Journal of Criminology and Criminal Law, 63(3), 7-30
Original Scientific Article
https://doi.org/10.47152/rkkp.63.3.1
UDK: 004.6:343.13(4-6EU)

RECEIVED: 27 October 2025
ACCEPTED: 29 November 2025

EncroChat, Sky ECC and Regulation (EU) 2023/1543: towards a new standards of digital evidence (I)*

Veljko Turanjanin[a]

This paper examines the transformation of digital evidence in European criminal procedure through the lens of Regulation (EU) 2023/1543 on European Production and Preservation Orders. Building on the lessons of the EncroChat and Sky ECC investigations, it analyses how the Regulation redefines the principles of mutual recognition and judicial cooperation in criminal matters, replacing traditional mutual legal assistance with a direct framework linking judicial authorities and private service providers. The study highlights how the new regime introduces harmonised safeguards—necessity, proportionality, and judicial oversight—intended to reconcile investigatory efficiency with fundamental rights protection. Special attention is devoted to questions of transparency, defence rights, and the prospective admissibility of digital evidence under the Regulation's standards. The paper further explores the implications for EU candidate countries, particularly Serbia, emphasizing the need to align domestic procedural law with the Union's digital-evidence framework and to prevent the misuse of the concept of "mutual trust." It concludes that the e-evidence package marks a decisive step toward a coherent, rights-based European model of digital proof and offers a normative blueprint for countries aspiring to integrate into the European Area of Freedom, Security and Justice.

KEYWORDS: EncroChat, Sky ECC, Regulation (EU) 2023/1543, digital evidence.

* This paper was written as part of the EU Criminal Law project, number 101176650 – ECL, funded by the European Union under the Erasmus+ Jean Monnet programme.

[a] Full professor, Faculty of Law, University of Kragujevac.
E-mail: vturanjanin@jura.kg.ac.rs. ORCID: https://orcid.org/0000-0001-9029-0037

Introduction

The digital transformation of crime and policing has profoundly reshaped the landscape of criminal justice in the European Union. The widespread use of digital technologies and online platforms for criminal purposes—often extending beyond classic forms of cybercrime—has created a pressing need for the continuous modernisation and adaptation of tools available to law enforcement and judicial authorities at both national and transnational levels (Sachoulidou, 2024, p. 257). Access to digital evidence has become an indispensable element of timely crime prevention and effective prosecution (Warken, 2017, pp. 290-291).

The exponential growth of digital communication has profoundly reshaped the landscape of criminal investigation and evidence gathering. Online platforms are no longer merely the scene of so-called "cybercrimes," but have become a pervasive infrastructure facilitating a wide spectrum of traditional offences with transnational dimensions. This development has prompted a sustained call for the modernisation and technological adaptation of law enforcement and judicial tools at both the national and European levels (Sachoulidou, 2024, p. 257). Access to electronic data has thus emerged as a central precondition for the timely prevention and effective prosecution of modern criminal activity (Warken, 2017, pp. 290-291).

At the same time, digitalisation and automation have exponentially expanded the capacity of public authorities to collect, classify, and process personal data. What was once a targeted and reactive investigative task has evolved into an ecosystem of data-driven policing (Ferguson, 2017), in which large volumes of information—often collected for non-criminal purposes—are algorithmically cross-referenced to generate predictive insights. While this transformation promises greater investigative efficiency, it also raises pressing questions about purpose limitation, data reuse, and the permissible boundaries of surveillance. The capacity to extract new meaning from aggregated datasets inevitably tests the limits of the rights to privacy and data protection, even for individuals who are not criminal suspects (Molder *et al.*, 2023, p. 513).

Recent EU initiatives on cross-border access to electronic evidence—including the Regulation on European Production and Preservation Orders—have been designed to reconcile these competing imperatives. Their dual objective is to enhance the effectiveness of transnational criminal investigations and to reinforce the protection of fundamental rights within the digital sphere (Sachoulidou, 2024, p. 259). Yet this balance remains fragile. As scholars have observed, penal law is inherently characterised by a tension between efficiency and guarantees: between the public interest in discovering truth and the individual's right to a fair and lawful trial (Kiejnich-Kruk, 2024, p. 127; Turanjanin, 2021). The challenge is particularly acute in the European Union, whose evolving legislative framework must decide whether its primary trajectory is the acceleration of judicial cooperation or the consolidation of procedural safeguards.

Behind the legislative momentum lies a shared concern with the persistent inefficiency of existing mechanisms in addressing both cybercrime and traditional offences, as electronic evidence increasingly supplants material forms of proof (Kiejnich-Kruk, 2024, p. 128). Yet, the reliance on private service providers for evidence production introduces additional risks. Orders for data disclosure may exceed their intended scope, capture inadmissible evidence, or raise conflicts of jurisdiction when the data subject's residence or location is uncertain (Monroy, 2022). These challenges illustrate how the EU's pursuit of operational efficiency in criminal justice is inseparable from deeper questions of sovereignty, accountability, and the rule of law in the digital age.

The accelerated digitalisation of society and advances in information technology have significantly expanded the capacity of police and prosecutorial bodies to collect, store, categorise, and analyse data. While information gathering has long been central to criminal investigations, the rise of automated analytical systems has enabled the emergence of so-called *data-driven policing*, in which vast datasets are processed and cross-referenced through algorithmic tools to generate new investigative leads (Ferguson, 2017). This model, however, raises fundamental questions about the permissible reuse of personal data and the boundaries of algorithmic profiling. Defining those limits and ensuring adequate safeguards for all individuals—whether suspects or not—lies at the core of the rights to privacy and data protection (Molder *et al.*, 2023, p. 513).

Within this evolving environment, the EU's legislative response to cross-border access to digital evidence pursues a dual objective: first, to enhance the efficiency and reliability of criminal investigations and prosecutions—thereby reinforcing security and public trust in the digital single market—and second, to strengthen the protection of fundamental rights for individuals affected by cross-border data-gathering measures (Sachoulidou, 2024, p. 259). Data-driven policing itself is a broad and evolving concept that spans a wide spectrum of technologies and forms part of the wider "big data revolution" transforming multiple sectors, including criminal justice (Molder *et al.*, 2023, p. 514; Davis *et al.*, 2022, p. 186).

An inherent feature of criminal law is its tension between efficiency and procedural guarantees. The enduring dilemma—whether to prioritise effective truth-finding or the protection of individual rights—persists at both national and EU levels. In the European Union context, this tension is reflected in the relationship between the newly adopted Regulation on European Production and Preservation Orders and the fundamental rights of suspects and accused persons (Kiejnich-Kruk, 2024, p. 127). The growing centrality of digital evidence in prosecutions has fuelled frustration with the inefficiency of existing mechanisms for addressing both cyber-specific and traditional offences, where electronic traces increasingly replace material evidence (Kiejnich-Kruk, 2024, p. 128).

Yet significant risks remain that such cross-border orders may extend beyond their intended scope or result in the collection of data inadmissible under national law. Moreover, uncertainties often persist regarding the residence or legal position of the affected individual, which may give rise to conflicts of jurisdiction (Monroy, 2022). The rapid digitalisation of modern life has also created a fragile landscape in which cybersecurity has emerged as a critical concern. The growing dependence on interconnected systems exposes societies to multifaceted risks—from data leaks to tangible harms (Moghior, 2025, p. 92). In light of these developments, the absence of a unified evidentiary standard across Member States underscores the need for coherent, fair, and efficient mechanisms for the cross-border collection of digital evidence. The European Investigation Order (EIO) was initially intended to fill this role, yet subsequent institutional developments—most notably the establishment of the European Public Prosecutor's Office (EPPO) and a series of digitalisation-driven legislative reforms—have prompted the EU to seek new solutions for accessing evidence located in other Member States (Salicius and Molienė, 2024, pp. 208-209).

