Journal of Criminology and Criminal Law, 64(1), 7-29
Original Scientific Article
https://doi.org/10.47152/rkkp.64.1.1
UDK: 004.6:343.13(4–6EU)

RECEIVED: 18 January 2026
ACCEPTED: 20 January 2026

EncroChat, Sky ECC and Regulation (EU) 2023/1543: Towards a New Standard of Digital Evidence (II)[1]

Veljko Turanjanin[a]

This article constitutes a continuation of the analysis initiated in the first part of the study "EncroChat, Sky ECC and Regulation (EU) 2023/1543: Towards a New Standard of Digital Evidence (I)". The first part of this study examined the emergence of EncroChat and Sky ECC evidence in European criminal proceedings, focusing on the factual background of the Sky ECC investigations, the role of AI-assisted investigative techniques, the operation of mutual recognition mechanisms, and the evolving jurisprudence of the European Court of Human Rights, particularly the case *M.N. v. France*. It further analysed the challenges of the existing legal framework and the adoption of Regulation (EU) 2023/1543 on electronic evidence (Turanjanin, 2025).

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

[1] 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

Core Mechanisms of the Regulation

The Regulation defines its subject matter broadly, introducing two novel instruments: the European Production Order (EPO) and the European Preservation Order (EPO-PR). These allow judicial authorities in one Member State to compel service providers in another to either produce or preserve electronic evidence, irrespective of the data's location. Crucially, the Regulation extends this possibility not only to prosecutors and investigating authorities but also to the defence, thereby reflecting the principle of equality of arms. The scope of application is confined to criminal proceedings and the enforcement of custodial sentences, while mutual legal assistance (MLA) procedures remain outside its ambit.

The Regulation harmonises the definitions of key categories of electronic evidence - subscriber data, traffic data, and content data - each linked to distinct safeguards. Importantly, the Regulation sets out two differentiated regimes: one offering greater flexibility for *subscriber data* and for *data requested solely for the purpose of user identification* in a specific criminal investigation - such as IP addresses and, where necessary, source ports and time stamps - considered less intrusive; and another, stricter regime for *traffic data* (not limited to user identification) and *content data*, deemed more intrusive and therefore subject to enhanced judicial oversight (Sachoulidou, 2024, p. 261). It further clarifies who qualifies as a "service provider" - a category encompassing providers of electronic communications, hosting services, cloud infrastructure, and even online marketplaces. Providers established outside the Union but offering services within its territory are obliged to appoint a legal representative in the Union, ensuring enforceability of orders.

Taken together, these provisions represent a significant departure from previous reliance on the European Investigation Order (EIO). While the EIO remains a general instrument for evidence-gathering across borders, it has proven too slow and cumbersome for volatile data that can be deleted within hours. By contrast, the EPO/EPO-PR mechanism is designed as a direct-to-provider tool, streamlining access to digital evidence while introducing procedural guarantees. In doing so, the Regulation addresses shortcomings in voluntary cooperation with service providers and aligns EU law with international instruments such as the Budapest Convention on Cybercrime. This regulatory framework thus cements, and indeed extends, a broader paradigm shift toward direct cooperation between competent national authorities and foreign service providers operating within the EU. Such cooperation occurs irrespective of the provider's place of establishment, effectively bypassing traditional inter-state channels and redefining the role of private actors in criminal investigations (Tosza, 2021, p. 9; Sachoulidou, 2024, p. 259). The EU legislator's decision to codify what had previously been an informal, voluntary practice of direct cooperation between national judicial authorities and foreign service providers was motivated by long-standing criticism of the inefficiency of mutual legal assistance mechanisms, particularly the European Investigation Order. The new Regulation thus seeks to transform ad hoc cooperation into a structured and enforceable framework, reinforcing both legal certainty and procedural accountability (Sachoulidou, 2024, p. 265).

Issuing Authority

The Regulation carefully calibrates the authority to issue orders depending on the type of data requested. For subscriber data and data requested solely for user identification (e.g. IP addresses and ports), competence is relatively broad: orders may be issued by judges, courts, investigating judges, public prosecutors, or even other competent authorities designated by national law, provided that in the latter case, prior validation by a judicial authority is obtained. By contrast, access to traffic data (with the exception of basic identification) and to content data is subject to stricter requirements. Such orders may only be issued directly by a judge, a court, or an investigating judge, or by another competent authority acting as an investigating authority but subject to mandatory validation by a judicial authority. This differentiation reflects the principle of graduated protection: the more intrusive the data category, the higher the level of judicial control required (Shurson, 2025).

For European Preservation Orders, which are limited to securing data for subsequent production, the Regulation adopts a more flexible approach. These may be issued by judges, courts, investigating judges, and prosecutors, or by other competent authorities with subsequent validation. Importantly, the Regulation introduces an emergency mechanism: in urgent cases involving imminent threats to life, physical integrity, or critical infrastructure, certain non-judicial authorities may issue production or preservation orders for subscriber and identification data without prior validation. However, such orders must be validated ex post within 48 hours; failure to obtain validation requires immediate withdrawal and deletion of the data. Finally, Member States may designate central authorities for the administrative transmission and receipt of orders, ensuring smoother cross-border cooperation. This feature underscores the Regulation's ambition to combine direct-to-provider enforcement with structured oversight mechanisms that safeguard fundamental rights.

Conditions for Issuing a European Production Order and European Preservation Order

The Regulation establishes a layered set of conditions that reflect the principles of necessity, proportionality, and respect for fundamental rights. These conditions are designed both to harmonize practice across Member States and to ensure that cross-border data requests are subject to safeguards equivalent to those in domestic proceedings.

First, general necessity and proportionality requirements apply to all orders (Art. 5(2)). A European Production Order (EPO) may only be issued if the same measure would have been permissible in a similar domestic case, thereby embedding the principle of equivalence between national and cross-border evidence gathering. Second, the Regulation draws a substantive distinction between data categories:

1. Subscriber data and identification data: these may be requested for any criminal offence, regardless of its gravity, and for the execution of custodial sentences or detention orders of at least four months. This broad scope mirrors current investigative realities where identification data often serves as the starting point for more intrusive measures.

2. Traffic and content data: stricter thresholds apply. Such orders may only be issued for (a) offences punishable by at least three years' imprisonment in the issuing State, or (b) specific categories of serious crimes, including fraud and counterfeiting of non-cash means of payment (Directive 2019/713), child sexual exploitation (Directive 2011/93/EU), cybercrime (Directive 2013/40/EU), and terrorism (Directive 2017/541).

Third, the Regulation sets out mandatory elements that must be included in every order, such as the identity of the issuing authority, the addressee, the specific data category, the applicable criminal provisions, timeframes, and a summary description of the case (Art. 5(5)). This procedural transparency aims to minimize abusive or overly broad data requests.

Fourth, the Regulation introduces special rules to address complexities in data processing: A) Orders should normally be directed to the controller, but may exceptionally be addressed directly to a processor if the controller cannot be identified or if contacting the controller would jeopardize the investigation (Art. 5(6)); B) professional secrecy and privilege receive explicit recognition: EPOs for traffic or content data involving lawyers, doctors, journalists, or other privileged professionals can only be issued under limited conditions (Art. 5(9)) and C) similarly, data that may fall under immunities or freedom of expression protections in the enforcing State require prior clarification, and orders must be withheld if such privileges apply (Art. 5(10)).

