, the logic followed by judges in the indictment review process is clear and expected in that context.

Nevertheless, there are several concerning circumstances. First and foremost, holders of the highest state offices have not demonstrated a sufficient level of responsibility in cases related to the so-called Sky ECC matters. Some of them consciously violated the presumption of innocence through public statements about the accused, a fact confirmed by the Ombudsman for Human Rights and Freedoms.[40] Statements of this nature can be characterized as a form of political pressure on the work of the court and the prosecution.

38 https://sudovi.me/vspg/sadrzaj/JQRl
39 https://www.cdm.me/hronika/predsjednik-viseg-suda-o-dokazima-iz-sky-aplikacije-samo-na-osnovu-pravosnazne-presude/
40 Opinion of the Protector of Human Rights and Freedoms of Montenegro No. 236/23 dated August 2, 2023 https://www.ombudsman.co.me/docs/1694250636_02082023_preporuka_pcg.pdf

Our Criminal Procedure Code, in Article 3, explicitly prescribes the obligation to adhere to the presumption of innocence for state authorities, media, citizens' associations, public figures, and other entities. The European Court of Human Rights has also taken a clear stance that the obligation to respect the presumption of innocence extends not only to judges or the court but also to other public authorities.[41] In the same case, the Court found a violation of the presumption of innocence under Article 6 para. 2 of the European Convention on Human Rights (ECHR) due to public statements by the French Minister of the Interior against the accused.[42] In the case of Konstas v. Greece,[43] the European Court of Human Rights identified a violation of the presumption of innocence due to inappropriate statements by the Greek Minister of Justice and the Deputy Minister of Finance. These statements were directed toward the accused who had been convicted in the first-instance proceedings, while the proceedings before the appellate court were still ongoing. According to the Ombudsman for Human Rights and Freedoms, *the Prime Minister's statements exceeded the acceptable threshold of freedom of information, violated the presumption of innocence.*[44]

When discussing freedom of information, it is important to address one of the long-standing issues in the work of Montenegrin media, which often violates the presumption of innocence. In the context of the Sky ECC cases, dozens of media headlines have been observed presenting the content of that communication as if the guilt of the accused has already been unquestionably established in the criminal proceedings, even though one of the prosecution's tasks in these cases is to prove the authenticity of the evidence and that the communication indeed belongs to the accused. According to the European Court of Human Rights, although media reporting on current events is part of the freedom of expression guaranteed by Article 10 of the European Convention on Human Rights (ECHR), such campaigns and publications, according to the European Court of Human Rights's stance, can jeopardize the fairness of the trial by influencing public opinion and thereby those who are to decide on the guilt of the accused.[45]

In just two indictments in which the Special State Prosecutor's Office (SDT) used Sky ECC evidence, the content of which was published in the media, a total of 27 individuals were charged, endangering their right to the presumption of innocence as one element of the right to a fair trial.

41 Allenet de Ribemont v. France, Application No. 15175/89, dated February 10, 1995
42 Ibid
43 Application No. 53466/07, dated May 24, 2011
44 Opinion of the Protector of Human Rights and Freedoms, op. cit., p. 17.
45 Khuzhin and others v. Russia, para. 93, Application No. 13470/02, dated January 23, 2009

In the context of media disclosures of Sky ECC communication, a particularly concerning circumstance is that a portion of this communication's content was accessible to the public. Some media outlets have been publishing and continue to publish excerpts of Sky ECC communication, allegedly based on insights into documentation from EUROPOL provided to Montenegrin investigative authorities. Besides details related to the criminal offenses attributed to the accused, other information from private life has begun to emerge in the public domain. This includes not only individuals covered by the indictments but also personal correspondence of judiciary officials not subject to any indictments, thus grossly violating the right to privacy of all these individuals. The Prosecutor's Office has not yet initiated an investigation to uncover how the media obtained this information. In addition to the potential violation of the presumption of innocence and the right to privacy, there is a risk of compromising the confidentiality of data in the investigation, and hence the integrity of the investigation. There is also a danger of jeopardizing the collaboration between domestic investigative bodies and the authorities of foreign states.