These conceptual and procedural tensions have been vividly illustrated in practice through high-profile European operations targeting encrypted communication networks. This became particularly evident in two emblematic cases—EncroChat and Sky ECC—which fundamentally reshaped the European debate on lawful interception, privacy, and the admissibility of evidence in the digital age. In both operations, law enforcement authorities across several EU Member States managed to infiltrate encrypted communication networks used predominantly by organised crime groups (Capus and Gilbert, 2024). The EncroChat operation, initiated by French and Dutch authorities in 2020, involved the remote installation of malware on servers and encrypted devices, allowing investigators to access millions of messages exchanged among users who believed their communications to be secure. Similarly, in the Sky ECC case, Belgian, Dutch, and French authorities dismantled another encrypted network in 2021, retrieving vast quantities of data that were subsequently shared with multiple EU jurisdictions. Dutch case-law shows that Article 6 ECHR functioned as a transparency lever: defence challenges compelled courts to disclose key aspects of the collection and processing workflow, while still admitting EncroChat data where reliability was forensically substantiated" (Oerlemans and van Toor, 2022).

While these operations yielded substantial prosecutorial successes—resulting in thousands of arrests and convictions—they simultaneously raised profound normative and procedural concerns. First, the interception and decryption techniques were conducted largely outside any harmonised EU legal framework, relying instead on ad hoc cross-border cooperation and mutual trust between national authorities. Second, the mass nature of the data acquisition blurred the line between targeted surveillance and generalised interception, raising questions under Articles 7 and 8 of the EU Charter of Fundamental Rights and Article 8 of the European Convention on Human Rights concerning privacy and data protection. Third, the absence of transparent judicial oversight and uniform procedural safeguards across Member States created uncertainty about the admissibility and evidentiary reliability of the data collected, as courts across Europe adopted divergent positions on whether the evidence was lawfully obtained.

Ultimately, the EncroChat and Sky ECC investigations underscored the urgent need for a coherent European regulatory framework governing cross-border access to digital evidence. They exposed the fragmentation of procedural safeguards, the tension between investigative efficiency and fundamental rights, and the inadequacy of existing instruments such as the European Investigation Order. Against this background, the adoption of Regulation (EU) 2023/1543 on European Production and Preservation Orders represents not only a legislative innovation but also an institutional attempt to reconcile the competing imperatives of security, efficiency, and fundamental-rights protection in the age of digital surveillance—a balance that remains at the heart of the EU's evolving criminal-justice architecture.

EncroChat and Sky ECC in European Case-Law

Factual Background of Sky ECC

Sky ECC was a subscription-based encrypted-messaging ecosystem operated by the Canadian company Sky Global. It combined modified devices—typically BlackBerry or Nokia handsets with cameras, microphones, and GPS disabled—with an end-to-end encrypted platform featuring timed deletion and "panic" wipes. The system was marketed at premium prices through a multilayer reseller network (Škulić, 2024, pp. 5-7). By early 2021, *Sky ECC* had a large user base concentrated around major European logistics hubs such as Rotterdam and Antwerp and was widely adopted by organised-crime groups for drug trafficking, money laundering, and violent offences. In March 2021 the infrastructure was disrupted and the service shut down, yet law-enforcement authorities retained access to "hundreds of millions" of historical encrypted messages, which continue to inform investigations across the EU (Europol, *Operation Sky ECC*). The transnational response was coordinated through Europol's *Operational Task Force LIMIT*, with Belgium, France, and the Netherlands as core partners and support from Eurojust, Frontex, INTERPOL, OLAF, EUIPO, and WADA.

Open-source reconstructions based on French case materials illustrate how the *Sky ECC* "universe" functioned in practice, documenting reseller tiers, handset provisioning, and the evidentiary value of decrypted chat logs and audio notes across multiple jurisdictions, including the Balkans (OCCRP, 2024). Serbian media and academic commentary likewise report that domestic prosecutions obtained *Sky ECC* data via mutual legal assistance (MLA) from France, coordinated by Europol, while defence teams systematically challenge admissibility and reliability owing to the secrecy of decryption methods and restricted access to technical files (Insajder, 8 Nov 2022/19 Apr 2024; Škulić, 2024; Sagittae, 2023; Bajović and Ćorić, 2025; Bajović, 2022).

The question of whether and to what extent a national court should verify the lawfulness of evidence obtained abroad lies at the heart of cross-border cooperation in criminal matters. As Steinborn and Święczkowski (2023) note, the European Investigation Order (EIO) mechanism requires the issuing state to ensure that evidence gathered in another Member State meets minimum procedural guarantees before it can serve as a basis for judgment. This approach complements the principle of *mutual trust* but simultaneously highlights the need for verification safeguards when evidence—such as EncroChat or SKY ECC communications—is obtained through technologically complex or covert means.

Courts across Europe are now seized of cases in which *Sky ECC* communications constitute central inculpatory material. Recurrent defence arguments concern: (i) the lawfulness of initial access (infrastructure hacking vs. provider requests); (ii) chain of custody and forensic integrity; (iii) scope-creep and proportionality (mass acquisition → targeted use); (iv) fair-trial equality of arms given classification of technical methods; and (v) cross-border admissibility (MLA/EIO vs. direct cooperation), often linked to forum-shopping concerns.

Some jurisdictions—e.g. Italy's *Corte di Cassazione*—have required greater disclosure of collection methods, whereas others have admitted *Sky ECC* evidence when corroborated by independent proof (Insajder; Škulić, 2024; see futher Buric *et al.*, 2023). A central unresolved issue in both *EncroChat* and *Sky ECC* proceedings concerns the defence's right of access to potentially exculpatory communications and technical files. Dutch practice is often cited as emerging best practice: in *Sky ECC*-related trials, the defence was granted access through the same forensic platform used by police authorities, enhancing equality of arms and the right to a fair trial (Lasagni, Caianiello and Rezende, 2025, p. 445). Transparency in how communications were intercepted and decrypted is not only procedural hygiene but a substantive requirement for assessing legality, proportionality, and the lawful issuance of European Investigation Orders (EIOs) under Article 6 of Directive 2014/41/EU.

The judgment of the Belgrade Appellate Court (Kž1 Po1 38/24, 11 July 2025) represents the first clearly articulated position of Serbian judicial practice regarding the admissibility of evidence obtained through the SKY ECC platform. In this case, the court upheld the legality of using communication data transmitted by the French authorities in response to a mutual legal assistance (MLA) request submitted by the Serbian Office of the Prosecutor for Organised Crime. The court emphasised that MLA constitutes the only legitimate channel for the exchange of evidence between sovereign states and that a relationship of mutual trust exists between them. In doing so, the judgment implicitly aligned itself with the *mutual trust* principle in EU law, stressing that it is not necessary for evidence to be obtained in accordance with domestic procedural rules, but rather that it must comply with the law of the requested state and relevant international treaties—such as the 1959 European Convention on Mutual Assistance in Criminal Matters and the 2000 UN Convention against Transnational Organized Crime. Furthermore, the court found that the collection and use of Sky ECC data did not amount to a disproportionate interference with the right to privacy under Article 8 ECHR, given the limited, encrypted nature of the platform and the legitimate aim of combating organised crime. This reasoning effectively bridges Serbian judicial practice with emerging European standards on digital evidence and cross-border data admissibility.