Finally, the Regulation embeds special protections for defence rights and for contexts involving public authorities. For example, orders concerning data held in infrastructures provided to public authorities are only permissible when the authority is located in the issuing State (Art. 5(8)). Taken together, Article 5 represents an attempt to strike a balance: it broadens the operational reach of EU judicial cooperation in the digital sphere while maintaining heightened safeguards for more intrusive categories of data and for constitutionally sensitive contexts.

The European Preservation Order (EPO-PR) is conceived as a complementary mechanism to the European Production Order, designed to secure data that might otherwise be lost before formal production can be obtained. Article 6 sets out the conditions under which such orders may be issued, reflecting a preventive rather than an evidentiary function. First, as with production orders, necessity and proportionality are central requirements. A preservation order may only be issued if it is strictly necessary to prevent the removal, deletion, or alteration of data pending a subsequent request for production through mutual legal assistance, a European Investigation Order, or a European Production Order (Art. 6(2)). This design reflects the volatile nature of electronic evidence, which is often at risk of rapid deletion or alteration.

Second, the scope of preservation is broader than production. Unlike production orders—which for traffic and content data are limited to serious offences - preservation orders may be issued for all criminal offences, provided that the same measure would be permissible under national law in a comparable domestic case (Art. 6(3)). This indicates the legislator's recognition that preservation is a minimally intrusive measure, justified by the need to secure potential evidence for future judicial scrutiny. Third, preservation orders must meet clear formal requirements. Each order must include the identity of the issuing (and, if relevant, validating) authority, the addressee, the specific user or unique identifier, the category of data to be preserved, the relevant time range, the applicable criminal law

provisions, and the justification for necessity and proportionality (Art. 6(4)). These elements ensure traceability and accountability, and they prevent the use of preservation as a "fishing expedition." Finally, the Regulation cross-references Article 5(8), making clear that preservation orders involving data stored on infrastructures provided to public authorities can only be issued if the relevant authority is located in the issuing State. This safeguard prevents one Member State from unilaterally freezing data held by the public institutions of another, thereby respecting the principle of state sovereignty.

In sum, Article 6 strikes a deliberate balance: it provides law enforcement with a rapid response tool for the fragile nature of electronic evidence, while maintaining procedural discipline and limiting the potential for abuse. By requiring subsequent judicial channels for production, the Regulation ensures that preservation remains a temporary and ancillary measure, not a substitute for formal evidence-gathering procedures. Overall, the Regulation establishes a more demanding threshold for the issuance of a European Production Order than for a European Preservation Order, reflecting the higher degree of interference with fundamental rights associated with the production of content and traffic data (Sachoulidou, 2024, p. 262).

Transmission, Notification and Execution of Orders

Articles 7–9 regulate the procedural architecture of how European Production Orders (EPOs) and European Preservation Orders (EPO-PRs) are directed, transmitted, and formalised. As a rule, orders are addressed directly to a service provider's designated establishment or legal representative within the Union. This ensures a clear point of contact and eliminates uncertainty for cross-border compliance. In exceptional emergency situations, however, if the designated entity does not respond within the prescribed deadlines, the order may be redirected to any other establishment or representative of the same provider in the Union. For requests involving traffic or content data—the most sensitive categories—the issuing authority must also notify the enforcing authority of the Member State where the provider is established or represented. This notification serves as a safeguard, allowing the enforcing authority to evaluate whether grounds for refusal apply. There is, however, a territorial nexus exception: if both the offence and the person whose data are sought are connected to the issuing State, notification is not required. Both EPOs and EPO-PRs are formalised through standardised certificates - EPOC and EPOC-PR. These certificates contain detailed information about the issuing authority, the addressee, the user identifiers, the data category, the applicable criminal law provisions, and the justification of necessity and proportionality. The harmonised forms reduce ambiguity, facilitate digital transmission, and support multilingual cooperation through built-in translation requirements.

Article 10 specifies the obligations of service providers (the "addressees") once they receive a European Production Order Certificate (EPOC). The Regulation imposes strict deadlines to ensure that electronic evidence is preserved before it can be deleted. In ordinary cases, providers must transmit the requested data within 10 days. If notification to the enforcing authority is required under Article 8, the countdown begins only after that authority has either explicitly approved or failed to object within the same 10-day window. In emergency situations—such as imminent threats to life or public safety - the provider must act within 8 hours, underlining

the Regulation's ambition to match the speed of cybercrime. If the enforcing authority raises a ground for refusal (Article 12), any data already transmitted must be deleted, restricted, or used only under specified conditions, preserving the primacy of fundamental rights.

Service providers are expected to flag situations where execution could interfere with immunities, professional privileges, or media freedoms. This is particularly relevant in cases involving journalists, lawyers, or other protected professions. In such instances, the issuing authority must review the order and decide whether to withdraw, adapt, or maintain it, while the enforcing authority retains the power to raise refusal grounds. Furthermore, the Regulation anticipates practical hurdles: incomplete or erroneous EPOCs, or de facto impossibility (e.g., data no longer exist, user not identifiable). Providers must promptly inform authorities using a standardised form, and data must be preserved until the situation is clarified. Even when production is delayed or contested, providers must preserve the data until final resolution, ensuring that evidence is not lost while legal questions are addressed.

Article 11 sets out the practical framework for how service providers must execute a European Preservation Order Certificate (EPOC-PR). Upon receipt, providers are obliged to preserve the requested data without undue delay, but this duty is time-limited. The standard period is 60 days, extendable once by an additional 30 days if necessary to allow for a subsequent production request (Art. 11(1)). If, during this period, the issuing authority confirms that such a request has been made, the obligation continues until the data are formally produced (Art. 11(2)). This creates a clear temporal framework and avoids indefinite data retention. The obligation ceases once preservation is no longer necessary, either because the issuing authority withdraws the order or because no follow-up request for production is forthcoming (Art. 11(3)). This provision reflects the principle of data minimisation, a cornerstone of EU data protection law under the GDPR.

The Regulation mirrors the safeguards from Article 10. Service providers must flag potential conflicts with privileges, immunities, or media freedom protections (Art. 11(4)), ensuring that preservation does not undermine fundamental rights. In such cases, the issuing authority may withdraw, adapt, or maintain the order after reconsideration. If the EPOC-PR is incomplete or contains errors, providers may suspend their obligations until clarifications are received, with a maximum waiting period of five days (Art. 11(5)). Similarly, where compliance is impossible due to external circumstances not attributable to the provider, the obligation lapses once impossibility is confirmed (Art. 11(6)). In any other case of non-preservation, the provider must promptly notify the issuing authority and justify the failure (Art. 11(7)). This ensures transparency and accountability, while giving authorities an opportunity to reassess the necessity of preservation.

Article 12 introduces a carefully circumscribed set of grounds on which an enforcing authority may refuse to execute a European Production Order (EPOC). These grounds reflect a compromise between the need for cross-border efficiency and the duty to safeguard constitutional traditions and fundamental rights in the Member States. Once notified pursuant to Article 8, the enforcing authority must act within 10 days (or 96 hours in emergencies) to assess the EPOC and, where applicable, raise grounds for refusal (Art. 12(1)). This short timeframe ensures that refusal powers do not become a vehicle for delaying investigations.