CONCLUSIONS AND RECOMMENDATIONS

The latest technological advancements continue to open new dimensions in the way the judiciary deals with evidence, especially in the context of secure communication. Recognizing the ubiquitous role of electronic evidence in criminal investigations, in the past few years, we have had the opportunity to observe how the judiciary grapples with the complexity and challenges posed by such evidence. While the digital era provides new possibilities for committing crimes in ways that limit or even prevent detection and proof by state authorities, as well as for investigating and prosecuting crimes, questions regarding the legality of collecting and using such evidence become increasingly relevant.

Observing the existing practice, it is clear that the legality of collecting such evidence, their authenticity, and the defense's ability to comment on them are key aspects in considering the use of evidence obtained by intercepting protected communication. Although the legality of collecting evidence may seem to be the crucial question at first glance, a deeper examination of this issue reveals that the defense's ability to comment on the evidence is, in fact, the foundational question. This opportunity for the defense allows it to challenge the legality and authenticity of the proposed evidence, thereby

providing a comprehensive response to the prosecution's claims. Courts in various European countries, regardless of the final decision to accept or reject the evidence, have been obliged to allow the defense to examine the evidence or to disclose how it was collected. However, this is not an absolute right of the defense. Even the practice of the European Court of Human Rights (ECtHR) does not treat this right as absolute but limits it by protecting the fundamental rights of other individuals and the public interest.

The outcome of proceedings in European countries where cases related to EncroChat and Sky ECC evidence were conducted largely depended on the details of national legislation. This was essentially confirmed by the Advocate-General of the European Court of Justice, Tamara Capeta, who expressed the opinion that Germany had lawfully obtained evidence from France, but the legality of using that evidence in criminal proceedings depended on national legislation.

The examples from other countries previously described provide a fairly clear picture of how courts in European Union member states handle this evidence. In proceedings before French courts, the legality of the actions of French investigative authorities has been established and is no longer questioned, playing a significant role in the decisions of other states where proceedings based on EncroChat and Sky ECC evidence have taken place. Courts in Germany and the Netherlands believe that there is no need to assess the legality of the actions of investigative authorities in another country, but rather to start from the principles of mutual trust and mutual recognition. Norway goes a step further, allowing the use of such evidence that has been legally obtained in other countries, even if such an approach would not be legal in Norway. Regarding Italy, the decision of the Supreme Court of Italy is based on the fact that the prosecution submitted operational data from Europol as evidence, not evidence provided by the court of another country.

When it comes to the use of this evidence before Montenegrin courts, our Law on International Legal Assistance in Criminal Matters, as well as ratified international conventions in this area, incorporate these principles. It can be concluded that, by the fact that the Higher Court treats them this way, evidence collected through the Sky ECC application is lawful, i.e., admissible in the indictment control proceedings, which also represents a phase of the proceedings where their legality is assessed. However, it can also be concluded that their ultimate fate is still partly unknown.

Namely, although the Criminal Procedure Code (ZKP) does not explicitly prescribe the possibility of reviewing the legality of evidence at the main

trial, it does not prohibit it either. In practice, there have been instances (even recently) of the defense proposing new evidence during the main trial, based on which the evidence proposed by the prosecution was excluded. Besides the potential for such a situation, it is certain that the fate of this evidence, i.e., its admissibility in judicial proceedings, will also depend on the decisions of international judicial bodies if they take a specific stance on this issue. It will also rely on the future harmonization of regulations in this area, leaving no room for ambiguity or free interpretation but clearly defining the framework for the use of such evidence.

In the end, it should be emphasized that the principle of a fair trial, within which is the presumption of innocence, is one of the values that reflects the level of development of the rule of law and democratic society. Non-compliance with fundamental principles of human rights protection leads to the erosion of citizens' trust in institutions and may result in potentially negative decisions at the international level. Irresponsible, unprofessional, and unethical behavior of state and other public officials, as well as the media, is not negligible and is not without consequences. Therefore, it is crucial for all of them to act in a manner that protects and respects fundamental human rights. This is not just a moral imperative but also a practical necessity for maintaining the rule of law and democratic order.