The Supreme Court of Montenegro, in its decision of 10 July 2025, confirmed the finality of the appellate judgment, thereby indirectly affirming the admissibility of Sky ECC evidence used in proceedings for organised crime and drug trafficking. Although the ruling focused procedurally on the inadmissibility of a third-instance appeal, its effect was to uphold the lower courts' reasoning and evidentiary assessments, including the reliance on Sky ECC communications transmitted via international judicial cooperation channels. Taken together with the jurisprudence of the Serbian courts, the Montenegrin case illustrates a converging regional trend: national judiciaries are increasingly recognising the evidentiary validity of encrypted communication data obtained abroad through mutual legal assistance mechanisms. This alignment mirrors the broader European movement toward harmonised standards for digital evidence collection and admissibility, as envisaged in Regulation (EU) 2023/1543.

AI-Assisted Investigations and Mutual Recognition

The fast-moving digitalisation of law-enforcement practice has transformed both the scale and nature of evidence gathering. As Sachoulidou (2024, p. 257) notes, the increasing reliance on electronic data has created a constant "modernisation imperative" for investigative authorities. Access to digital data is now integral to the timely prevention and prosecution of crime (Warken, 2017, pp. 290-291). Modern technology enables police to collect, store, and analyse massive datasets, fuelling what Ferguson (2017) termed *data-driven policing*. Yet such practices raise deep normative questions about secondary use and re-use of personal data (Molder *et al.*, 2023, p. 513). As Kiejnich-Kruk (2024, p. 127) observes, EU criminal procedure perpetually oscillates between efficiency and guarantees—a tension magnified by digital investigations.

Between April and June 2020, French authorities captured over 120 million messages from roughly 60,000 EncroChat devices within a JIT with the Netherlands and Europol, with the dataset subsequently feeding hundreds of prosecutions, including over 200 judgments in the Netherlands within two years (Oerlemans and van Toor, 2022). The EncroChat and Sky ECC operations epitomise this duality. In 2020, French and Dutch authorities—supported by Eurojust and Europol—dismantled the EncroChat encrypted network. Operating as a parallel Android system, EncroChat provided enhanced anonymity, with hardware modifications disabling cameras, microphones, and GPS, and a software "panic" function allowing remote data erasure. Its widespread adoption by organised-crime networks led to the creation of a Joint Investigation Team (JIT) between France and the Netherlands. Acting under judicial authorisation, investigators infiltrated the system, captured encrypted messages for months, and later distributed hundreds of thousands of decrypted messages via EIOs. When EncroChat collapsed, criminals migrated to Sky ECC. France, Belgium, and the Netherlands—again via a JIT—used targeted hacking, cryptanalytic tooling, and large-scale digital-forensic analysis to intercept more than one billion messages. The data were shared through EIOs, sparking extensive litigation. Defence challenges focused on the opacity of algorithmic tools and the limited disclosure of datasets. Typically, only filtered "tertiary" (derived) data reached the defence, while raw and intermediate datasets remained inaccessible. This asymmetry—especially for States receiving data via EIOs rather than as JIT members—raised equality-of-arms and algorithmic-accountability concerns (Lasagni and Contissa, 2025, pp. 19-22).

The structural flaw lies in the EIO Directive itself. Article 1(1) permits the use of EIOs for "evidence already in possession" of executing authorities—a clause designed for static documents, not for dynamic, algorithmically filtered bulk data. When evidentiary selection occurs abroad, defendants cannot influence the criteria guiding automated extraction. Consequently, the principle of mutual recognition risks replacing procedural participation with institutional trust, leaving unresolved whether such trust can substitute for effective defence rights.

As Galič, Stevens and Koops (2023) observe, the ongoing shift from targeted, *case-seeks-evidence* investigations toward data-driven, *evidence-seeks-case* policing exposes a normative gap between criminal procedure law and data-protection law. The resulting asymmetry—strong rules on data collection but weak regulation of subsequent data analysis—complicates judicial oversight of large-scale interception operations such as EncroChat and Sky ECC and underscores the need for integrated safeguards across the entire data-processing cycle.

The Grand Chamber's Judgment in M.N. (EncroChat) and ECtHR Jurisprudence

The CJEU's Grand Chamber judgment in *M.N. (EncroChat)* (C-670/22, 30 April 2024, EU:C:2024:372) delineates a crucial doctrinal boundary between collection and transmission of electronic evidence under Directive 2014/41/EU. Where an EIO seeks only the transfer of evidence already held by executing authorities, issuance may lie with a public prosecutor rather than a judge, provided domestic law would authorise the same in an analogous internal case (Arts 1(1), 2(c), 6(1)).

The proportionality test remains anchored in the issuing State's law; individualised suspicion for each affected user is not an EU-law requirement at the transmission stage. Lawfulness of collection in the executing State cannot be re-litigated—reflecting mutual trust—but the issuing authority must ensure domestic safeguards and fair-trial rights.

Two findings are pivotal. First, device infiltration used to obtain content, traffic, or location data qualifies as "interception of telecommunications" (Art. 31), triggering a duty to notify the Member State where the target is located, preserving both sovereignty and user protection. Second, under Art. 14(7), national courts must exclude evidence the accused cannot effectively contest if it may decisively influence findings—an equality-of-arms guarantee especially relevant when collection methods are classified.

This framework preserves the executing State's primacy over collection-lawfulness review while ensuring that transmission and trial use remain bound by issuing-State law and EU fair-trial guarantees. As Salicius and Moliene (2024, pp. 208-215) observe, the EIO embodies the principle *forum regit actum*, allowing evidence to be gathered under the procedural law of the requesting State, replacing the earlier *locum regit actum* model (Kusak, 2019, p. 391). Yet digitalisation challenges this balance: the "liquidity" of electronic evidence renders classical EIO procedures too slow, prompting new instruments—the European Production and Preservation Orders. Although transposition of the EIO Directive proceeded smoothly, divergences in prosecutorial powers persist (Catanzariti, 2025, pp. 454, 473; Lasagni, Caianiello and Rezende, 2025, p. 439).

The ECtHR has simultaneously refined its approach to digital evidence implicating Articles 8 and 6 ECHR. *Big Brother Watch and Others v. United Kingdom* and *Centrum för Rättvisa v. Sweden* laid the foundations for surveillance oversight; later judgments tackled the downstream use of lawfully intercepted data. In *Akgün v. Turkey* (2021) the Court held that conviction based on ByLock-app data without independent verification violated fair-trial guarantees, underscoring transparency and defence access.

A more nuanced analysis appeared in *Ships Waste Oil Collector B.V. and Others v. the Netherlands* ([GC], nos. 2799/16 *et al.*, 1 Apr 2025). The Grand Chamber acknowledged that onward transmission of intercepted data from criminal to administrative proceedings constitutes a separate interference with Article 8 rights but found no violation, given sufficient domestic safeguards. The Court articulated four minimum standards: collection must be Convention-compliant; circumstances for transmission must be clearly set out in law; rules must govern examination, storage, use, onward transfer, and destruction; and independent judicial review must be ensured.

While prior judicial authorisation is not indispensable, robust ex post review is mandatory. The Court accepted secrecy during ongoing investigations and viewed effective competition-law enforcement as a legitimate aim under Art. 8(2). This jurisprudence shifts the focus toward the life-cycle of digital evidence—from collection through secondary use—and reaffirms that legality, proportionality, and oversight remain indispensable throughout.

In *Ships Waste Oil Collector B.V.*, the Grand Chamber explicitly referenced CJEU case-law, signalling a convergence between Strasbourg and Luxembourg. In *Lietuvos Respublikos generalinė prokuratūra* (C-162/22, 7 Sept 2023, EU:C:2023:631), the CJEU ruled that data retained for serious-crime investigations cannot be reused for lesser purposes such as disciplinary proceedings, because Article 15(1) of the ePrivacy Directive enumerates permissible aims exhaustively and hierarchically (paras. 34–44). Combined with *M.N. (EncroChat)*, this establishes the EU's purpose-limitation principle, ensuring data are not repurposed beyond their authorised scope. The ECtHR's proportionality analysis under Article 8 ECHR complements this standard, both courts insisting on independent judicial control at every stage.

