LULËZIM BARJAMEMAJ[*] & KRISZTINA KARSAI[**] & GIOLA CAMI[***]

Intersections. EEJSP
11(4): 158–173. (2024)
https://doi.org/10.17356/ieejsp.v11i4.1515
https://intersections.tk.hu

Cross-border interception of telecommunications in relation to sovereignty and fundamental rights and freedoms:

The case of Albania

[*] [lulezim.barjamemaj@fdut.edu.al] (Lecturer, Department of Criminal Law, University of Tirana)

[**] [Karsai.Krisztina@juris.u-szeged.hu] (Prof. Dr. Habil., Full Professor, Institute of Criminal Law, University of Szeged)

[***] [cami.giola@stud.u-szeged.hu] (PhD Candidate, Institute of Criminal Law, University of Szeged)

Abstract

Evidence collection in criminal procedure requires a careful balance between effective investigative powers and the protection of fundamental rights. While traditional mechanisms of international cooperation are grounded in territorial jurisdiction and formal procedural safeguards, cross-border interception of communications challenges these models, particularly in the context of electronic evidence. Due to efficiency concerns with lengthy procedures in traditional mechanisms, newer cooperation instruments reconfigure jurisdictional and procedural powers. This study examines how cross-border evidence-gathering mechanisms implicate the principle of state sovereignty and fundamental rights, particularly where procedural safeguards differ across legal systems. It analyses the interaction between the Council of Europe framework for mutual legal assistance, centered on letters rogatory, and European Union instruments governing interception and electronic evidence. Employing normative analysis on the jurisprudence of the European Court of Justice and the European Court of Human Rights, this study argues that newly established cross-border evidence-gathering mechanisms entail asymmetric implications for state sovereignty and fundamental rights, as legal systems embed different levels of procedural safeguards and judicial oversight. This structural imbalance is exemplified by the regulatory framework and judicial practice of Albania, serving as a case study of how state sovereignty and fundamental rights are balanced in cross-border interception practices.

Keywords: *cooperation instruments, procedural powers, sovereignty, fundamental rights.*

1 Introduction

In recent decades, particularly following the end of the Cold War, the acceleration of telecommunication and information technology has played a pivotal role in driving transformation and innovation (Smil, 2025). These developments have diversified interactions among individuals and institutions and have redefined and challenged the traditional *modus operandi* of engagement within society. While globalization has unprecedentedly facilitated cross-border openness and interconnectedness[1], the increased use of computers and the internet has si-

[1] The 'openness' term was presented in conjunction with globalization in 2010 when the United Nations Office on Drugs and Crime reported their assessment on The Globalization of Crime: A Transnational Organized Crime Threat Assessment. See https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf (Accessed on

multaneously introduced new challenges for criminal law. Specifically, the emergence of digital telecommunication has resulted in the proliferation of vast datasets distributed across transnational environments, complicating investigative efforts in criminal proceedings. Encrypted telecommunication services such as EncroChat and SkyECC have marked a turning point in assessing the necessity of and control over access to such datasets, raising critical legal and operational challenges for law enforcement agencies (de Jonge & de Vries, 2024). In particular, data-driven work in a cross-border context has encountered several novel complexities in the realm of international cooperation, as traditional instruments such as Mutual Legal Assistance (hereinafter referred to as MLA) are commonly associated with lengthy and cumbersome procedures (Tosza, 2024, p. 143). *Letters rogatory* – anchored at the core of the MLA, are a formal request issued by the judicial authorities of one state to the competent authorities of another aimed at obtaining evidence. This mechanism, grounded in territorial sovereignty, requires the involvement of central authorities, such as ministries of justice, as well as compliance with the procedural safeguards of the requested state – a procedural chain of authorizations associated with extended timelines.

This has prompted law enforcement authorities to establish and adapt both substantive and procedural regulations to address transnational crime challenges, especially those correlated with the governance of cross-border interception of telecommunications and/or access to electronic evidence[2]. As technology innovates and integrates intensely in society, investigative measures are bound to technological developments such as internet-based and encrypted applications. As a result, investigative powers now extend access to subscriber, traffic and content data, often obtained in cross-border operations, rather than exclusively within a single national territory.

In this context, cross-border telecommunication refers to the legally authorized act of accessing and capturing a subject's telecommunication data—whether transmitted via wire, radio, electromagnetic, photoelectronic, or photo-optical systems—by law enforcement agencies for the purpose of criminal investigation (Council of the European Union, 1995). Under recent instruments governing procedural powers in criminal matters, the interception of telecommunications is no longer viewed as limited solely to the content of telecommunications. It also encompasses the collection of traffic and location data correlated with such telecommunication (Directive 2014/41/EU of the European Parliament and of the Council, 2014, para. 30).

As the MLA framework has been criticized for its limited functionality—largely due to its reliance on outdated principles of territoriality (Tosza, 2023, p. 216)—new data-gathering instruments have been introduced. These tools establish a direct interplay between the judicial authority of the prosecuting state (issuing state) and a private entity outside its jurisdiction (Forlani, 2023). The debate on cross-border data access centers on the tension between traditional legal instruments and the growing practice of direct access to service providers. In particular, discussions surrounding the interception of telecommunications highlight issues of state sovereignty in criminal matters. Such investigations frequently intersect with the principle of territoriality, raising complex jurisdictional and sovereignty concerns (European

February 20, 2025).

[2] In 2018, the European Commission reported that over half of all investigations involved a cross-border request for access to electronic evidence. See their Impact Assessment Report 'Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings,' No. 118, pp.14, 2018, Brussel. See https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN (Accessed on February 20, 2025).

Commission, 2024).