Four main grounds are recognized:

1. Immunities, privileges, and media freedom (Art. 12(1)(a)) - Data cannot be produced if protected under the law of the enforcing State (e.g., parliamentary privilege, professional secrecy, journalistic source protection). This aligns with Article 11 CFR and ECtHR jurisprudence on freedom of expression.
2. Fundamental rights (Art. 12(1)(b)) - In "exceptional situations," an order may be refused if there is specific and objective evidence that compliance would result in a manifest breach of fundamental rights under Article 6 TEU and the Charter. This ground is framed restrictively to avoid abuse but remains a crucial safety valve.
3. *Ne bis in idem* (Art. 12(1)(c)) - Orders may not be executed if they would breach the principle against double jeopardy. This ground situates the Regulation firmly within broader EU criminal law guarantees, mirroring CISA and Article 50 CFR.
4. Dual criminality (Art. 12(1)(d)) - Execution may be refused if the underlying conduct is not an offence in the enforcing State. However, this is limited: dual criminality is not required for the Annex IV list of serious offences (terrorism, cybercrime, child sexual abuse, organised crime), provided they carry a maximum sentence of at least three years in the issuing State.

Before refusing, the enforcing authority is encouraged to consult with the issuing authority to seek adaptation of the order (Art. 12(3)). This dialogue-based approach reflects the EU's preference for mutual trust over adversarial refusal. Refusal may also be partial: the enforcing authority may allow transmission of some data or impose conditions on their use (Art. 12(4)). This flexibility prevents total failure of cooperation while respecting national sensitivities. Where immunities or privileges can be waived by a competent body (e.g., national parliament, professional bar association, or even an international organisation), the issuing authority may request such a waiver through the enforcing authority (Art. 12(5)).

We can say that Article 12 illustrates the limits of mutual recognition in EU criminal law. Unlike purely administrative measures, electronic evidence directly touches upon privacy, expression, and fair trial rights, which remain deeply embedded in national constitutional traditions. As such, the refusal grounds represent not a breakdown of trust, but rather its structured accommodation (see Salicius, Moliene, 2024, p. 215).

In addition to the core mechanisms of issuing and executing orders, the Regulation introduces ancillary provisions on user notification, confidentiality, and reimbursement of costs. Article 13 establishes, as a rule, the obligation of the issuing authority to inform the person whose data have been requested, thereby reinforcing transparency and the right to an effective remedy under Article 47 of the Charter. This duty, however, is subject to limitations: notification may be delayed, restricted, or omitted where disclosure would jeopardise the investigation, a tension that is particularly salient in covert operations such as *EncroChat* or *Sky ECC*. At the same time, service providers are required to adopt state-of-the-art technical and organisational safeguards to preserve the confidentiality and integrity of both orders and transmitted data. Article 14 addresses the financial dimension, allowing service providers to claim reimbursement of costs, but only under the same conditions as in domestic proceedings, thereby ensuring consistency and avoiding disproportionate burdens on providers.

While these provisions may appear ancillary, they highlight the Regulation's attempt to reconcile investigatory efficiency with fairness toward both individuals and private actors, situating e-evidence within a broader framework of procedural justice and economic feasibility.

Penalties and Enforcement

A distinctive feature of the Regulation is the introduction of explicit penalties and enforcement mechanisms aimed at ensuring compliance by service providers. Article 15 obliges Member States to establish rules on pecuniary sanctions for infringements of obligations under Articles 10, 11, and 13(4). The ceiling of these penalties is set at up to 2% of the provider's total worldwide annual turnover, a level comparable to the GDPR sanctioning framework. This marks a clear departure from the previous reliance on voluntary cooperation, signalling the EU's determination to move from "soft law" arrangements to hard enforcement mechanisms. At the same time, the Regulation shields providers from liability toward users for damages resulting from good-faith compliance, thus balancing legal certainty with deterrence.

Article 16 complements this sanctioning regime by detailing the procedure for enforcement. If a provider fails to comply with an EPOC or an EPOC-PR without justification, the issuing authority may request the enforcing authority to ensure compliance. Article 16 of the Regulation sets out the procedure for the enforcement of EPOs and EPOs-PR in cases where the service provider does not comply with the respective certificate without providing reasons accepted by the issuing authority, and where, if applicable, the enforcing authority has not raised any of the grounds for refusal listed above (Sachoulidou, 2024, p. 264). The enforcing authority must act without delay, recognising and enforcing the order within five working days, unless specific refusal grounds apply. Notably, the Regulation ensures a procedural dialogue: providers are informed of their rights to object, the possible penalties, and the relevant deadlines. Enforcement may be refused on narrowly defined grounds, largely mirroring those in Article 12, including fundamental-rights concerns and media-freedom protections.

Together, these provisions illustrate a dual dynamic: on the one hand, they strengthen the credibility of the Regulation by making non-compliance economically unattractive; on the other, they preserve the principle of proportionality by embedding safeguards and procedural checks. In doctrinal terms, this enforcement model reflects the broader EU trend of "compliance through deterrence," while adapting it to the sensitive field of criminal evidence gathering.

Article 18 of Regulation (EU) 2023/1543 codifies the right to effective remedies as a cornerstone safeguard in cross-border data access. Under Article 18(1), *any person whose data were requested* via a European Production Order (EPO) is entitled to seek an effective remedy against the order. This formulation marks a deliberate expansion compared to Article 17 of the Commission's original proposal, which had limited the right to *suspects and accused persons whose data were obtained* through an EPO. The final wording thus broadens the personal scope of protection, covering not only those whose data were actually transmitted but also individuals whose data were merely *sought* (Kiejnich-Kruk, 2024, p. 134; Topalnikos, 2023). Nevertheless, the right applies exclusively to

EPOs and does not extend to European Preservation Orders (EPO-PRs), thereby leaving a notable procedural gap in the protection framework.

Pursuant to Article 18(2), the right to an effective remedy must be exercised before a court in the issuing State, and it includes the possibility to challenge the legality, necessity, and proportionality of the measure - consistent with Article 47 of the Charter of Fundamental Rights of the European Union. However, this allocation of jurisdiction to the issuing State's courts raises practical and normative concerns, since the data subject may reside in the enforcing State or even outside the Union. Scholars have therefore argued that the remedy should be exercisable either in the enforcing or in the residence State, depending on the individual's choice—a position supported in the literature as enhancing both accessibility and compliance with the principle of effective judicial protection (Kiejnich-Kruk, 2024, pp. 134–136).

Critical Assessment

The adoption of Regulation (EU) 2023/1543 on e-evidence constitutes a landmark in the European Union's long-standing effort to harmonise cross-border access to electronic data in criminal proceedings. By introducing the European Production and Preservation Orders, the Regulation aims to replace the fragmented and often sluggish framework of mutual legal assistance with a direct, judicially controlled system of evidence gathering. In this sense, it responds to the growing need for timely and efficient access to digital material in an era where virtually every criminal act leaves an electronic trace.

Yet the Regulation also prompts a deeper reflection on its capacity to confront the realities of modern digital investigations, as starkly demonstrated by the *EncroChat* and *Sky ECC* operations. In both cases, European law enforcement agencies relied on sophisticated interception and infiltration techniques, obtaining vast quantities of encrypted communications outside any harmonised legal framework. These operations showcased the immense investigative potential of digital surveillance but simultaneously revealed the absence of a coherent EU-level approach to cross-border data collection in encrypted ecosystems.

Against this backdrop, the question arises whether Regulation 2023/1543, despite its procedural sophistication, genuinely resolves the normative and operational dilemmas exposed by such cases - or whether it merely codifies a partial solution centred on provider cooperation, leaving broader surveillance practices in a legal grey zone. A substantial body of scholarship has already scrutinised the European Production Order (EPO) framework, highlighting persistent doubts about the legal status of private actors and the adequacy of safeguards for fundamental rights. Commentators increasingly question whether the Regulation's efficiency-driven design can truly preserve the procedural guarantees embedded in EU law (Tosza, 2021; Matić Bošković, 2021; Fuster and Maymir, 2020; Kiejnich-Kruk, 2024, p. 127).