Taken together—*Lietuvos Respublikos generalinė prokuratūra*, *M.N. (EncroChat)*, *Akgün v. Turkey*, and *Ships Waste Oil Collector B.V.*—a European evidentiary paradigm emerges: the CJEU emphasises competence, proportionality, and purpose limitation; the ECtHR guarantees fairness, transparency, and privacy; and their mutual reinforcement is producing a transnational evidentiary model that balances effective law enforcement with fundamental-rights protection. In this sense, *EncroChat* and *Sky ECC* transcend their operational origins—they have become catalysts for a pan-European judicial dialogue redefining the boundaries of mutual recognition, digital sovereignty, and algorithmic accountability in criminal justice.

Challenges of the Current Framework

The transfer and admissibility of evidence in criminal proceedings constitute one of the central issues of modern criminal procedure law. This is particularly evident in transnational cases, where evidence collection necessarily entails some restriction of the rights of the accused, raising the question of how to balance procedural efficiency with the protection of human rights. One of the most significant legal instruments in this field is the European Investigation Order (EIO), introduced by Directive 2014/41/EU of 3 April 2014, adopted on the basis of Article 82(1)(a) of the Treaty on the Functioning of the European Union (Ruggeri, 2014, p. 4; Vervaele, 2005; Vogler, 2014, p. 45; Allegrezza, 2014, p. 52; Dediu, 2018, p. 300). The initiative for the Directive originated in 2010 from eight Member States, aiming to replace the fragmented legal instruments previously governing the cross-border transfer of evidence within the EU—most notably, Framework Decision 2003/577/JHA and Framework Decision 2008/978/JHA. The Directive thus established a unified and coherent mechanism for evidence gathering—its first and most evident advantage.

The EIO is defined as a judicial decision issued or validated by a judicial authority of one Member State (the issuing State) with a view to carrying out one or more investigative measures in another Member State (the executing State) for the purpose of obtaining evidence. In addition to prospective investigative acts, the EIO may also be issued for the transfer of evidence already in possession of the executing authorities. Member States are obliged to recognise and execute an EIO on the basis of the principle of mutual recognition (Zimmerman, Glaser and Motz, 2011, p. 56; Heard and Mansell, 2011, p. 354; Belfiore, 2014, p. 93; Szilvia, 2011, p. 39; Ivanović and Ivanović, 2015, p. 210).

The concept of an issuing authority is defined broadly: it may include a court, a judge, an investigating judge, a public prosecutor, or any other competent authority acting as an investigative body in a given case. Before transmitting an order, the issuing authority—typically a judge or prosecutor—must verify its compliance with the conditions laid down in the Directive. The executing authority is responsible for recognising and enforcing the order, and in some national systems, judicial authorisation is additionally required. Although investigative measures are in practice often implemented by the police, the Directive expressly insists on the preservation of the judicial role in the chain of decision-making.

The EIO covers all investigative measures, except for the establishment of Joint Investigation Teams (JITs), which are governed by separate instruments. It may be issued in a variety of procedural contexts: in criminal proceedings conducted before judicial authorities; in administrative proceedings that may result in a judicial decision in criminal matters; and in proceedings concerning the liability of legal persons. The Directive also introduces a standardised form, containing information on the issuing and validating authorities, the person concerned, a description of the criminal offence and applicable legal provisions, as well as details regarding the requested measures and evidence.

The key conditions for issuing an EIO are set out in Article 6 of the Directive. The issuing authority may make an order only if two cumulative requirements are met: the measure is necessary and proportionate to the purpose of the proceedings, taking into account the rights of the suspect or accused; and the same measure could have been taken in a similar domestic case under national law. If the executing authority believes that these conditions are not satisfied, it may request clarification or even question the execution of the order. In such cases, the issuing authority may decide to withdraw the EIO. The EIO must be transmitted to the executing authority by any means capable of producing a written record and verifying its authenticity, including through the European Judicial Network's secure communication systems. If the authority receiving the order lacks competence, it must forward it to the competent authority and notify the issuing authority accordingly.

The EIO was thus designed to reduce the duration of cross-border investigations and increase their efficiency. Yet many scholars emphasise that procedural acceleration must not come at the expense of the rule of law and the protection of fundamental rights (Farries, 2010, p. 432; Mirisan, 2018, p. 225; Ruggeri, 2014, p. 225; Armada, 2015, pp. 8-9). Issues such as conflicts of jurisdiction, forum shopping, and the respect for defence rights remain central challenges in the practical application of the EIO.

The executing authority is obliged to recognise an EIO without further formalities and to execute it under the same conditions as if the investigative measure had been ordered by a domestic authority. Exceptions exist only where grounds for non-recognition, non-execution, or postponement explicitly provided in the Directive apply. During execution, the executing authority must respect the formalities and procedures indicated by the issuing authority, unless these would be contrary to the fundamental principles of the executing State's legal system. Finally, the issuing authority may request that its representatives be present in the executing State to assist in the execution of the order, provided this occurs in accordance with the domestic law of the executing State and without any powers of criminal prosecution. Such officials are subject to the laws of the host State for the duration of their presence.

The rapid digitalization of modern society has profoundly transformed the operational environment of criminal justice. As technological dependence deepens, cybersecurity vulnerabilities and data-driven criminality have become systemic risks, exposing gaps in traditional procedural frameworks (Moghior, 2025, p. 92). While the European Investigation Order (EIO) was conceived as a comprehensive response to such challenges, the accelerating pace of digitization continues to test its adaptability.

One of the principal obstacles lies in the absence of a unified evidentiary standard across Member States. National systems differ considerably in defining, gathering, and admitting evidence—disparities that become particularly visible in cross-border digital investigations. The EIO was intended to offer a single, harmonised mechanism for obtaining evidence across jurisdictions (Salicius and Moliene, 2024, pp. 208-210), yet the emergence of new institutions such as the European Public Prosecutor's Office (EPPO) and the adoption of digital-evidence-specific legislation have progressively diversified the investigative landscape. These developments compel the EU legislator to explore alternative pathways for accessing evidence located in another Member State, thereby diluting the EIO's original unifying purpose (Salicius and Moliene, 2024, pp. 209-211).

A key procedural innovation of the EIO is its endorsement of the forum regit actum principle—meaning that the requested investigative measure should be executed in accordance with the formalities and procedures specified by the issuing State. This approach replaced the earlier locus regit actum principle under the pre-existing conventions, which tied evidentiary procedures to the State where the evidence was physically located (Salicius and Moliene, 2024, p. 211; Kusak, 2019, p. 391). The shift reflected a conceptual move toward recognising the functional sovereignty of the requesting authority and aimed to strengthen mutual trust as the cornerstone of EU judicial cooperation.

Nonetheless, digital evidence has revealed the practical limits of this model. The liquid and transient nature of electronic data—constantly shifting across servers and jurisdictions—renders the conventional EIO procedure often too slow for effective use (Salicius and Moliene, 2024, p. 215). For this reason, the recent "electronic evidence package," comprising the European Production and Preservation Orders, does not replace the EIO but rather supplements it with a faster, direct-access mechanism specifically tailored for the volatile context of digital data.

The distinctive evidentiary character of electronic content further complicates procedural harmonisation. Such data constitute a rich but unstable source of probative information whose collection raises acute questions about privacy, admissibility, and reliability. Member States apply divergent approaches to their acquisition and use, producing a fragmented regulatory environment that undermines mutual recognition (Kusak, 2024). To address these divergences, recent scholarship argues for the development of EU-level minimum standards governing electronic content data, coupled with a presumption of admissibility for evidence gathered in conformity with those standards. Instead of harmonising specific investigative techniques, this model would operate on the level of data categories, ensuring that any measure targeting electronic content meets uniform EU safeguards (Kusak, 2024).