This study selectively analyzes the procedural regulations governing MLA in Albania, an EU Candidate country. While Albania is a party to the European Convention on Mutual Assistance in Criminal Matters and continues to apply a sovereignty-centered MLA framework based on letters rogatory, it is simultaneously engaged in accelerated efforts to approximate its domestic legislation with the EU acquis. This two-fold positioning anchors Albania at the intersection of traditional international cooperation mechanisms and novel mechanisms of cross-border evidence gathering in compliance with EU Acquis. A case study of Albania, hence, elucidates asymmetries between territorial principled safeguards and new practices seeking to bypass lengthy procedural processes. Under the Albanian legal framework, state sovereignty is primarily exercised through judicial and investigative authority, which governs the state's ability to prosecute, investigate, and adjudicate criminal offenses (Republic of Albania, 1998, Art. 7, parts 9–10). As a fundamental component of criminal procedural law, this authority is closely linked to the principle of territoriality, rendering cross-border investigative measures—especially in the context of telecommunication interception—a particularly sensitive issue in the sovereignty debate (Republic of Albania, 1995, Art. 2). Article 148 of the Constitution grants to the prosecution the authority to conduct criminal prosecutions and represent cases in court. When evidence collection significantly intrudes on privacy, the Criminal Procedure Code mandates judicial oversight to ensure proportionality through a court-issued decision. Within Albania's jurisdiction, investigative actions are readily enforceable, as judicial decisions are binding on all individuals and entities—public and private—within the national territory[3].

Nevertheless, when evidence collection extends beyond Albania's borders, neither the courts nor the prosecution possess direct authority over foreign individuals or entities. In such cases, interstate cooperation becomes essential for accessing and collecting evidence, necessitating legal engagement with the jurisdiction of another state. As organized crime is increasingly spanning through the territories of multiple countries (Eurojust, 2024), there is need for enhanced cross-border investigations. As a result, state authorities collaborate to access telecommunications while ensuring that evidence interception respects state sovereignty and complies with the legal frameworks of each jurisdiction. Legal complications emerge when a state intercepts telecommunications abroad without approval, particularly under legal systems that differ from those where the evidence is eventually employed. This study argues that evidence obtained vis-à-vis cross-border interception procedures, potentially outcomes asymmetric implications, particularly where such investigatory powers involve jurisdictions operating under uneven procedural safeguards and lying outside the scope of mutual trust framework.

Consequently, the admissibility of such evidence comes under legal scrutiny, as demonstrated in the EncroChat operation (Europol, 2023), where French authorities intercepted telecommunications without prior authorization from the states where the subjects, encompassing those located in Albania, were situated (*MN* (EncroChat), 2024). The case raises a critical question: Is such evidence legally admissible in criminal proceedings in Albania, and does it comply with domestic and international legal standards?

The current study explores the complex interplay between state sovereignty, due process, and cross-border telecommunication interception and aims to answer the following questions: First, how do cross-border telecommunication interceptions challenge national sovereignty? Second, how does the Albanian legal framework regulate the use of intercepted

[3] We are referring to the Albanian legislation, as it is the subject of the paper, but we can say that the same rules apply mutatis mutandis to other jurisdictions.

telecommunications as evidence, and to what extent does it align with standards set by the European Union (EU) and the Council of Europe (CoE)? Third, what are the implications of cross-border interceptions for fundamental rights, particularly in terms of due process and the admissibility of cross-border evidence?

The first part of the analysis will examine doctrinal developments related to the concept of state sovereignty and the challenges encountered in cross-border criminal investigations, with globalization and technological advancements blurring the lines. The analysis will also explore the theoretical distinction between the interception of telecommunications and the collection of electronic evidence, focusing on the human rights implications arising from data externalization.

The second part of the analysis will investigate the interaction between state sovereignty and international legal frameworks, assessing how CoE and EU instruments regulate cross-border cooperation while safeguarding privacy and due process. Additionally, it will review the European Court of Human Rights (ECtHR) and the Court of Justice of the EU (CJEU) case law, including the EncroChat ruling *(MN (EncroChat), 2024),* to clarify key legal challenges associated with cross-border evidence gathering and the preservation of state sovereignty. Ultimately, this study seeks to address the tensions between state sovereignty, transnational crime, and legal standards and determine whether procedural reforms are necessary to achieve a more balanced approach for governing cross-border data processing.

2 Methodology

This doctoral research adopts a qualitative legal methodology, integrating an in-law analysis of scholarly literature on one side, and regulations composed of statutory provisions and case-law interpretations on the other side. We critically examine procedural norms, legal doctrines, and judicial jurisprudence governing cross-border telecommunication interception to assess their legal consistency, as well as compliance with human rights and sovereignty principles. This research employs doctrinal analysis of Albanian constitutional and criminal procedural law, focusing on norms governing the interception of telecommunications and the admissibility of evidence. Particular attention was given to provisions that mandate judicial authorization and define procedural consequences for unlawfully obtained evidence. Moreover, the investigation reviews jurisprudence based on relevant ECtHR and CJEU rulings. Case law was selected for its relevance to state sovereignty, the protection of fundamental rights, and the use of cross-border evidence in criminal proceedings. While the selected ECtHR judgments establish minimum standards, CJEU rulings assess the implications of procedural safeguards within EU cooperation mechanisms. In addition, selected Albanian case law clarifies how domestic courts balance sovereignty with evidence. Finally, the study proposes *de lege ferenda* recommendations to refine the integrity of cross-border data collection with regard to telecommunication interception.

3 Doctrinal perspectives

3.1. State sovereignty in international criminal law

The principle of sovereignty has been foundational to the concept of nation-states since 1648, when the Peace of Westphalia ended the Thirty Years' War and established the framework for the modern international order. International law has long considered territoriality a defining feature of state sovereignty, constituting, *in concreto,* the legitimate exercise of criminal

jurisdiction within a state's territorial boundaries (Beale, 2023). Hence, sovereignty is intrinsically linked to jurisdiction; international law defines the boundaries of sovereignty by limiting how states exercise jurisdiction to prevent conflicts (Kelsen, 1952). *In stricto*, the enforcement of criminal law across borders is constrained by international law through the principle of jurisdiction, which empowers states to prescribe, adjudicate, and enforce (Liivoja, 2010; Malanczuk, 1997; Payer, 2023). *Prima facie*, sovereignty is, hence, understood as a fixed, well-defined, and unchangeable concept. However, this monolithic and rigid view has been increasingly challenged by scholars who characterize sovereignty as dynamic and flexible (Kelsen, 1960), capable of evolving within legal frameworks and international relations (Cryer, 2005). Although initially treated as a theoretical matter, the traditional Westphalian notion of absolute state sovereignty has been challenged by the emergence of human rights and transformed into a more limited and accountable concept (Brooks, 2012).