By 2024, digital traces featured in the vast majority of criminal investigations within the European Union - estimated at over 80 percent. Despite this pervasive reliance on electronic data, EU law still lacks common standards to assess the *authenticity* and *reliability* of such material once introduced as evidence in court. The Court of Justice of the European Union has repeatedly confirmed that, under current law, the admissibility and evidentiary value of digital material remain matters for national procedural autonomy. Most Member States,

consequently, operate under a presumption that digital evidence is genuine unless proven otherwise. Yet this approach becomes increasingly fragile in an era of algorithmic decision-making, automated data processing, and the proliferation of manipulated or synthetic content such as *deepfakes*. The absence of harmonised reliability benchmarks not only weakens mutual trust but also jeopardises the equality of arms in criminal proceedings.

The European legislator has begun to acknowledge these systemic vulnerabilities. Recital 59 of the forthcoming Artificial Intelligence Act (Regulation 2024/1689) explicitly recognises that certain AI systems used by police and judicial authorities may endanger fundamental procedural rights, including the presumption of innocence and the right to a fair trial, when their operation lacks transparency or explainability. Such systems are therefore classified as "high-risk," underscoring the need for accountability, accuracy, and traceability in their deployment. Nonetheless, the interface between the AI Act and the e-Evidence Regulation remains largely undefined. It is still unclear how the former will contribute to developing standards for verifying the reliability of digital evidence generated or processed by AI systems. This regulatory gap is particularly striking given that Article 82(2) TFEU empowers the Union to establish minimum standards on the mutual admissibility of evidence across Member States. For now, however, the EU appears reluctant to exercise this competence - despite its clear implications for procedural fairness and effective judicial protection (Okunrobo Perez, 2025). As Erbežnik (2023) notes, the introduction of pan-European production and preservation orders under the e-evidence package represents not merely a procedural innovation but a paradigmatic shift in the concept of mutual recognition within EU criminal law. By allowing judicial authorities to address service providers directly, without mediation by the executing state, the Regulation transforms mutual recognition from a principle of *interstate cooperation* into one of *functional interconnectivity* between national authorities and private actors. This evolution, as Erbežnik argues, reflects the broader digitalisation of justice and necessitates a re-examination of traditional guarantees of judicial oversight, territorial sovereignty, and defence rights in the digital environment.

Perhaps the most disruptive feature of the Regulation lies in its mandatory framework for direct cooperation between law enforcement authorities and private service providers. Although such cooperation has existed informally in the past, it previously depended entirely on the providers' willingness and internal procedures, often resulting in long delays or even outright refusals to cooperate (Kiejnich-Kruk, 2024, p. 128; Fuster and Maymir, 2020). The new mechanism seeks to overcome this inefficiency - where data can be deleted or relocated within seconds, while cross-border requests can take months - by compelling service providers to respond swiftly to European Production and Preservation Orders. However, this acceleration comes at a price. Scholars have voiced growing concern over the shifting role of private actors in safeguarding fundamental rights. Unlike public authorities, service providers are not bound by public law duties of due process or transparency, and their compliance is primarily motivated by the need to avoid sanctions rather than by procedural fairness (Corhay, 2021; Kiejnich-Kruk, 2024, p. 131). This direct cooperation model thus operates largely outside the framework of general judicial review, leaving limited opportunities for courts to exercise oversight over the execution of such orders. Equally troubling is the absence of an unconditional obligation to inform individuals whose data are sought.

Without notification, affected persons may be deprived of any meaningful opportunity to challenge the legality or proportionality of the measure, thereby undermining their right to an effective remedy (Monroy, 2022; Rojszczak, 2022; Kiejnich-Kruk, 2024, p. 132).

The unresolved issue of bulk interception

The relationship between technology and society has long been one of interdependence and tension, but the exponential development of digital technologies has fundamentally altered how individuals interact with one another and with the state (Kiernan and Mueller, 2021, p. 22; Leavens, 2015, p. 709). Scholars have repeatedly warned that one of the most efficient methods by which governments can erode personal liberties is through the deprivation of privacy (Weber, 1971, p. 358; Turanjanin, 2023). While surveillance has accompanied societies for centuries, mass digital surveillance - enabled by advanced communication technologies - represents a qualitatively new phenomenon (Franks, 2017, p. 425). The rise of such technologies has increased the ease with which governments can monitor, store, and process the everyday communications of citizens, often beyond the limits of traditional legal safeguards (Yadin, 2017, p. 709).

This section builds upon earlier analyses of the ECtHR's bulk interception jurisprudence (Turanjanin, 2022; 2023), updated to reflect the Court's latest case-law and its implications for digital evidence. The development of mass surveillance regimes coincided with a growing awareness that the right to privacy must evolve to meet technological change (Cole, 2016, p. 679; Jayawickrama, 2017, p. 650). As Siemion (2015, p. 20) observes, the pace of innovation has created a dangerous gap between existing legal frameworks and the technical capacity of the state to circumvent them. Law enforcement and intelligence bodies have increasingly relied on digital interception, data retention, and algorithmic profiling - techniques that were unimaginable only a generation ago (Manes, 2019, p. 505; Solove, 2004, p. 1267). These transformations challenge long-established understandings of procedural fairness and proportionality in criminal justice (Moonen, 2010, p. 98; Spencer, 2013, p. 374).

Within this context, bulk interception of cross-border communications—a form of mass data acquisition by intelligence services - has become one of the most controversial aspects of contemporary surveillance (Ünever, 2018). Unlike targeted interception, which focuses on specific suspects, bulk interception involves the large-scale collection of communications data—sometimes including content - based on technical filters applied to transnational communication flows (Freiwald, 2008, p. 333; Landau, 2016, p. 61). This practice is typically justified by the need to safeguard national security or combat terrorism and serious transnational crime (Sales, 2014, p. 524; Berman, 2016; Banks, 2017, p. 703; Kalanges, 2014; Swire, 2004; Kadidal, 2014; Banks and Bowman, 2000; Setty, 2015; Bellia, 2005, p. 1285).

The European Court of Human Rights (ECtHR) has developed a complex jurisprudence on the compatibility of bulk interception with Article 8 of the European Convention on Human Rights, which guarantees the right to respect for private and family life, home, and correspondence. In its earlier judgments (*Weber and Saravia v. Germany*, *Liberty and Others v. the United Kingdom*), the Court accepted that states enjoy a margin of apprecia-

tion in determining whether such regimes are necessary for national security. However, as the practice expanded and technology advanced, the Court recognised the need for stricter proportionality assessments and procedural safeguards. This evolution culminated in the Grand Chamber's twin judgments of *Big Brother Watch and Others v. the United Kingdom* and *Centrum för Rättvisa v. Sweden* (2021), which set out the most detailed framework to date for evaluating bulk surveillance (Turanjanin, 2023).

The Court reaffirmed that Article 8 does not per se prohibit bulk interception systems, but that they must operate within a narrow margin of appreciation and under strict conditions. It elaborated six minimum legal safeguards that must be clearly established to avoid abuse of power: the nature of the offences that may justify interception; definition of the categories of persons liable to have their communications intercepted; limits on the duration of interception; procedures for examining, using, and storing data obtained; precautions to be taken when communicating data to other parties and conditions for erasure or destruction of data once no longer needed (Schweda, 2015, p. 61; Scott, 2017, p. 110; *Roman Zakharov v. Russia*).