From an institutional perspective, the field of judicial cooperation remains broad and multi-layered, encompassing both police and judicial actors and covering areas of increasingly overlapping competences (Catanzariti, 2025, p. 454). Against this backdrop, the EIO Directive represents a landmark codification—a single framework intended to simplify and accelerate cross-border investigations by replacing traditional mutual legal-assistance mechanisms (Catanzariti, 2025, p. 473).

Empirical assessments indicate that the transposition and implementation of Directive 2014/41/EU have, overall, been smooth. By 2018, all Member States had amended their domestic legislation to comply with the Directive's requirements, and major systemic difficulties have not been reported (Lasagni, Caianiello and Rezende, 2025, p. 439). Nonetheless, isolated critiques—such as those directed at Germany's transposition for insufficient emphasis on mutual trust and judicial reciprocity—demonstrate that the practical success of the EIO depends less on formal compliance and more on the depth of normative alignment among national legal cultures.

While the Directive sets out a unified procedural framework, its practical effectiveness depends on the range and regulation of investigative measures available under domestic law. Although in practice it often happens that a specific investigative measure requested through an EIO does not exist in the domestic legislation of the executing State, the Directive nonetheless prescribes a minimum set of measures that the executing authority must be able to provide. These include: obtaining already existing information and evidence in the possession of public authorities; access to police and judicial databases; questioning of witnesses, victims, experts, or suspects; so-called *non-coercive measures*; and identification of users of a telephone number or IP address. An alternative measure may be applied if it achieves the same result with less intrusiveness, but only after informing the issuing authority. Where a requested measure does not exist under domestic law and no adequate alternative can be provided, the executing authority must notify the issuing authority that execution is not possible. In practice, such cases raise defence-right concerns, particularly regarding the examination of witnesses in light of the ECtHR's jurisprudence on fair-trial guarantees.

Articles 22–31 of Directive 2014/41/EU establish a special regime for certain investigative measures which, due to their nature and degree of interference with individual rights and freedoms, require more detailed regulation. These include measures involving the physical presence of persons (e.g. temporary transfer of detained individuals), the use of modern technological means (e.g. videoconferencing), access to sensitive financial information (e.g. bank account data), and those that most profoundly interfere with privacy (e.g. interception of communications). The detailed regulation of these measures aims to ensure both the efficiency of criminal proceedings and the proportionality and protection of fundamental rights of the individuals concerned. Among these, communication surveillance occupies a particularly sensitive position. This evidentiary measure directly engages the right to privacy under Article 8 of the European Convention on Human Rights (Turanjanin, 2021, pp. 34-60). It is also one of the most costly investigative measures, and during the drafting of the Directive, proposals were made to introduce a specific ground for refusal of an EIO based on the excessive costs of its execution (Arasi, 2014, p. 133).

An EIO may be issued for the interception of telecommunications in a Member State from which technical assistance is required. Where several Member States are able to provide full technical support for the same interception, the order shall be addressed to only one of them—preferably the State where the interception subject is located or will be located. The order must include information necessary to identify the subject of interception, the duration of the interception, and sufficient technical details for its implementation. The issuing authority must also justify why this measure is essential for the criminal proceedings. Execution may be refused not only on general grounds but also if the investigative measure would not be authorised in a comparable domestic case. The executing State may further condition its consent on the fulfilment of any domestic legal requirements.

The EIO for interception may be executed in two ways: through direct transmission of the intercepted communication to the issuing State, or by recording and subsequently transmitting the results to the issuing State. The issuing and executing authorities are expected to consult each other regarding the practical arrangements for carrying out the interception. Additionally, during issuance or execution, the issuing authority may—where justified—request a transcript, decoding, or decryption of the data, which remains subject to the executing authority's consent (Article 30, Directive 2014/41/EU).

When a competent authority of one Member State ("the intercepting State") authorises the interception of telecommunications, and the communication address of the interception subject is being used on the territory of another Member State ("the notified State") whose technical assistance is not required, the intercepting State must notify the competent authority of the notified State. Notification must occur: before interception, if the intercepting State knows at the time of issuing the order that the subject is or will be located in the notified State; or during or after interception, as soon as it becomes known that the subject is or was located in the territory of the notified State. A standardised form is prescribed for such notification. However, the notified State may, if the interception would not have been authorised in a comparable domestic case, inform the intercepting State within 96 hours of receiving the notification that the interception must not be carried out or must be discontinued. The notified State may also stipulate that any material intercepted while the subject was within its territory may not be used, or may only be used under specified conditions (Article 31, Directive 2014/41/EU).

In essence, the special investigative measures regulated by Directive 2014/41/EU illustrate the delicate balance between the efficiency of criminal prosecution and the protection of fundamental rights. Whether involving the temporary transfer of detained persons, technologically assisted hearings, access to financial data, or the interception of communications, all such measures raise questions of proportionality, procedural guarantees, and mutual trust among Member States. Their practical implementation largely depends on the judicial culture and institutional capacity of each State, often leading to uneven application in practice. Consequently, these measures represent the most sensitive dimension of the European Investigation Order—one that most clearly exposes both its efficiency advantages and its human-rights vulnerabilities.

Beyond traditional evidentiary tools, the rise of digital technologies has introduced a new category of cross-border evidence that tests the limits of the EIO's procedural design. The European Investigation Order (EIO) is one of the central instruments of judicial cooperation in criminal matters within the European Union. It was designed to facilitate rapid, efficient, and standardised gathering of evidence from other Member States without the delays associated with traditional mutual legal assistance procedures. The EIO is particularly significant in the context of digital evidence, as modern criminal investigations increasingly rely on electronic data such as emails, metadata, cloud-stored content, or app-based communications. However, despite its normative value, practice has revealed numerous challenges in its implementation.

First, although the EIO operates within the EU, digital evidence is frequently stored outside the Union's territory. Many major service providers (e.g. Google, Meta, Microsoft) host data on servers located in third countries, most commonly in the United States or Ireland. In such situations, investigative authorities must combine the EIO with mutual legal assistance (MLA) instruments, which significantly slows down the process. This difficulty becomes especially acute when dealing with real-time data or volatile content that can be quickly altered or deleted—contexts in which speed of execution is crucial. Second, divergences in national legislation among Member States add another layer of complexity. In some jurisdictions, public prosecutors are authorised to issue orders for the collection of electronic evidence, whereas in others, such powers are reserved exclusively for the judiciary. These differences create legal uncertainty and lead to practical delays, as executing States often require judicial confirmation even where, under the law of the issuing State, a prosecutor could have issued the order. Comparative analyses show that this "lowest common denominator" approach may in practice reduce the efficiency of the EIO mechanism.

Third, the collection of digital evidence inevitably entails restrictions on fundamental rights, particularly the right to privacy guaranteed by Article 8 of the European Convention on Human Rights (ECHR) and the rights to privacy and data protection under Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. Consequently, every measure taken under an EIO must pass a strict necessity and proportionality test. The experience of Member States demonstrates that courts frequently have to balance investigative needs with the protection of individual rights, introducing further legal and ethical dilemmas into the process. Fourth, although Directive 2014/41/EU formally covers electronic data, its provisions have proven insufficient for the swift and effective acquisition of digital evidence in practice. This shortcoming prompted the adoption of Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023, establishing the European Production Order and the European Preservation Order. This Regulation aims to create a direct and uniform mechanism for obtaining digital data from service providers across the EU, thereby overcoming the limitations of the EIO in this domain. As a directly applicable legal instrument, it enhances legal certainty and harmonisation of practice, ensuring that uniform rules apply throughout all Member States without the need for national transposition.