The most significant challenge to the monolithic view of state sovereignty in criminal law arises from the evolving nature of crime, fuelled by rapid advancements in telecommunications and technology. The proliferation of cross-border data exchange in the digital space has defied legal governance, prompting lawmakers to adopt normative regulations embedded in the principle of state intervention (Glen, 2014). A core argument concerns the position of current state measures along the spectrum between techno-authoritarianism and protectionism in safeguarding data and digital infrastructure fall (Burwell and Propp, 2022). Although the debate remains underdeveloped, the question whether cyberspace should be regarded as a distinct domain, given its borderless and decentralized architecture, could bolster claims of autonomy from territorial sovereignty (Wu, 1997). This proposition has largely been rejected in favour of applying territorial sovereignty and jurisdiction to cyber infrastructure (Heintschel von Heinegg, 2012).

Against this theoretical background, evidence collection—involving access to data either produced or stored in another state's jurisdiction—has been increasingly subject to cross-border investigative powers. Nonetheless, when data are accessed from foreign territories, concerns emerge regarding potential infringements on state sovereignty (Sieber and Neubert, 2017). The transnational nature of crime has made international cooperation crucial for the exercise of investigative powers; such cooperation depends on instruments established in international treaties through which signatory states voluntarily cede a degree of sovereignty by committing to shared rights and obligations (Ouwerkerk, 2015). The principle of dual criminality has traditionally upheld state sovereignty by restricting foreign interference in domestic legal matters. Nevertheless, as cross-border crimes have grown increasingly complex, the principle of territoriality has been adjusted through cooperative mechanisms designed to address these challenges more effectively (Braum, 2020). In the EU, the mutual recognition principle[4] enshrined in Article 82 of the Treaty on the Functioning of the European Union (TFEU) strengthens cooperation in criminal matters, notwithstanding inefficiencies that have been raised when cross-border data access interfered with sovereignty (Braum, 2020).

Cross-border data gathering poses the most significant challenge to the state sovereignty, as it allows states to assert extraterritorial enforcement jurisdiction, compelling entities to disclose data stored in foreign territories, and often bypassing MLA treaties (Currie, 2017). Investigative powers in a cross-border context have redefined jurisdiction by adapting sovereignty to a new principle of 'extended territoriality', which permits states to assert authority over

[4] The principle of mutual recognition as the foundation of judicial cooperation in criminal cases was first presented in 1999 at the Tampere European Council. The European Arrest Warrant (2002) was the first major implementation of the principle in criminal law. However, the Treaty of Lisbon (2009) further reinforced its legal basis in the TFEU, formally attributing mutual recognition as the foundation of judicial cooperation in criminal matters.

data that is substantially connected to their territory, even if physically located elsewhere (Coughlan et al., 2014, p. 35–36). In this context, extraterritoriality revises rather than erodes the traditional understanding of state sovereignty tied to national territory, as data cannot be reduced to a purely technical category. Because data inherently carry human rights implications, and its flow is indifferent to the physical borders, jurisdictional conflicts expose the limits of classic territorial jurisdiction (Obendiek, 2022). Although extraterritorial jurisdiction is legitimated as a procedural remedy to cross-border data flows, its relational interplay with data legality, over protectionist policies, and data protection norms gives rise to tensions with traditional conceptions of state sovereignty. These tensions have elicited divergent distinct approaches. The International Court of Justice stipulates that states should exercise their sovereignty within the limits of international law (Permanent Court of International Justice [PCIJ], 1927, p. 19). EU policymaking has adopted a pluralist approach to transnational law within the Union, therefore softening the hierarchical or exclusive conception of sovereignty to accommodate policies in favour to interacting legal orders. National law, EU cooperation mechanisms, and human rights frameworks concurrently exercise authority over data, leaving courts burdened with the responsibility to assess the proportionality legal issues. For instance, the Convention Implementing the Schengen Agreement allows for the relaxation of sovereignty constraints between EU Member States to allow cross-border surveillance or hot pursuit, prioritizing efficiency and expediency in criminal investigations (Convention Implementing the Schengen Agreement, 1990, Art. 40). In certain cases, practical considerations may override national sovereignty, potentially paving the way for more collaborative, transnational policing. Cross-border interception of communications exemplifies this tension, as EU cooperation mechanisms interplay with domestic procedural regimes within a partially integrated framework of procedural safeguards.

3.1 Legal and procedural considerations in cross-border telecommunications

Within the framework of international law governing cross-border access, the CoE offers procedural powers that allow the search, seizure, preservation, and interception of data, all of which are applicable in the context of administering electronic evidence in criminal proceedings (Council of Europe, Cybercrime Convention Committee [T-CY], 2012). The Budapest Convention on Cybercrimes (hereinafter referred to as the Budapest Convention) classifies electronic evidence into three categories: subscriber data, traffic data, and content data[5], the latter is obtained via real-time collection or recording of content data on specified telecommunications (Council of Europe, 2001, Art. 21, para. 2). Additionally, the Explanatory Report to the Budapest Convention examines the investigative powers enabling the real-time interception of content data, encompassing technical means such as direct system access, eavesdropping, or tapping devices, which enable monitoring, recording, or collecting telecommunications within the jurisdiction of the issuing state (Council of Europe, 2001, para. 53). This provision is crucial for enhancing investigative efficiency in handling electronic evidence by introducing measures that may overlap with the interception of telecommunications, a distinct investigative power. Such dynamics have been addressed in a ruling by the CJEU, which clarifies that decrypting telecommunications from internet-based applications constitutes interception rather than mere monitoring, particularly when it involves capturing traffic, loca-

[5] The three categories of evidence are stipulated in Articles 18, 20, and 21 of the Convention on Cybercrime, Budapest, 23.11.2001, ETS No. 185. While subscriber data and traffic data differ in substance from the interception of communication, content data bears a closer resemblance to interception, as it contains the actual substance of a communication. Nonetheless, the key distinction lies in the temporal aspect—content data refers to already stored information, whereas interception encompasses real-time access to ongoing telecommunications.

tion, and content data in real time (*MN* (EncroChat), 2024).This distinction is fundamental because interception necessitates notification to the state where the targeted individuals are located, whereas traditional electronic evidence collection does not.