The ECtHR further emphasised the need for independent oversight mechanisms, notification procedures (where feasible), and effective legal remedies. Secret surveillance, by its very nature, must be accompanied by safeguards that are both accessible and foreseeable, ensuring that individuals are protected from arbitrary interference (*Weber and Saravia*, para. 46; *Malone*, para. 68; *Leander*, para. 51; *Huvig*, para. 29; *Bykov*, para. 78). Importantly, in *Big Brother Watch* and *Centrum för Rättvisa*, the Grand Chamber characterised bulk interception as a gradual, multi-stage process in which the degree of interference increases progressively: (a) interception and initial retention of communications and related data; (b) application of selectors and filters; (c) examination by analysts; and (d) subsequent retention, dissemination, and use of intelligence (*Big Brother Watch*, para. 325; *Centrum för Rättvisa*, para. 238). Each of these phases requires a proportionality assessment and corresponding safeguards. The Court noted that while the initial collection and immediate discarding of irrelevant data might seem minimally intrusive, even that stage entails significant interference since it places the totality of communications under state control. This view was strongly endorsed by Judges Lemmens, Vehabović, and Bošnjak in their joint opinion, who stressed that mass acquisition itself - even without analysis - represents an intrusion of constitutional magnitude.

Despite these clarifications, the Court's reasoning has not been without criticism. The earlier standards, developed more than a decade ago, are increasingly difficult to apply in today's digital context, where communications data have multiplied exponentially and the qualitative nature of digital interaction has changed (Big Brother Watch, para. 341; Centrum för Rättvisa, para. 255). Bulk interception now frequently involves international data flows, encompassing communications of persons both inside and outside the jurisdiction of the intercepting state (*Big Brother Watch*, para. 345; *Centrum för Rättvisa*, para. 258). The use of "strong selectors" (such as email addresses or device identifiers) to target individuals within bulk datasets blurs the line between mass and targeted surveillance.

From the perspective of the rule of law, the ECtHR's case-law underscores that any domestic legislation authorising such measures must be precise, publicly accessible, and

foreseeable. Where legal discretion is too broad or undefined, surveillance measures cannot be considered "in accordance with the law" (*Valenzuela Contreras v. Spain*, para. 67; *Kopp v. Switzerland*, para. 72; *P.G. and J.H. v. the United Kingdom*, para. 39). As scholars note, this requirement stems from the very essence of democratic governance: the law must indicate the scope of discretion and conditions of use to provide adequate protection against arbitrary interference (Fenyvesi, 2006, p. 183; Clark, 1990, p. 155; Esen, 2012, p. 164; Moonen, 2010, p. 98; Spencer, 2013, p. 374; Henderson, 2015–2016, p. 28).

The Court's evolving approach reflects the broader understanding that surveillance in democratic societies must remain exceptional and narrowly tailored. Yet, as technological developments outpace legal reform, the practical distinction between targeted and bulk interception has become increasingly blurred. The danger lies in normalising measures initially conceived as extraordinary tools for national security. As several commentators have observed, modern investigative needs must not be allowed to erode the very procedural guarantees that distinguish the rule of law from authoritarian governance (Nomikos, 2017, p. 122; Jacobs, 2009, p. 19; Robis, 2014, p. 203).

Although the ECtHR has provided a detailed normative framework, it remains largely reactive - addressing state practices *ex post* rather than preventing systemic overreach. The exponential expansion of digital evidence in criminal proceedings, coupled with the transnational character of modern crime, exposes a persistent gap between principle and practice. This gap is especially visible in the operations *EncroChat* and *Sky ECC*, where national authorities relied on network-level interception and infiltration of encrypted communication systems outside any harmonised EU legal framework. These cases illustrate the grey zone between targeted surveillance authorised by judicial warrant and the mass interception of digital communications carried out for intelligence purposes, later repurposed for criminal prosecution.

While *Weber and Saravia* laid the initial foundation for assessing secret surveillance, the Court itself recognised in *Big Brother Watch* and *Centrum för Rättvisa* that the rapid evolution of digital interception technologies rendered parts of the earlier six-criteria test insufficient. In particular, the requirements concerning the nature of offences that may justify interception, the definition of categories of individuals subject to interception, and the existence of reasonable suspicion - central to targeted interception - were found to be only partially applicable in the context of bulk interception. Nevertheless, the Court insisted that national legislation must still provide clear and detailed rules governing the use of such measures, specifying both the *grounds* on which bulk interception may be authorised and the *circumstances* under which an individual's communications may be intercepted (*Big Brother Watch*, para. 348; *Centrum för Rättvisa*, para. 262).

As Judges Lemmens, Vehabović, and Bošnjak observed in their joint partly concurring opinion, these references to "grounds" and "circumstances" remain vague and indeterminate, a concern echoed by Judge Pinto de Albuquerque, who criticised the Court's reasoning as inadmissibly imprecise. Such ambiguity, they argued, risks undermining the foreseeability required by Article 8 of the Convention.

Recognising the inherent risks of abuse in mass surveillance regimes, the ECtHR emphasised that bulk interception must be governed by "end-to-end safeguards" - a continuous framework of oversight and proportionality checks covering each stage of the interception process (*Big Brother Watch*, para. 350; *Centrum för Rättvisa*, para. 264). The Court identified three essential components of this system: an assessment of necessity and proportionality at every stage of interception; independent authorisation at the outset by a body separate from the executive; and ongoing supervision and post-facto review by an independent authority.

Although judicial authorisation is widely regarded as a cornerstone of procedural fairness (van der Sloot and Kosta, 2019, p. 258), the Court held that it is not an indispensable requirement, provided that authorisation is issued by an independent body empowered to assess necessity and proportionality and to scrutinise the selection of communication routes subject to interception (*Big Brother Watch*, paras. 351–352; *Centrum för Rättvisa*, paras. 265–266).

The use of selectors - keywords, addresses, or technical identifiers that determine which communications will be analysed - was singled out as the most critical stage of the process. Given the vast number of selectors employed and the need for operational flexibility, not all can feasibly be listed in an authorisation order. However, the Court demanded that at least the *types or categories* of selectors be identified in advance and that strong selectors associated with identifiable individuals be subject to enhanced safeguards. Each such selector must be individually justified, recorded, and authorised through a separate, objective internal review (*Big Brother Watch*, para. 355; *Centrum för Rättvisa*, para. 269). The Court further underlined that continuous supervision by an independent authority is vital to ensure that interference remains "necessary in a democratic society" (*Roman Zakharov*, para. 232; *Klass*, paras. 49–59; *Kennedy*, paras. 153–154). Yet, as Vladeck (2014, p. 578) notes, the creation of a truly adversarial judicial review system for secret surveillance programs may be structurally impossible. To mitigate this, the Court required that detailed records be maintained at all stages of interception and that individuals have access to an effective remedy - either to challenge the lawfulness of specific measures or to contest the overall compatibility of the regime with the Convention (*Big Brother Watch*, para. 356; *Centrum för Rättvisa*, para. 270).