Regulation (EU) 2023/1543 on E-Evidence

Digital Evidence in the European Criminal Justice Context

Beginning in 2013, EU agencies and other institutions started issuing a series of guidelines concerning the handling and use of electronic evidence (Buono, 2019). Despite this growing institutional attention, there is still no universally accepted definition of digital evidence, and various understandings of the concept can be found across the literature. Since there is no universally accepted definition of *digital evidence*, various understandings of this concept can be found throughout the literature. Primarily, *digital evidence* is a term often used synonymously with *electronic computer evidence*. It is generally considered a form of evidence that differs from other material evidence by the format in which information is embedded — the *digital form* — which involves some kind of electronic or magnetic device and manifests as a sequence of ones and zeros that can be translated into a human-readable form through an electronic device (Lukić, 2012, p. 182).

Alternatively, digital evidence may be defined as any *electronic data capable of establishing a significant link between the perpetrator of a criminal offence and the victim* (Pladna, 2025, p. 3), or as *information of evidential value that is stored, transmitted, or retrieved in binary form* (Leacock, 2008, p. 221). It may also be understood as *any data stored or transmitted by computer systems that support or contradict a theory of how an offence occurred, or that address critical elements of the crime such as intent or alibi* (Hamidović, 2011, p. 362). Another approach defines digital evidence as *any information, regardless of human intervention, that can be extracted from a computer and must be in a format readable or interpretable by experts* (Ghosh, 2004, p. 9). In a broader sense, the term can be understood as *any information of probative value stored or transmitted in digital form*, implying that digital evidence encompasses data stored on, processed through, or retrieved from computers or other electronic devices such as audio, video, communication, or photographic equipment (Chaikin, 2006, pp. 240-241). Ultimately, the concept of digital evidence may be used to denote *the establishment of proof of misuse within systems employing digital technology in the broadest sense of the term* — that is, *any information in digital form that has evidential value and is either stored or transmitted in that format*.

Internationally recognised standards play a particularly significant role in the handling of digital evidence, as they ensure its authenticity, integrity, and admissibility in criminal proceedings. ISO/IEC standards 27037, 27041, 27042, and 27043 provide comprehensive guidelines for the identification, collection, acquisition, preservation, analysis, and interpretation of digital evidence, as well as for the overall process of digital investigation. In addition, the International Organization on Computer Evidence (IOCE) has adopted fundamental principles of digital forensics, insisting on the preservation of original data, the documentation of all procedural steps, and the regular updating of procedures. The Scientific Working Group on Digital Evidence (SWGDE) develops practical guidelines for handling different types of digital evidence, such as mobile phones, cloud systems, and CCTV recordings. The implementation of these standards in practice not only guarantees the reliability of digital evidence but also safeguards the procedural rights of the parties, in accordance with Article 6 of the European Convention on Human Rights (Britz, 2004, p. 157).

On this basis, *digital evidence* may be defined as any information in electronic or digital form that possesses evidentiary value in criminal proceedings, which is stored, processed, or transmitted through a computer or other electronic device and may be used as proof in accordance with law and international standards. This category encompasses a wide range of content: emails and attachments, data from messaging applications (such as Viber, WhatsApp, Signal, and Telegram), cloud files, metadata accompanying communications (IP addresses, MAC addresses, logs), geolocation data, content and interactions from social media platforms (Facebook, Instagram, TikTok), as well as digital photographs and video recordings. In both theory and practice, a distinction is commonly drawn between *content data* (e.g., the text of a message), *metadata* (e.g., time of sending, sender's IP address), and *transactional data* (e.g., information about cryptocurrency payments).

The importance of digital evidence in contemporary criminal proceedings continues to grow. In cases involving cross-border criminality—such as cybercrime, organised crime, and terrorism—digital evidence often constitutes the only material enabling the identification and prosecution of perpetrators. Its distinctive feature lies in the fact that it leaves traces invisible in the physical world, yet capable of reconstructing the entire sequence of criminal events. The concept of the *digital footprint* encapsulates the idea that nearly every human activity—from making a phone call to browsing the internet—leaves an electronic record that may hold evidential value. However, digital evidence also poses a number of challenges. First, its immaterial and easily alterable nature raises questions of authenticity and integrity. Forensic methods such as the calculation of hash values thus become crucial for demonstrating that data have not been tampered with. Second, digital evidence is frequently stored on servers located outside the territory of the state conducting the proceedings, creating complex issues of jurisdiction and the need for cross-border cooperation. Third, obtaining such data necessarily interferes with the right to privacy and data protection, as guaranteed by Article 8 of the European Convention on Human Rights and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. Therefore, the collection of digital evidence must always be subjected to a strict test of necessity and proportionality.

Scholars have long recognised that digital evidence has *"changed the paradigm"* of criminal proceedings. It not only expands the range of evidentiary means but also transforms the very concept of proof, as it often has the potential to reconstruct a criminal act objectively and conclusively. Yet, this potential can only be realised if procedural guarantees are respected—particularly the rights of the defence and the principle of equality of arms.

At the European level, the growing importance of digital evidence initially became apparent through the practices of national investigative authorities and within the implementation of the European Investigation Order (EIO). However, the increasing reliance of criminal investigations on data held by private service providers soon exposed the limitations of existing mutual legal assistance mechanisms. This development ultimately prompted the adoption of Regulation (EU) 2023/1543 on European Production and Preservation Orders for electronic evidence, intended to facilitate direct access to such data across borders while preserving essential procedural safeguards and fundamental rights (Signorato, 2023, p. 10). In contemporary criminal proceedings, digital—or electronic—evidence encompasses any probative information stored or transmitted in digital form. The omnipresence of information and communication technologies (ICT) means that cross-border collection of such data frequently arises during investigations. For instance, photographs, messages, or documents relevant to a case may be stored on servers or devices physically located abroad. According to the European Commission, digital evidence is required in approximately 85 per cent of criminal investigations, and nearly two-thirds of such data are held by service providers established outside the investigating Member State (European Commission, 2024).

Background and Rationale

As Juszczak and Sason (2023) explain, the adoption of the e-evidence package marks a pivotal stage in the development of the European Area of Freedom, Security and Justice. Embedded in the EU's broader security architecture, the initiative seeks to reconcile two imperatives: protecting individuals from the misuse of digital technologies and enabling judicial and law enforcement authorities to access electronic evidence across borders "in a swift and legally sound manner" (Juszczak and Sason, 2023, p. 182). The package—comprising Regulation (EU) 2023/1543 and Directive (EU) 2023/1544—modernises the investigative framework in response to lessons drawn from the 2016 terrorist attacks and subsequent Council conclusions on improving criminal justice in cyberspace. Prevention, detection, and enforcement were identified as interdependent pillars of EU internal security, with electronic evidence positioned at the core of this triad. As Forlani (2023) further observes, the e-evidence package was the outcome of a lengthy and politically delicate negotiation process that pushed the principles of mutual trust and mutual recognition to their limits. The negotiations, initiated with the Commission's 2018 proposals, centred on striking a balance between investigative efficiency and the protection of privacy and defence rights. The most contentious issue concerned the degree of involvement of judicial authorities in the Member State where a service provider is located in verifying and executing cross-border orders. This "e-evidence scenario," as Forlani terms it, departed from traditional models of judicial cooperation based on territoriality and letters rogatory, replacing them with a direct procedural link between investigating authorities and private service providers. The final compromise reached in 2023 thus embodies a cautious equilibrium—enhanced procedural efficiency combined with a strengthened framework of fundamental rights safeguards.