In the same spirit, following the cross-border interception of data from the Sky ECC application, the Constitutional Court in Albania (Constitutional Court of Albania, 2024) distinguishes the interception of telecommunications from evidence by asserting that interception is merely a method of collecting information in real time and does not automatically qualify as admissible evidence. Moreover, the court noted that intercepted data must undergo legal validation before being employed in judicial proceedings, ensuring compliance with procedural guarantees, authenticity requirements, and due process principles. The court established that intercepted data alone is insufficient unless processed according to established evidentiary rules.

3.2 A Perspective on human rights implications

Digitalization's interference with sovereignty requires a substantial procedural reconsideration of established data governance frameworks, especially in light of the significant challenges posed by cross-border data acquisition and investigative powers. The un-territoriality of data (Daskal, 2015) has primarily raised jurisdictional dilemmas, with the most delicate issue being the balance between public interest and privacy, and broader implications for human rights. The CoE and the EU have established shared safeguards for human rights, particularly in the criminal law domain, enshrined in two key instruments: the European Convention on Human Rights (ECHR) and the Union's Charter on Fundamental Rights (CFREU) (Bose, 2023). The ECtHR has particularly addressed the violations of Article 8 in some cases, ruling that authorized measures have interfered with the relevant rights, specifically in the context of investigative powers correlated with interception and surveillance (European Court of Human Rights, 2002, 2018). Furthermore, the Court has held that laws mandating bulk retention of all internet communications, providing unrestricted access to security services, and requiring decryption of end-to-end encrypted messages breach Article 8 when they lack adequate safeguards and undermine the right to private life (European Court of Human Rights, 2024). This ongoing debate underscores the urgent need for robust mechanisms to ensure fairness in data processing, grounded in the principles of legality and necessity (Topalnakos, 2023). Nevertheless, the aforementioned safeguards are rooted in data protection legal guarantees, which are asymmetrical among jurisdictions and offer imbalanced protection levels (Alimonti, 2022). Thus, some jurisdictions applying stricter protection rules have pushed for the extraterritoriality of domestic data protection law toward other jurisdictions, with perceived weaker standards (Hornkohl, 2022; Taylor, 2015). Notably, the CJEU has institutionalized the EU's externalization of its data protection law by systematically evaluating whether third countries meet the Union's standards (Fabbrini and Celeste, 2021; Tzanou, 2021), notably in its Schrems I & II case law (Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Schrems II), 2020; Maximillian Schrems v Data Protection Commissioner, 2015).

4 Discussion

4.1 Legal conditions for the interception of telecommunications under Albanian law

The notion of legally obtained evidence is first introduced in Article 32 (2) of the Constitution of the Republic of Albania, which stipulates that *no one can be declared guilty based on*

evidence collected unlawfully. While this constitutional provision establishes a standard for the admissibility of evidence at trial, it is the domain of criminal procedural legislation—as a special law (*lex specialis*)—to define what constitutes unlawful collection (*contra legem*) and how such evidence should be sanctioned. Accordingly, Article 151 of the Code of Criminal Procedure of the Republic of Albania (CPrC) stipulates that evidence obtained in violation of legal prohibitions may not be used at trial. Hence, the constitutional term 'evidence obtained unlawfully' should not be interpreted as referring to any evidence gathered with mere procedural irregularities; it only indicates evidence collected in breach of explicit legal prohibitions. The concept of inadmissibility implies that the evidence completely loses its probative value and cannot be subjected to judicial evaluation. Thus, inadmissibility should be understood as a procedural sanction that affects evidence collected in violation of legal prohibitions (Ligori, 2015, p. 101).

An analysis of Articles 222–226 of the CPrC reveals that Albanian procedural law aligns with the minimum standards established at the European level. Article 221(a) of the CPrC stipulates that the interception of a person's private telecommunications, utilizing any transmitting device, is permissible only in cases involving intentional crimes for which the maximum penalty is no less than seven years of imprisonment. Article 221(b) and (c) expands the scope of offenses eligible for interception beyond the general rule tied to maximum penalties, allowing for interception in certain lower-penalty crimes. Considering that interception fundamentally infringes upon the right to private life, Article 221(3) of the CPrC stipulates that interception may be ordered against the following subjects: (i) a person suspected of committing a criminal offense; (ii) a person suspected of receiving or transmitting telecommunications from the suspect; (iii) a person involved in transactions with the suspect; and iv) a person whose surveillance could result in the discovery of the suspect's location or identity. From a literal and purposive interpretation of this provision, we conclude that interception may be ordered only against the subjects listed exhaustively in this provision. Thus, *a contrario*, interception cannot be authorized against individuals who have no connection—even indirect—with the criminal offense under investigation.

Referring to the standards established by the ECtHR, and in order to understand the national legislative approach, it appears that the Albanian legislator has aimed to ensure and reflect every jurisprudential development and safeguard established by the ECtHR. Specifically, the ECtHR stated that, to legalize secret interception measures, states must meet certain guarantees to prevent abuse of power. These include the following: (i) the legal provision must contain a definition of the nature of the criminal offenses for which this evidence-gathering tool may be employed; (ii) the legal provision must contain a definition of the categories of persons responsible for the interception; (iii) a time limit for the duration of the interception must be established; (iv) the procedure to be followed for examining, utilizing, and storing the obtained data must be regulated; (v) precautionary measures during the telecommunication of the data to other parties must be established; and (vi) the circumstances in which the recordings may or must be deleted or destroyed must be stipulated (*Roman Zakharov v. Russia*, 2015).

Finally, Article 225 of the CPrC provides for the possibility of employing and transferring the results of interceptions beyond the specific criminal proceeding in which they were obtained. Thus, for the purposes of another criminal proceeding, interception results gathered for a previous criminal proceeding are submitted to another prosecuting authority.