The issue of notification emerged as a crucial element of this remedy. In *Klass and Others v. Germany*, the Court had already recognised that post-surveillance notification enhances the effectiveness of judicial redress (para. 57). Later cases reaffirmed that individuals must, in principle, be informed of surveillance measures once this can be done without compromising their purpose (*Weber and Saravia*, para. 135; *Leander v. Sweden*, para. 66; *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, para. 90). In *Szabó and Vissy v. Hungary*, the Court found a violation of Article 8 partly due to the absence of any notification mechanism (Boroi, 2013, p. 59). However, *Big Brother Watch* introduced a more pragmatic approach: notification is not an absolute requirement if an alternative, independent, and adversarial remedy exists that provides comparable procedural guarantees (*Big Brother Watch*, para. 358; *Centrum för Rättvisa*, para. 272). In this regard, the powers and procedural guarantees of the oversight body are decisive in assessing effectiveness. The reviewing authority need not be judicial in nature, but it must be fully independent of the executive and capable of issuing binding decisions, including

the cessation of unlawful interception and the destruction of unlawfully obtained material (*Segerstedt-Wiberg and Others v. Sweden*, para. 120; *Leander v. Sweden*, paras. 81–83).

In its most recent jurisprudence, the ECtHR expanded its scrutiny beyond the six *Weber* safeguards, establishing eight criteria that states must satisfy when operating bulk interception regimes (*Big Brother Watch*, para. 361; *Centrum för Rättvisa*, para. 275): the grounds on which bulk interception may be authorised; the circumstances under which individual communications may be intercepted; the procedure for granting authorisation; the procedure for selecting, examining, and using intercepted material; safeguards for transmission to third parties; limits on duration, storage, and destruction of data; mechanisms for supervision and enforcement by an independent authority; and procedures for ex post facto review and redress.

A particularly sensitive issue concerns international data-sharing between intelligence services. The Court acknowledged that some states permit foreign partners direct access to their systems, yet it has not elaborated comprehensive safeguards for such transfers. Nonetheless, four essential principles were established: (1) the conditions for transfer must be explicitly defined in domestic law; (2) the transferring state must ensure that the recipient guarantees adequate data security and proportional use; (3) special safeguards must apply to the transfer of confidential or journalistic material; and (4) all such transfers must be subject to independent oversight (*Big Brother Watch*, para. 362; *Centrum för Rättvisa*, para. 276).

Finally, the Court rejected the notion that communications metadata are inherently less intrusive than content data, affirming that both forms require equivalent legal protection (Murray and Fussey, 2019, p. 54; Buono and Taylor, 2017; Mulligan, 2016; Robertson, 2017, p. 151; Ünever and Kim, 2016; Propp, 2019; *Big Brother Watch*, para. 363; *Centrum för Rättvisa*, para. 277). While acknowledging that metadata and content may be handled differently in practice, the Court insisted that the same fundamental safeguards must apply to both categories to ensure compliance with the principle of proportionality (*Big Brother Watch*, para. 364; *Centrum för Rättvisa*, para. 278).

Judicial oversight and proportionality controls

The Regulation introduces essential procedural safeguards, notably the requirement of prior judicial authorisation for access to content data and the application of necessity and proportionality tests. These provisions aim to align cross-border evidence-gathering with the constitutional traditions of EU Member States and the guarantees enshrined in Articles 7 and 8 of the Charter of Fundamental Rights. Nevertheless, several questions arise as to whether these safeguards are sufficiently robust in practice. First, the catalogue of offences permitting the issuance of European Production Orders remains broad, extending beyond "serious crime" to include the offences listed in Annex IV, such as cybercrime, child sexual exploitation, and a variety of technology-enabled offences. While the inclusion of such categories is understandable from a policy standpoint, the lack of a clear threshold for seriousness risks diluting the proportionality principle.

Second, the Regulation's model of oversight relies heavily on mutual trust and procedural cooperation among Member States. The enforcing authority is notified in certain

instances, yet its capacity to conduct substantive review of the issuing authority's proportionality assessment is limited. In effect, judicial control is exercised ex ante only in the issuing state, while the executing state's role remains largely formal. This asymmetry may prove problematic in situations where national standards of fundamental rights protection diverge. Third, while Article 8 of the Regulation requires issuing authorities to consider less intrusive measures, it does not mandate a comprehensive balancing test comparable to that applied by the ECtHR in surveillance cases. The proportionality assessment thus risks becoming a procedural formality rather than a substantive guarantee. In sum, the Regulation represents a step forward in codifying judicial oversight at the EU level, yet its reliance on mutual recognition and trust places considerable weight on domestic compliance cultures. Without harmonised standards of review and clearer thresholds for gravity, the practical effectiveness of these safeguards may remain contingent upon the integrity and diligence of national authorities.

The Regulation's ambitious objective of streamlining cross-border access to electronic evidence within the EU must be viewed in the broader international context. While it enhances efficiency and cooperation among Member States, it simultaneously highlights the absence of a coherent global framework for digital evidence collection. One of the most pressing risks lies in the potential conflict of laws with third-country regimes, most notably the U.S. CLOUD Act, which allows American authorities direct access to data stored abroad by U.S. providers. This legislative model contrasts sharply with the EU's rights-based approach, prioritising individual privacy and judicial control. Without a comprehensive transatlantic agreement, service providers operating in both jurisdictions may face irreconcilable obligations - to disclose data under U.S. law while simultaneously respecting EU privacy and fundamental rights standards.

The problem extends beyond transatlantic relations. Countries such as China, Russia, and India have also developed domestic frameworks for cross-border data access, often driven by security and sovereignty concerns. The proliferation of these divergent regimes threatens to fragment the global legal order into competing data sovereignties, each asserting control over information flows within its territorial or regulatory reach.

In this evolving landscape, the EU's Regulation (EU) 2023/1543 may be seen as both a model of procedural innovation and a reflection of systemic fragmentation. While it provides a harmonised structure for intra-EU cooperation, it does little to resolve tensions with external jurisdictions or to address the technological realities of global cloud infrastructure. In practice, investigators may still resort to informal cooperation, open-source intelligence, or even extra-legal methods such as bulk interception when formal mechanisms prove inadequate. Ultimately, the Regulation embodies a paradox: it institutionalises trust within the Union but leaves uncertainty beyond it. By focusing on provider compliance rather than global interoperability, it risks cementing a regional enclave of legal certainty within an otherwise divided digital world. The challenge ahead lies not merely in perfecting the EU's internal mechanisms but in promoting an international consensus that reconciles efficiency with fundamental rights and the rule of law.

EncroChat, Sky ECC and the Future of Digital Evidence in Light of Regulation (EU) 2023/1543

The investigations known as *EncroChat* and *Sky ECC* revealed both the potential and the fragility of digital evidence in contemporary criminal justice. They demonstrated how encrypted communications could expose large criminal networks, but also how fragmented the European approach to the admissibility of such data remains. National courts reached diverging conclusions concerning legality, authenticity, and proportionality: French and Dutch courts largely endorsed the operations on the basis of mutual trust and joint investigation cooperation, whereas German and Scandinavian courts expressed doubts regarding the technical chain of custody and the limits of cross-border surveillance. Montenegro's Supreme Court later confirmed the finality of a conviction based on Sky ECC material, showing how national jurisdictions in the wider European area continue to depend on general principles of legality and mutual assistance rather than a common standard for digital evidence.

Regulation (EU) 2023/1543 on the European Production and Preservation Orders for electronic evidence introduces the first genuinely harmonised framework for obtaining data across borders. It replaces slow mutual-legal-assistance requests with direct judicial orders addressed to service providers and their designated representatives within the European Union. This approach transforms mutual recognition from a principle of cooperation between states into a functional mechanism connecting judicial authorities and private actors. Had the EncroChat or Sky ECC data been obtained under this regime, the process would have followed uniform procedures for issuing, certifying, and logging orders, ensuring verifiable authenticity and minimising controversies about extraterritorial hacking or the lack of judicial oversight. Yet the Regulation would still require post-factum judicial review and defence access to relevant metadata, safeguarding the balance between operational efficiency and the right to a fair trial.