The beginning of the twenty-first century was marked by the intensive normative activity of the European Union in the field of criminal law, through the adoption of directives and framework decisions, complemented by the rapid development of the case law of the Court of Justice of the European Union (Mitsilegas, 2007). At the same time, the Western Balkan states, as candidates or potential candidates for EU membership, developed their own regimes of mutual legal assistance in criminal matters (Klip, 2016; Plešničar and Šugman Stubbs, 2009).

The traditional mechanism of mutual legal assistance proved to be slow and ineffective, thereby opening the way for a more radical concept in the EU—the mutual recognition of foreign judicial decisions. Since the early 2000s, this principle has become the "cornerstone" of judicial cooperation, with the European Arrest Warrant as its most prominent instrument (Christou, Kouzoupi and Xanthaki, 2009; Klimek, 2015, 2017). The principle of mutual recognition, developed as early as the Cassis de Dijon case (1979), served as the basis for overcoming the difficulties of harmonizing diverse national legislations (Diez, 2015). Its four key functions—legislative, interpretative, optimizing, and balancing—enabled it to become a flexible instrument of European legal integration (Suominen, 2014).

From this same logic emerged the further development of instruments in the field of digital evidence. If the European Arrest Warrant represented the paradigm of mutual recognition in the area of deprivation of liberty, the new Regulation (EU) 2023/1543 aspires to become its counterpart in the field of obtaining and preserving electronic evidence. Its essential role is to replace the traditional mechanisms of mutual legal assistance (marked by slowness, complexity, and the risk of forum shopping) with a more efficient regime that directly binds service providers and introduces explicit safeguards for the protection of fundamental rights.

A central part of the Regulation is found in recitals 10–20, which repeatedly stress the necessity of aligning investigatory efficiency with fundamental rights protection. These provisions underline that the collection of electronic evidence, due to its intrusive nature, must respect the guarantees of the Charter of Fundamental Rights of the European Union, particularly Articles 7 (respect for private and family life), 8 (protection of personal data), and 47 (right to an effective remedy and fair trial). The Regulation thus frames digital investigative powers not merely as technical tools but as measures conditioned by strict constitutional requirements. The recitals make clear that necessity and proportionality operate as guiding principles in assessing production or preservation orders. Investigative authorities must demonstrate that such measures are indispensable for the criminal proceedings at hand and that no less intrusive alternative is available. This proportionality test resonates with the case law of the Court of Justice of the EU in areas such as data retention (*Digital Rights Ireland*, C-293/12, and *Tele2 Sverige*, C-203/15), where broad and indiscriminate collection of data was held incompatible with fundamental rights. By embedding these references, the Regulation acknowledges the tension between expansive law enforcement needs and the individual's right to privacy.

Another key element highlighted in these recitals is the protection of privileged communications and sensitive professions. Orders should not undermine professional secrecy, such as lawyer–client communications, journalistic sources, or medical confidentiality. This safeguard reflects the Court's jurisprudence, as well as the European Court of Human Rights' repeated emphasis on the chilling effect of surveillance on freedom of expression and defense rights (see *Michaud v. France*, *Big Brother Watch v. UK*). Such provisions are particularly significant when evaluating operations like EncroChat and Sky ECC, where entire networks of communications were intercepted indiscriminately, raising questions about whether the rights of non-suspects, professionals, and third parties received adequate protection. Finally, recitals 10–20 address the principle of judicial oversight. The Regulation specifies that the most intrusive categories of data—such as content data—must be subject to prior authorization by a judicial authority. This procedural safeguard seeks to ensure impartial scrutiny before data is accessed or disclosed, thereby reinforcing the legitimacy of cross-border requests. At the same time, the recitals leave unresolved questions regarding bulk interception and "hacking measures": practices that were central to the EncroChat investigations, but which are not easily reconcilable with the Regulation's model of targeted, case-specific orders. The gap between the Regulation's safeguards and the investigative reality of encrypted network infiltration highlights a potential challenge for its practical application in future high-profile cases.

Recitals 21–34 focus on the substantive scope of the Regulation by defining the categories of electronic data that can be subject to production or preservation orders. The Regulation distinguishes between four main categories: subscriber data, access data, transactional data, and content data. Each of these is associated with different thresholds of protection and procedural safeguards, reflecting the varying degree of interference with privacy and other fundamental rights. Subscriber and access data are presented as the least intrusive categories. They cover information identifying the user of a service (e.g., name, address, IP address) and data necessary for logging into a service. Recitals argue that because these data types typically do not reveal the substance of communications, they can be obtained under a less strict legal standard. Nevertheless, the aggregation of such data has been shown in practice to generate detailed user profiles, raising the question whether their classification as "low intrusive" remains adequate in light of technological realities (Koops and Leenes, 2014).

Transactional data—such as metadata indicating when, how, and between whom communications took place—are recognized as more sensitive. The Regulation explicitly notes that transactional data may allow the reconstruction of entire social networks and movement patterns. Therefore, production orders for such data must pass a higher threshold, requiring demonstration of necessity and proportionality and, in many cases, judicial authorization. The emphasis on metadata reflects lessons from the CJEU's jurisprudence (*Digital Rights Ireland*; *Tele2 Sverige*), where the Court found that metadata could be just as revealing as content.

The most sensitive category, content data, receives the highest level of protection. The recitals state that access to the substance of communications requires prior judicial approval, and such measures must be restricted to serious criminal offences. Since Regulation (EU) 2023/1543 has not yet entered into force, its safeguards could not have been applied to past investigations such as EncroChat and Sky ECC. Nevertheless, these operations provide a crucial stress test for the Regulation's future framework. The contrast between the Regulation's model of targeted, judicially authorised production orders and the reality of bulk interception techniques illustrates the potential limitations of the forthcoming regime. The central question is thus prospective: whether the Regulation will effectively regulate such investigative practices in the future, or whether they will continue to exist in a legal grey zone outside the scope of harmonised EU law.

Finally, the recitals stress the importance of legal certainty and harmonisation across Member States. By clarifying categories of data and corresponding safeguards, the Regulation seeks to prevent divergent national practices and "forum shopping" by investigators. However, critics note that the complexity of distinguishing between data types may create interpretative uncertainty, particularly in cases involving advanced encryption technologies or mixed data sets (Bignami, 2020). This interpretive ambiguity will likely become a contested issue in future judicial review before the CJEU and national courts.

References

Allegrezza, S. (2014) 'Collecting criminal evidence across the European Union: The European Investigation Order between flexibility and proportionality', in: Ruggeri, S. (ed.) *Transnational Evidence and Multicultural Inquiries in Europe*. Cham: Springer, 59-82.

Apelacioni sud u Beogradu (2025) *Presuda Kž1 По1 38/24, 11 July*. Beograd: Posebno odeljenje za organizovani kriminal.

Armada, I. (2015) 'The European Investigation Order and the lack of European standards for gathering evidence', *New Journal of European Criminal Law*, *6*(1), 8-33.

Bajović, V. (2022). 'Evidence from encrochat and sky ecc encrypted phones', *CRIMEN: časopis za krivične nauke*, *13*(2), 154-179.

Bajović, V. and Ćorić, V. (2025) 'EncroChat and Sky ECC data as evidence in criminal proceedings in light of the CJEU decision', *European Journal of Crime*, *Criminal Law and Criminal Justice*, 33, 235-262.

Belfiore, R. (2014) 'Critical remarks on the proposal for a European Investigation Order and some considerations on the issue of mutual admissibility of evidence', in: Ruggeri, S. (ed.) *Transnational Evidence and Multicultural Inquiries in Europe*. Cham: Springer, 125-145.

Britz, M. (2004) *Computer Forensics and Cyber Crime: An Introduction*. New Jersey: Prentice Hall.

Buono, L. (2019) 'The Genesis of the European Union's New Proposed Legal Instrument(s) on e-Evidence', *ERA Forum*, *19*(3), 307-312.
doi:10.1007/s12027-018-0525-4.