4.2 CoE and EU legal framework for mutual legal assistance

The CoE adopted the European Convention on Mutual Assistance in Criminal Matters of 1959 (hereinafter referred to as the '*Convention'*) to establish a legal framework for MLA in criminal matters. This Convention was ratified by Albania in 1999[6] and is an integral part of the domestic legal system.[7] Additionally, the CPrC [8] and the Law No. 10 193, dated 3.12.2009, 'On Jurisdictional Relations with Foreign Authorities in Criminal Matters,'[9] offer more detailed provisions implementing international norms in this area. The Convention aims to allow parties to offer one another legal assistance in criminal matters within the scope of their respective jurisdictions.

While the Convention seeks to facilitate the exchange of evidence between Member States, this does not imply that a European legal framework has been adopted that allows for the automatic and unimpeded provision of legal assistance. The contracting parties retain full sovereign rights and have full discretion over whether to execute a request from another state. The requested state may refuse MLA if it considers that executing the request would compromise its sovereignty, security, or the fundamental interests of its legal order. Similarly, to protect its sovereignty and legal system, Article 505 of the CPrC provides that the Minister of Justice of Albania shall not grant a letter rogatory if the investigative actions requested by a foreign authority are expressly prohibited by Albanian legislation. This provision confirms that Albania cannot extend legal assistance to a foreign authority when such investigative actions contradict the core principles of its national legal order.

Article 15 of the Convention embodies the political design of letters rogatory, by designating the Ministry of Justice as the intermediary in cross-border cooperation, including the scrutiny of requests in urgent cases.

Meanwhile, within EU's jurisdiction, the European Parliament and the Council adopted Directive 2014/41/EU on the European Investigation Order in Criminal Matters (hereinafter referred to as 'EIO Directive') to facilitate the exchange of evidence without the interference and decision-making of administrative and political authorities. The EIO, enforceable among Member States [10] based on the principle of mutual recognition of criminal judgments, differs from traditional MLA by replacing the 'requesting/requested State' terminology with 'issuing/executing State' (Karsai, 2019, 9.156). An EIO allows the issuing state to request either the gathering of new evidence abroad or the transfer of evidence already obtained by another Member State and must be executed without added formalities by the executing authority, as enshrined in the *forum regit actum principle.* The executing authority must follow EIO formalities and procedures unless this is contrary to its fundamental principles and legal order (Tomasits, 2021, p. 85).

Since its implementation in 2017–2018, the EIO has become the primary instrument for obtaining evidence across EU Member States, facilitating cross-border investigations while still encountering legal and practical challenges (Guerra and Janssens, 2019, p. 46).

Articles 31 and 32 of the EIO Directive differentiate between cases requiring communication with the executing state and those allowing interception without it. When technical assistance from the state where the subject is located is essential, the execution of the EIO to authorize and continue the interception may be refused if a similar investigative measure (in-

[6] The Convention was ratified by the means of Law No. 8498, dated 10.6.1999, 'On Jurisdictional Relations with Foreign Authorities in Criminal Matters' OJ. 21-1999.
[7] Art. 5 in. review with Art. 122 of the Constitution.
[8] Art. 505 et seq. of the Code of Criminal Procedure.
[9] Art. 13–30.
[10] While the EIO has been adopted by most of the EU Member States, Denmark and Ireland have not implemented it within their national legal frameworks.

terception) is not authorized by the state's authorities in a domestic context. This provision is fundamentally based on the principle of equivalence, which affirms that the same legal remedies (*actiones*) and procedural rules applicable under the national legislation of Member States should be applied analogously to legal actions according to EU legislation, as noted by the Advocate General (Jääskinen, 2013). This principle is applied to preserve sovereign rights and guarantee the protection of the rights of intercepted subjects, with the state conducting the interception having the right and the obligation to make decisions in accordance with its domestic law. Notably, this instrument does not have a suspensive or abrogative effect on Member States' obligations to respect fundamental rights and legal principles enshrined in Article 6 of the Treaty on the EU, encompassing rights correlated with the effective protection of individuals in criminal proceedings and any obligations placed on procedural authorities in this regard (Kordík and Kurilovská, 2018, p. 4). Conversely, the EIO Directive is the first EU instrument based on the principle of mutual recognition of judicial decisions that explicitly establishes the protection of fundamental rights and freedoms of individuals as valid grounds for refusing execution (Dediu, 2018, p. 207).

When the technical assistance of the state in which the target of interception is located is not required, the proceeding state (the notifying state) must inform the state where the interception will be performed (the notified state) before the commencement of the interception if known in advance. If the cross-border nature of the interception only becomes apparent during or after its execution, then the notifying state must give notice as soon as it is aware of this fact. Should the legislation of the notified state prohibit such an interception in a similar domestic context, it has the right to request, within 96 hours of obtaining the notification from the proceeding state, the termination of the interception and the destruction of the data acquired up to that point. Contrarily, if the notified state does not act within this timeframe, then it is deemed to consent to the interception being conducted by the proceeding state within its territory.

In addition to real-time cross-border interception, the EIO Directive provides for the possibility of transferring the results of the interception of telecommunications already in the possession of a Member State. Nonetheless, in this case, the EIO Directive ensures that the issuance of an EIO must pass the legality test of the requested investigative action, stipulating that the order for obtaining evidence already in the possession of an authority in one Member State is allowed only if such a measure (the transfer of already gathered evidence) would have been ordered in a similar domestic case.

4.3. General overview of the ECtHR jurisprudence regarding cross-border evidence

The adoption of international instruments in the field of MLA in criminal matters naturally raises concerns regarding the elements of due process, particularly when evidence is obtained outside the territory of the prosecuting state. Such situations challenge the full application of the principle of equality of arms (*audi alter partem*). As affirmed by the ECtHR, the Convention does not contain specific provisions on the admissibility of evidence. Therefore, its assessment as a court extends only to the violation of Article 6 of the ECtHR during the procedure of collecting evidence, highlighting that the accused and their representative must have the opportunity to effectively challenge the cross-border evidence during the trial (*audi alter partem principle*).