The new framework also responds to persistent concerns about transparency and the rights of the defence. It obliges competent authorities to inform affected persons of the use of production or preservation orders once secrecy is no longer justified, establishes controlled channels for notification between Member States, and ensures that data subjects or their representatives may challenge the legality of an order before a judicial body. These mechanisms directly address the opacity that characterised many EncroChat-related trials, where defendants were denied information on decryption techniques or on the technical origin of intercepted material. By embedding disclosure and judicial-review obligations, the Regulation turns transparency into a procedural right rather than an investigative concession.

While the Regulation entered into force in 2023, it will apply only from 2026 and has no retroactive effect. Nonetheless, its principles - judicial accountability, proportionality, and verifiable data integrity - are likely to influence courts dealing with ongoing prosecutions that originated under the previous regime. In practice, national judges may interpret existing procedural rules through the lens of the Regulation to ensure compatibility with the evolving standards of fairness under European human-rights law. The

normative influence of the new instrument will thus extend beyond its temporal scope, gradually shaping a common evidentiary culture within the Union.

The broader implication of these developments is the emergence of a European standard of digital proof. Regulation 2023/1543 institutionalises lessons learned from EncroChat and Sky ECC: the need for rapid access to electronic data must never eclipse judicial control and defence rights. Its success will depend on consistent implementation by Member States and on how effectively national courts reconcile technological innovation with procedural safeguards. In this sense, the Regulation marks both a culmination of two decades of experimentation with electronic evidence and a new starting point for building a coherent, rights-based digital-justice order in Europe.

Implications for Candidate Countries

The adoption of Regulation (EU) 2023/1543 and its accompanying Directive has implications that reach well beyond the borders of the European Union. For candidate countries such as Serbia, Montenegro, and North Macedonia, aligning domestic criminal-procedure laws with the new European framework is not merely a technical requirement of the accession process but a structural necessity for ensuring the admissibility and credibility of digital evidence in transnational proceedings. The integration of these standards is crucial for two reasons: first, to guarantee that evidence exchanged with EU Member States meets the same procedural and data-protection guarantees; and second, to ensure that investigative cooperation based on mutual recognition can function effectively once accession occurs.

One of the central challenges for candidate countries lies in the uncritical use of the term *mutual trust*. In EU law, mutual trust presupposes a shared level of rule-of-law protection and a minimum of procedural safeguards among Member States. When transplanted into legal systems that have not yet achieved full judicial independence or robust data-protection oversight, the concept can be misused to justify the automatic acceptance of foreign evidence without proper verification of its origin or legality. This risks transforming mutual trust into blind faith and eroding the very legitimacy of cross-border cooperation. Candidate states must therefore approach alignment not as a formal transposition exercise but as a deeper reform process aimed at achieving the institutional and procedural conditions that make mutual trust credible.

In the Serbian context, this means revising the domestic Criminal Procedure Code to introduce explicit rules on digital evidence gathering and admissibility, consistent with the logic of the EU's e-evidence framework. Current provisions treat electronic material under the general category of documents, offering limited guidance on authenticity, chain of custody, or defence access. A dedicated chapter on electronic evidence - covering production and preservation orders, conditions for accessing data from foreign service providers, and rules for judicial control - would bridge this gap. Equally important is the introduction of narrowly defined *hacking measures* and intrusive digital-forensic techniques under strict judicial authorisation. The EncroChat and Sky ECC experiences demonstrate that, in the absence of clear statutory limits, such methods can blur the line between legitimate surveillance and mass interception. Serbia and other candidate countries should regulate

these techniques explicitly, setting conditions for proportionality, data minimisation, and subsequent disclosure to the defence once operational secrecy is no longer justified.

To reinforce accountability, domestic law should establish *ad hoc* oversight bodies with mixed judicial, prosecutorial, and technical expertise. These bodies would review the implementation of intrusive measures, supervise the handling of encrypted or intercepted data, and verify compliance with fundamental-rights standards. Regular reporting to parliament or an independent data-protection authority would further enhance transparency and public trust. Ultimately, aligning with the EU's e-evidence framework is not only about harmonising statutes but about embedding a culture of legality, transparency, and rights protection in digital investigations. Candidate countries that adopt this approach will not only facilitate smoother judicial cooperation with the EU but also strengthen the legitimacy of their own criminal-justice systems in the face of rapid technological change.

Conclusion

The adoption of Regulation (EU) 2023/1543 represents a turning point in the evolution of digital evidence within the European Area of Freedom, Security and Justice. By establishing the European Production and Preservation Orders, the EU has introduced a new model of cross-border cooperation that replaces slow and fragmented mutual legal assistance procedures with a harmonised, direct, and technologically attuned mechanism. However, the efficiency gains brought by this framework also come with delicate challenges. The Regulation's reliance on mutual trust between Member States presupposes an equal level of protection of fundamental rights and procedural guarantees across the Union—an assumption that remains aspirational rather than fully realised.

The analysis of the EncroChat and Sky ECC cases demonstrates both the potential and the risks of the new paradigm. While large-scale interception operations have proven essential for dismantling organised criminal networks, they have also exposed persistent gaps in transparency, judicial oversight, and the rights of defence. Under the new regime, such evidence would likely be admissible provided that it meets the standards of necessity, proportionality, and judicial validation. Yet the broader question remains whether procedural safeguards will evolve at the same pace as technological capabilities.

For candidate countries such as Serbia, alignment with the e-evidence framework is not merely a technical obligation but a constitutional imperative. Transposing the Regulation's principles into domestic law requires the introduction of clear procedural safeguards, judicial review mechanisms, and ad hoc oversight bodies to prevent misuse of intrusive investigative powers. Above all, the concept of "mutual trust" must not become a substitute for mutual accountability. Ultimately, the e-evidence package marks a decisive shift towards a European digital justice system founded on interoperability, legality, and respect for human rights. Its success will depend on constant monitoring, transparent implementation, and a shared commitment to uphold the rule of law in the digital age.

References

Banks, W. (2017) 'Cyber espionage and electronic surveillance: Beyond the media coverage', *Emory Law Journal*, 66, 513-525.

Banks, W. and Bowman, M. (2000) 'Executive authority for national security surveillance', *American University Law Review*, 50, 2-130.

Bellia, P.L. (2005) 'Spyware and the limits of surveillance law', *Berkeley Technology Law Journal*, 20, 1283-1344.

Berman, E. (2016) 'The two faces of the Foreign Intelligence Surveillance Court', *Indiana Law Journal*, 91, 1192-1250.

Buono, I. and Taylor, A. (2017) 'Mass surveillance in the CJEU: Forging a European consensus', *Cambridge Law Journal*, 76, 250-253. https://doi.org/10.1017/s0008197317000526

Clark, W. (1990) 'Electronic surveillance and related investigative techniques', *Military Law Review*, 128, 155-224.

Cole, D. (2016) 'After Snowden: Regulating technology-aided surveillance in the digital age', *Capital University Law Review*, 44, 677-691.

Corhay, M. (2021) 'Private Life, Personal Data Protection and the Role of Service Providers: The EU e-Evidence Proposal', *European Papers*, *6*(1), 467-490. doi:10.15166/2499-8249/477.