Buric, Z., Engelhart, M., Novokmet, A. and Roksandic, S. (2023) 'The admissibility of the results of mass surveillance of communication as evidence on Croatian criminal procedure: the Sky ECC case', *Croatian Annual of Criminal Sciences and Practice*, *30*(2), 243-274.

Capus, N. and Gilbert, D. (2024) 'Intercept evidence from foreign language communications: Reliability and minimum standards in the interests of justice', *The International Journal of Evidence & Proof*, *28*(4), 280-297.
doi: 10.1177/13657127241283662.

Catanzariti, M. (2025) 'Piercing the Veil of Ignorance of Fundamental Rights Protection: What Is Transnational in EU Judicial Cooperation?', in: *Facilitating Judicial Cooperation in the EU*. Leiden: Brill, Nijhoff. doi:10.1163/9789004705791_016.

Chaikin, D. (2006) 'Network investigations of cyber attacks: The limits of digital evidence', *Crime, Law & Social Change*, *46*(2), 141-158.

Davis, J., Purves, D., Gilbert, J. and Sturm, S. (2022) 'Five ethical challenges facing data-driven policing', *AI and Ethics*, *2*(2), 185-193.

Dediu, D. (2018) 'Protection of fundamental rights in the light of the Directive regarding the European Investigation Order', *Conferința Internațională de Drept, Studii Europene și Relații Internaționale*, 2018, 1-10.

Farries, A. (2010) 'The European Investigation Order: Stepping forward with care', *New Journal of European Criminal Law*, *1*(4), 445-457.

Ferguson, A.G. (2017) *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York: New York University Press.

Forlani, G. (2023) 'The e-evidence package: The happy ending of a long negotiation saga', eucrim – The European Criminal Law Associations', *Forum*, *18*(2), 174-181. doi:10.30709/eucrim-2023-013.

Galič, M., Stevens, L. and Koops, B.-J. (2023) 'Editorial: A trialogue on regulating data-driven criminal procedure', *New Journal of European Criminal Law*, *14*(4), 423-433. doi:10.1177/20322844231213484.

Ghosh, A. (2004) 'Guidelines for the Management of IT Evidence', *APEC Telecommunications and Information Working Group*, 29th Meeting, Hong Kong.

Hamidović, H. (2011) 'Osnovne karakteristike digitalnih dokaza', *Kriminalističko-forenzička istraživanja*, *4*(1), 55-69.

Heard, C. and Mansell, D. (2011) 'The European Investigation Order: Changing the face of evidence-gathering in EU cross-border cases', *New Journal of European Criminal Law*, *2*(4), 351-370.

Ivanović, A. and Ivanović, A. (2015) 'Evropski dokazni nalog i Evropski nalog za istragu u krivičnim stvarima', *Pravne teme*, *3*(5), 112-130.

Juszczak, A. and Sason, E. (2023) 'The use of electronic evidence in the European Area of Freedom, Security and Justice: An introduction to the new EU package on e-evidence', eucrim – The European Criminal Law Associations', *Forum*, *18*(2), 182-200. doi:10.30709/eucrim-2023-014.

Kiejnich-Kruk, K. (2024) 'Quo vadis Europa—balancing between efficiency and guarantees in criminal proceedings using the example of EU production and preservation orders', *New Journal of European Criminal Law*, *15*(2), 126-145. doi:10.1177/20322844241247482.

Kusak, M. (2019) 'Mutual admissibility of evidence and the European investigation order: aspirations lost in reality', *ERA Forum*, *19*(1), 1-15.

Kusak, M. (2024) 'EU Cross-Border Gathering and Admissibility of Electronic Content Data', *European Journal of Crime, Criminal Law and Criminal Justice*, *32*(2), 126-155. doi:10.1163/15718174-bja10054.

Lasagni, G. and Contissa, G. (2025) 'Effective Rights and Remedies in the Computable Era: Facing Informative Asymmetry When AI Adds to Transnational Cooperation', in: *Facilitating Judicial Cooperation in the EU*. Leiden: Brill, Nijhoff. doi:10.1163/9789004705791_003.

Lasagni, G., Caianiello, M. and Rezende, I.N. (2025) 'Comparative Remarks on Mutual Recognition Instruments of Judicial Cooperation in Criminal Matters', in: *Facilitating Judicial Cooperation in the EU*. Leiden: Brill, Nijhoff. doi:10.1163/9789004705791_015.

Leacock, C. (2008) 'Search and seizure of digital evidence in criminal proceedings', *Digital Evidence and Electronic Signature Law Review*, 5, 83-92.

Lukić, T. (2012) 'Digitalni dokazi', *Zbornik radova Pravnog fakulteta u Novom Sadu*, 2, 105-120.

Mirisan, L. (2018) 'The European Investigation Order', *Annales Universitatis Apulensis Series Jurisprudentia*, 21, 89-103.

Moghior, C. (2025) 'Cyber-securitization in light of the Snowden revelations: effects on institutional reform in the US and EU', *Europolity: Continuity and Change in European Governance*, *19*(1), 91-120.

Molder, R., Fedorova, M., Dubelaar, M. and Lestrade, S. (2023) 'The principle of purpose limitation in data-driven policing: A guiding light or an empty shell?', *New Journal of European Criminal Law*, *14*(4), 512-533. doi:10.1177/20322844231212749.

Monroy, M. (2022) *What's the problem with the EU regulation on the release of electronic evidence*? Available at: https://digit.site36.net/2022/03/04/whats-the-problem-with-the-eu-regulation-on-the-release-of-electronic-evidence/ (Accessed: 15 August 2025).

Oerlemans, J.J. and van Toor, D.A.G. (2022) 'Legal aspects of the EncroChat operation: A human-rights perspective', *European Journal of Crime, Criminal Law and Criminal Justice*, 30, 309-328.

Sachoulidou, A. (2024) 'Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of "judicial" cooperation', *New Journal of European Criminal Law*, *15*(3), 256-274. doi:10.1177/20322844241258649.

Sagittae, G. (2023) 'On the lawfulness of the EncroChat and Sky ECC operations', *New Journal of European Criminal Law*, *14*(3), 273-293. doi:10.1177/20322844231159576.

Salicius, M. and Moliene, R. (2024) 'The problem of obtaining evidence from EU countries while achieving the "crime does not pay" goal', *Baltic Journal of Law and Politics*, *17*(2), 207-227.

Signorato, S. (2023) 'Cross-border gathering of e-evidence: different legal frameworks in European Union and Council of Europe', *Journal of Eastern-European Criminal Law*, *2023*(1), 9-18.

Turanjanin, V. (2021) 'The principle of immediacy versus the efficiency of criminal proceedings: Do changes in the composition of the trial panel violate the right to a fair trial?', *Nordic Journal of Human Rights*, *39*(1), 73-87. doi:10.1080/18918131.2021.1923242.

Vervaele, J. (2005) *European Evidence Warrant: Transnational Judicial Inquiries in the EU*. Antwerp: Intersentia.

Vogler, R. (2014) 'The European Investigation Order: Fundamental rights at risk?', in: Ruggeri, S. (ed.) *Transnational Evidence and Multicultural Inquiries in Europe*. Cham: Springer, 147-165.

Warken, C. (2017) 'Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus, Teil 1. Beweissicherung im Zeitalter der digitalen Cloud', *Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht* (NZWiSt), *2017*(5), 289-295.

Zimmerman, F., Glaser, S. and Motz, A. (2011) 'Mutual recognition and its implications for the gathering of evidence in criminal proceedings: A critical analysis of the initiative for a European Investigation Order', *European Criminal Law Review*, *1*(1), 55–84.

© 2025 by authors

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution 4.0 International