Following a 2001 ECtHR judgement, the applicant claimed a breach of the right to a fair trial because his conviction was largely based on evidence acquired through international procedures via letters rogatory from the United States, with no opportunity to cross-examine the witnesses (European Court of Human Rights, 2001). The ECtHR reiterated that all evi-

dence should be presented in a public hearing, in the presence of the accused, allowing for an adversarial argument. Nevertheless, this does not mean that testimonies must invariably be made in public court sessions.

In another case involving similar claims regarding the violation of due process due to the inability to question a witness in a public hearing, the ECtHR ruled in favor of the applicant (A.M. v. Italy, 1999). Additionally, the court has reasoned that the information, which emanates from diverse, objective, and concurring sources, establishes that there was, at the material time, a 'real risk' that the impugned statements had been acquired in Morocco utilizing methods prohibited by Article 3 of the Convention (European Court of Human Rights, 2012).

These three ECtHR rulings serve as guidelines for cross-border evidence-gathering procedures, reiterating the significance of respecting the principles of due process. While acquiring evidence beyond the territorial borders of the prosecuting state is not in itself contrary to the ECtHR, it is essential to guarantee that the right to effectively challenge such evidence is preserved during or after its acquisition.

4.3 CJEU jurisprudence: standards deriving from the 'EncroChat' case

Based on the above discussion, recent developments in the case law of the CJEU are particularly significant. For instance, numerous critical questions were raised regarding the interpretation of the EIO Directive's provisions and the legality of transferring data acquired through cross-border interception by one state outside of its own territory and without permission or notification of other states where the intercepted subject was located *(MN (EncroChat), 2024)*.

The case concerns decryption and subsequent comprehensive collection of data from the servers of a mass telecommunication application. Specifically, the French police, assisted by Dutch experts and acting under authorization from a national court in accordance with domestic regulations, succeeded in breaching the encrypted service of the *EncroChat* telecommunication application (MN (EncroChat), 2024). The case raises concerns about compliance with the EIO Directive, as French authorities unilaterally decrypted and recorded all EncroChat data without temporal or territorial limitations, subsequently transferring that data to Germany based on EIOs issued by German prosecutors.

The case is pivotal for clarifying the EIO Directive, particularly regarding competent authorities, conditions for evidence transfer, the nature of decryption processes, requirements for notification and cooperation in cross-border interception, and the evidentiary use and contestability of such intercepted data CJEU clarified that the EIO Directive does not exclusively designate judicial authorities as the issuing authority for EIOs, concluding that a prosecutor also has the authority to request evidence from outside their state's territory, provided this authority is recognized under the domestic law of the issuing state.

Regarding the conditions for issuing an EIO for the transfer of evidence already in the possession of the executing state, the CJEU explained that the EIO Directive sought to unify the fragmented legal basis concerning cross-border evidence exchange. It added that the issuing state, under the principle of mutual recognition of judicial decisions, cannot question the evidence-gathering procedure by the executing state. Accepting the contrary would render the entire new system regulated by the EIO Directive ineffective. Nonetheless, the CJEU also clarified that this does not imply a waiver of guarantees correlated with fair legal process.

In interpreting Article 6 of the EIO Directive, the court explicated that this legal instrument does not itself limit the issuance of an EIO for evidence already held by another Member

State but instead requires compliance with the principle of equivalence pursuant to the issuing state's law.

The CJEU also addressed the procedural nature of measures involving the penetration of endpoint devices to collect traffic, location, and telecommunication data from an internet-based telecommunication service, interpreting that this process constitutes "communication interception". If conducted outside the territory of the executing state, according to Article 31 of the EIO Directive, it must be processed with notification to the state where the intercepted subjects are geographically located.

After exhausting all procedural tests, the CJEU concluded that data acquired from decrypting applications such as 'EncroChat' may be employed as evidence by national criminal courts. However, such evidence must be excluded from trial if it has a predominant impact on determining guilt and the defendant has not been provided with a meaningful opportunity to challenge and contest the legality and evidentiary value of the data.

4.4 Possibility of utilizing cross-border interception as evidence

As previously explained, interception of telecommunications as a means of evidence collection must be ordered by a court, in strict adherence to the legal conditions for permitting such interception of telecommunications. From the Albanian perspective, the legal assessment is not confined solely to the verification of the legal conditions (applicable law and factual circumstances) of the foreign authority's decision but also extends to the legal implications of such interceptions when conducted by individuals who acted within the Albanian territory.

A narrow (*strictu sensu*) interpretation of Article 222 of the CPrC, in conjunction with Article 226, reveals that the Albanian legislator allows the admissibility of interception of telecommunication results acquired from foreign authorities, only when they are being processed through letters of rogatory. The lack of a decision from Albanian judicial authorities, for interceptions conducted on subjects located within Albanian territory, would constitute an unlawful exercise of procedural powers, infringing upon state sovereignty. The investigative power correlated with the interception of telecommunications belongs to the courts of the Republic of Albania, as one of the elements of exercising sovereignty independently. Even more so, when the foreign authority conducts an interception without identifying the subject being intercepted as provided for in Article 221 (3) of the *CPrC* of the Republic of Albania, the evidence becomes inadmissible.

The argument against the admissibility of telecommunication interception results obtained in this manner is also correlated with the inability of the intercepted subject to effectively challenge the judicial decision that authorized such interception jeopardizing the rights granted in Article 6 of the ECtHR. Consequently, a decision authorizing the interception of telecommunications of such a subject outside the territory of the state conducting the investigation may exceed the legal conditions outlined above. Consequently, the data obtained from the interception of telecommunications would be ruled inadmissible, barring no probative value.