RECOMMENDATIONS:

1. Modernize procedural legislation

To effectively address the challenges posed by digitization and crypto-communication to the judicial system, it is necessary to modernize the Criminal Procedure Code. In addition to clearly defining what constitutes digital evidence, it is necessary to establish clear protocols and standards for their authentication and use in criminal proceedings. These standards should encompass certification protocols that confirm the validity and authenticity of digital evidence, as well as criteria that must be met for such evidence to be admissible in the proceedings.

In the absence of such norms, the Supreme Court plays an important role. It should adopt clear standards and guidelines on whether and how digital evidence, such as that collected through Sky ECC communication, can be gathered, used, and evaluated in criminal proceedings, with a special focus on protecting human rights. The question is not only of a technical nature (how to ensure evidence) but also how to guarantee a fair trial. To achieve this, the Supreme Court should monitor the decisions and guidelines of other

countries that have faced similar issues, as well as decisions of international judicial bodies such as the European Court of Human Rights and the European Court of Justice.

2. Consistently respect the presumption of innocence

Comments and statements about ongoing proceedings can have a negative impact on the human rights of the accused, specifically their right to a fair trial. Such statements, when coming from high-ranking government officials, can be perceived as a form of pressure on the prosecution and the court. Politicians and public officials should refrain from commenting on specific cases and avoid making derogatory remarks, both about the accused and the work of the courts or individual judges, in order to preserve the independence of the judiciary and uphold the human rights of all citizens.

Regarding the media, when reporting on ongoing criminal proceedings, they should be aware of the impact their headlines and content can have on public opinion and the fairness of the trial. Media outlets should use neutral language that does not presume guilt, minimizing the potential influence on judicial impartiality and the integrity of the legal system, ultimately respecting the right of the accused to be considered innocent, which is a crucial element of a fair trial.

3. Preserve integrity and trust in international cooperation

It is necessary to seriously consider the potential negative impact that the leakage of information to the public can have on international cooperation in future investigations. All necessary steps should be taken to preserve trust and integrity in collaboration with foreign investigative authorities. In this regard, an investigation should be conducted to determine responsibility for the information leakage and appropriate legal actions should be taken.

4. Ensure a higher level of security for the courts

Considering that the accused individuals in cases involving evidence from the Sky ECC application are mostly in detention, and in light of last year's hacking attack on the government's information system and this year's theft of evidence from the Higher Court's depot, it is necessary to adopt security protocols both at the physical and digital levels to prevent unnecessary delays in trial hearings or even the dismissal of charges due to the compromise of evidence.

It is also essential to continue working on the implementation of a new unified judicial information system, which is currently stalled, requiring a significantly higher budget than currently allocated. Additionally, the judicial information system should not depend on the government's information

system. Therefore, it is crucial to develop mechanisms for a certain degree of decentralization. The goal is to ensure that the judicial information system continues to operate without hindrance, even if the government's information system is compromised or non-functional. Employees should also be provided with cybersecurity training to reduce the possibility of human error, which often serves as an entry point for attackers.

5. Organize trainings on new technologies and electronic evidence in judicial proceedings

The complexity of digital technology requires a certain level of expertise among judicial officials. Therefore, continuous education should be introduced to keep pace with rapid technological advancements. Training judges and prosecutors in new technologies and electronic evidence should be tailored to their needs, conducting a needs assessment and considering existing international standards and cooperation instruments, especially the Budapest Convention on Cybercrime. All holders of judicial functions should undertake a continuous education program in new technologies and electronic evidence.

Additionally, introducing an incentive system related to judicial and prosecutorial training in these areas would be beneficial. Participation in international projects for judicial training in electronic evidence would further strengthen the judiciary's position and is crucial for effectively addressing the transnational nature of issues related to electronic evidence.

ISBN 978-9911-556-11-0

9 789911 556110 >

CIP - КАТАЛОГИЗАЦИЈА У ПУБЛИКАЦИЈИ
НАЦИОНАЛНА БИБЛИОТЕКА ЦРНЕ ГОРЕ, ЦЕТИЊЕ

ISBN 978-9911-556-11-0

COBISS.CG-ID 28050436