In a similar case, the former Court of Appeal for Serious Crimes (CASC) reasoned that the interceptions conducted by foreign authorities against individuals who were geographically located in the Republic of Albania were inadmissible in the criminal proceedings being held in Albania (Court of Appeal for Serious Crimes, 2009, Decision No. 2). CASC argued that, under the interpretation of the procedural criminal law and the international conventions ratified by Albania, the interception of Albanian nationals' phone conversations within the territory of the Republic of Albania was a violation of the country's sovereignty in exercising criminal prosecution and administering justice. CASC clarified that Italian authorities

had intercepted fixed and mobile phone numbers assigned by Albanian telecommunication companies employed by Albanian nationals engaged in drug trafficking extending to Albania, Italy, and beyond. By doing so, the Italian judicial authority performed investigative actions within the Albanian territory—it exercised its jurisdiction (judicial function) within the territory, and assumed the exclusive functions of the Albanian state, without such a right being granted by Albanian domestic law or any bilateral international agreements, thereby infringing upon Albanian sovereignty (Court of Appeal for Serious Crimes, 2009, Decision No. 2, p. 30).

The limits on the admissibility of cross-border interceptions do not prevent the prosecution from investigating the criminal act through other lawful means of searching/obtaining evidence. Although the results of the telecommunication interceptions conducted as described above are inadmissible, they may still provide the prosecution with grounds to initiate an in-depth investigation, in line with the principle of due process.

5 Conclusions

In the broader analysis of the regulatory framework governing the collection of cross-border evidence and the usage of interception as an evidentiary tool, we contend that, despite the shared purpose of facilitating cross-border evidence gathering—MLA instruments and the newly introduced EU mechanisms—propel asymmetric implications for state sovereignty and fundamental rights. While letters rogatory remain anchored in territorial sovereignty and preserve ex ante judicial oversight, newer mechanisms prioritize procedural efficiency and post hoc safeguards, with the effect of reallocating control over investigative powers. Sovereignty in the context of investigative measures involving digital components is no longer exercised solely through territorial control; instead, it is being reconfigured through legal powers and procedural controls over investigative actions. Cross-border interception practices exemplify how sovereignty is recalibrated with authority being reconsidered in layered legal orders, with courts policing jurisdictional boundaries vis-à-vis the assessment of proportionality, legality, and fundamental rights protection.

This procedural divergence is particularly relevant for Albania, a non-EU member, currently engaged in accelerated accession procedures. Although the mutual recognition paradigm and its associated procedural safeguards have not been yet incorporated into the domestic legal order, Albania's reliance on prior judicial authorization and stringent admissibility rules, rather than outdated practices, reflects a constitutional commitment mitigating risks arising from cross-border interception practices. In this sense, the Albanian approach contributes to a broader European debate on procedural guarantees, affirming a sovereignty-conscious approach mitigating the attenuation of constitutional guarantees in the pursuit of investigative efficiency.

Where conflicts stem between Albanian constitutional standards and nascent evidentiary practices, the limits of legal convergence are reflected. For intercepted data obtained by means of EU mechanisms without prior territorial authorization, Albanian courts remain constitutionally bound to assess such evidence against domestic guarantees of due process and privacy, as mandated by Articles 6 and 8 of ECHR. This tension suggests that mutual trust paradigm is insufficient to sustain effective cross-border cooperation, and that, in this regard, differences in sovereignty and fundamental rights protection must be taken into account, particularly for jurisdictions engaged in EU accession processes. With regard to the ongoing debate within the EU, CJEU has already clearly articulated the nature of the decryption process of the 'EncroChat' application and the conditions under which data acquired

through this process may be lawfully utilized. While the CJEU lacks the authority to render a binding decision beyond its jurisdiction, we argue that this decision is, nonetheless, instructive for Albanian courts for several reasons. First, the CJEU's ruling is distinctive within European jurisprudence, providing Albanian courts with a precedent for defining the decryption process of the 'EncroChat' application and similar platforms. Second, this decision addresses critical questions and informs on the establishment of appropriate safeguards for defendants during the evidentiary debate, an issue that should be carefully considered by Albanian courts for ensuring procedural fairness. Third, considering that comparative law is a recognized method of legal interpretation, the spirit of this decision holds relevance for comprehending the broader issues addressed by the ECtHR in its jurisprudence.

References

Alimonti, V. (2022). Assessing new protocol to the Cybercrime Convention in Latin America: Concerns, human rights considerations, and mitigation strategies. Electronic Frontier Foundation. https://necessaryandproportionate.org/files/protocol-cybercrime-convention-latam.pdf.

Beale, J. H. (2023). The jurisdiction of a sovereign state. *Harvard Law Review*, 36:241–262.

Bose, M. (2023). Fundamental rights protection. In Ambos, K. and Rackow, P., editors, *The Cambridge Companion to European Criminal Law*, page 57–86. Cambridge University Press.

Braum, S. (2020). 'Rechtsstaat' and European criminal law – From the end of sovereignty. *New Journal of European Criminal Law*, 11(4):1–9.

Brooks, R. (2012). Strange bedfellows: The convergence of sovereignty-limiting doctrines in counterterrorist and human rights discourse. *Georgetown Journal of International Affairs*, 13(2):125–133.

Burwell, F. G. and Propp, K. (2022). *Digital sovereignty in practice: The EU's push to shape the new global economy*. Atlantic Council.

Constitutional Court of Albania (2024). *Ruling No.* 86, dated 30 December 2024.

Coughlan, S., Currie, R. J., Kindred, H. M., and Scassa, T. (2014). *Law beyond borders: Extraterritorial jurisdiction in an age of globalization*. Irwin Law.

Council of the European Union (1995). Resolution on the lawful interception of communications. *Official Journal of the European Communities, C*, 329:1–2.

Cryer, R. (2005). International criminal law vs. state sovereignty: Another round. *European Journal of International Law*, 16(5):979–1000.

Currie, R. J. (2017). Cross-border evidence gathering in transnational criminal investigation: Is the Microsoft Ireland case the 'next frontier'? Canadian Yearbook of International Law, 54, 63–97. https://doi.org/10.1017/cyl.2017.7.

Daskal, J. (2015). The un-territoriality of data. *The Yale Law Journal*, 125(2):326–398.

Dediu, D. (2018). The European Investigation Order in criminal matters – Grounds for non-recognition or non-execution. *Lex et Scientia International Journal*, 25:202–210.

Eurojust (2024). Annual report 2023. https://www.eurojust.europa.eu/sites/default/files/assets/eurojust-annual-report-2023-en.pdf.

European Commission (2024). Concluding report of the High-Level Group on access to data for effective law enforcement.

European Court of Human Rights (2001). Solakov v. the Former Yugoslav Republic of Macedonia, Application No. 47023/99, Judgment of 31 October 2001. https://hudoc.echr.coe.int/eng?i=001-5738.

European Court of Human Rights (2002). Taylor-Sabori v. the United Kingdom, Application No. 47114/99, Judgment of 22 October 2002. https://hudoc.echr.coe.int/eng?i=001-5879.

European Court of Human Rights (2012). El Haski v. Belgium, Application No. 649/08, Judgment of 25 September 2012. https://hudoc.echr.coe.int/eng?i=001-113445.

European Court of Human Rights (2018). Mockutė v. Lithuania, Application No. 66490/09, Judgment of 27 February 2018. https://hudoc.echr.coe.int/eng?i=001-181202.

European Court of Human Rights (2024). Podchasov v. Russia, Application No. 33696/19, Judgment of 13 February 2024.

Europol (2023). Europol. (2023, June 27). Dismantling encrypted criminal EncroChat communications leads to over 6,500 arrests and close to EUR 900 million seized. https://www.europol.europa.eu/media-press/newsroom/news/dismantling-encrypted-criminal-encrochat-communications-leads-to-over-6-500-arrests-and-close-to-eur-900-million-s

Fabbrini, F. and Celeste, E. (2021). EU data protection law between extraterritoriality and sovereignty. In Fabbrini, F., Celeste, E., and Quinn, J., editors, *Data protection beyond borders: Transatlantic perspectives on extraterritoriality and sovereignty*, page 35–58. Hart Publishing.

Forlani, G. (2023). The E-evidence package: The happy ending of a long negotiation saga. *Eucrim*, 2:174–181.

Glen, C. M. (2014). Internet governance: Territorializing cyberspace. *Politics & Policy*, 42(5):635–657.

Guerra, J. E. and Janssens, C. (2019). Legal and practical challenges in the application of the European Investigation Order. *Eucrim: The European Criminal Law Associations' Forum*, 1:46–53.

Heintschel von Heinegg, W. (2012). *Territorial sovereignty and neutrality in cyberspace.* NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE).

Hornkohl, L. (2022). The extraterritorial application of statutes and regulations in EU law. Max Planck Institute Luxembourg for Procedural Law Research Paper Series No. 2022 (1). https://doi.org/10.2139/ssrn.4036688.

Jääskinen, N. (2013). Opinion of Advocate General Jääskinen delivered on 7 February 2013, Bundeswettbewerbsbehörde v. Donau Chemie AG and Others, Case C-536/11, EU:C:2013:67. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62011CC0536.

Kelsen, H. (1952). *Principles of international law.* Rinehart.

Kelsen, H. (1960). Sovereignty and international law. *The Georgetown Law Journal*, 48(4):627–640.

Kordík, M. and Kurilovská, L. (2018). European Investigation Order and the 'Brussels' bureaucracy. *Public Governance, Administration and Finances Law Review*, 3(2):99–109.

Ligori, H. (2015). *Study of the invalidity of acts in the Albanian criminal procedure system (Doctoral dissertation).* Faculty of Law, University of Tirana.

Liivoja, R. (2010). The criminal jurisdiction of states: A theoretical primer. *No Foundations: Journal of Extreme Legal Positivism*, 7:25–58.

Malanczuk, P. (1997). *Akehurst's modern introduction to international law (7th ed.).* Routledge.

Obendiek, A. S. (2022). What are we actually talking about? Conceptualizing data as a governable object in overlapping jurisdictions. International Studies Quarterly, 66(1), sqab080. https://doi.org/10.1093/isq/sqab080.

Ouwerkerk, J. W. (2015). Criminal justice beyond national sovereignty: An alternative perspective on the Europeanisation of criminal law. *European Journal of Crime, Criminal Law and Criminal Justice*, 23(1):11–31.

Payer, A. (2023). The territorial principle as a basis for state criminal jurisdiction: Particularly with regard to cross-border offences and attempts, and to multiple parties to an offence acting in different countries. *International Criminal Law Review*, 23:175–238.

Sieber, U. and Neubert, C.-W. (2017). Transnational criminal investigations in cyberspace: Challenges to national sovereignty. In F. Lachenmann, T. J. Röder, R. Wolfrum, & Max Planck Foundation for

International Peace and the Rule of Law (Eds.), Max Planck Yearbook of United Nations Law (Vol. 20, pp. 241–321). Brill Nijhoff. https://hdl.handle.net/21.11116/0000-0000-807B-5.

Smil, V. (2025). *Creating and transforming the twentieth century (Rev. & expanded ed.)*. Oxford University Press.

Taylor, M. (2015). The EU's human rights obligations in relation to its data protection laws with extraterritorial effect. *International Data Privacy Law*, 5(4):246–256.

Tomasits, R. (2021). The European Investigation Order in criminal matters: Selected issues. *Journal of Criminal Law and Penal Studies*, 25:81–92.

Topalnakos, P. G. (2023). Critical issues in the new EU regulation on electronic evidence in criminal proceedings. *Eucrim*, (2):200–203.

Tosza, S. (2023). Gathering electronic evidence for administrative investigations: Exploring an under-the-radar area. *Eucrim*, (2):216–222.

Tosza, S. (2024). Mutual recognition by private actors in criminal justice? E-evidence regulation and service providers as the new guardians of fundamental rights. *Common Market Law Review*, 61:139–166.

Tzanou, M. (2021). Schrems I and Schrems II: Assessing the case for the extraterritoriality of EU fundamental rights. In Fabbrini, F., Celeste, E., and Quinn, J., editors, *Data protection beyond borders: Transatlantic perspectives on extraterritoriality and sovereignty*, page 97–116. Hart Publishing.

Wu, T. (1997). Cyberspace sovereignty? The Internet and the international system. *Harvard Journal of Law & Technology*, 10(3):647–666.