Erbežnik, A. (2023) 'Impact of digital evidence gathering on the criminal justice system: A broader perspective', in Franssen, V. and Tosza, S. (eds.) *The Cambridge Handbook of Digital Evidence in Criminal Investigations*. Cambridge: Cambridge University Press, 557-572. doi:10.1017/9781009338508.031.

Esen, R. (2012) 'Intercepting communications "in accordance with the law"', *The Journal of Criminal Law*, 76, 164-178.

Fenyvesi, C. (2006) 'The legal and criminalistic aspects of secret data and information collection', *Acta Juridica Hungarica*, 47, 183-199.

Franks, M.A. (2017) 'Democratic surveillance', *Harvard Journal of Law & Technology*, 30, 425-489.

Freiwald, S. (2008) 'Electronic surveillance at the virtual border', *Mississippi Law Journal*, 78, 333-368.

González Fuster, G. and Maymir, S.V. (2020) 'Cross-border Access to E-Evidence: Framing the Evidence', *Liberty and Security in Europe*, 2020(2), 1-20. Available at: https://www.ceps.eu/wp-content/uploads/2020/03/LSE2020-02_Cross-border-Access-to-E-Evidence.pdf (Accessed: 15 August 2025).

Henderson, S. (2016) 'A rose by any other name: Regulating law enforcement bulk metadata collection', *Texas Law Review*, 94, 28-59.

Jacobs, B. (2009) 'Keeping our surveillance society non-totalitarian', *Amsterdam Law Forum*, 1, 19-34.

Jayawickrama, N. (2017) *The Judicial Application of Human Rights Law: National, Regional and International Jurisprudence*. Cambridge: Cambridge University Press.

Kadidal, S. (2014) 'NSA surveillance: The implications for civil liberties', *Journal of Law and Policy for the Information Society*, 10, 433-479.

Kalanges, S. (2014) 'Modern private data collection and National Security Agency surveillance: A comprehensive package of solutions addressing domestic surveillance concerns', *Northern Illinois University Law Review*, 34, 644-679.

Kiernan, C. and Mueller, M. (2021) 'Standardizing security: Surveillance, human rights, and the battle over TLS 1.3', *Journal of Information Policy*, 11, 1-25. https://doi.org/10.5325/jinfopoli.11.2021.0001

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. https://doi.org/10.1177/20322844241247482

Landau, S. (2016) 'Choices: Privacy & surveillance in a once & future internet', *Daedalus*, 145, 54-64.

Leavens, A. (2015) 'The Fourth Amendment and surveillance in a digital world', *Journal of Civil Rights and Economic Development*, 27, 709-746.

Manes, J. (2019) 'Secrecy & evasion in police surveillance technology', *Berkeley Technology Law Journal*, 34, 504-566.

Matić Bošković, M. (2021) 'Impact of Modern Technologies on Free Movement of Evidence in European Union', *Journal of Criminology and Criminal Law 59*(3): 123-140. https://doi.org/10.47152/rkkp.59.3.6

Monroy, M. (2022) 'What's the problem with the EU regulation on the release of electronic evidence?', *Digit Site36*, 4 March. 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).

Moonen, T. (2010) 'Special investigation techniques, data processing and privacy protection in the jurisprudence of the European Court of Human Rights', *Pace International Law Review Online Companion*, 1, 197-236.

Mulligan, A. (2016) 'Constitutional aspects of international data transfer and mass surveillance', *Irish Jurist*, 55, 199-208.

Murray, D. and Fussey, P. (2019) 'Bulk surveillance in the digital age: Rethinking the human rights law approach to bulk monitoring of communications data', *Israel Law Review*, *52*(1), 31-60. https://doi.org/10.1017/s0021223718000304

Nomikos, L. (2017) 'Are we sleepwalking into a surveillance society?', *Bristol Law Review*, 111-122.

Okunrobo Perez, S. (2025) 'Proliferation of e-Evidence: Reliability Standards and the Right to a Fair Trial', *European Journal of Crime, Criminal Law and Criminal Justice*, *33*(1-2), 187-211. https://doi.org/10.1163/15718174-bja10070

Propp, K. (2019) 'US surveillance on trial in Europe: Will transatlantic digital commerce be collateral damage?', *Atlantic Council*, 1-6.

Robertson, R. (2017) 'The unconstitutionality of bulk data collection', *Boston University Public Interest Law Journal*, 26, 151-176.

Robis, L.A. (2014) 'When does public interest justify government interference and surveillance', *Asia Pacific Journal on Human Rights and the Law*, 5, 203-218. https://doi.org/10.1163/15718158-15010209

Rojszczak, M. (2022) 'E-Evidence Cooperation in Criminal Matters from an EU Perspective', *Modern Law Review*, *85*(4), 1002-1003. https://doi.org/10.1111/1468-2230.12749

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.

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. https://doi.org/10.2478/bjlp-2024-00022

Sales, N. (2014) 'Domesticating programmatic surveillance: Some thoughts on the NSA controversy', *Journal of Law and Policy for the Information Society*, 10, 523-548.

Schweda, S. (2015) 'UK surveillance under judicial scrutiny: GCHQ intelligence sharing with NSA contravened human rights, but is now legal', *European Data Protection Law Review*, 1, 61-69. https://doi.org/10.21552/edpl/2015/1/12

Scott, P. (2017) 'General warrants, thematic warrants, bulk warrants: Property interference for national security purposes', *Northern Ireland Legal Quarterly*, *68*(2), 99-121. https://doi.org/10.53386/nilq.v68i2.32

Setty, S. (2015) 'Surveillance, secrecy, and the search for meaningful accountability', *Stanford Journal of International Law*, 51, 69-103. https://doi.org/10.31228/osf.io/uyjmh

Shurson, J. (2025). 'The balance of efficiency and fundamental rights in the EU e-Evidence Regulation', *New Journal of European Criminal Law*, *16*(3), 278-299. https://doi.org/10.1177/20322844251357090.

Siemion, R. (2015) 'Protecting privacy in the digital age: Beyond reforming bulk telephone records collections', *Human Rights Law Review*, 41, 17-20.

Solove, D. (2004) 'Reconstructing electronic surveillance law', *The George Washington Law Review*, 72, 1701-1747. https://doi.org/10.2139/ssrn.445180

Spencer, S. (2013) 'The surveillance society and the third-party privacy problem', *Scottish Constitutional Law Review*, 65, 374-410.

Swire, P. (2004) 'The system of foreign intelligence surveillance law', *The George Washington Law Review*, 72, 1307-1372.

Topalnakos, P. (2023) 'Critical Issues in the New EU Regulation on Electronic Evidence in Criminal Proceedings', *Eucrim – The European Criminal Law Associations' Forum*, 2023(2), 202–210. https://doi.org/10.30709/eucrim-2023-015

Tosza, S. (2021) 'Internet service providers as law enforcers and adjudicators: A public role of private actors', *Computer Law & Security Review*, 43, 105614. https://doi.org/10.1016/j.clsr.2021.105614

Turanjanin, V. (2022) 'Special investigative measures: Comparison of the Serbian Criminal Procedure Code with the European Court of Human Rights standards', *The International Journal of Evidence & Proof*, *26*(1), 34-60. https://doi.org/10.1177/13657127211055230

Turanjanin, V. (2023) 'When does bulk interception of communications violate the right to privacy? The limits of the state's power and the European Court of Human Rights approach', *International Cybersecurity Law Review*, 4, 115-136. https://doi.org/10.1365/s43439-022-00074-7

Turanjanin, V. (2025) 'EncroChat, Sky ECC and Regulation (EU) 2023/1543: Towards a New Standard of Digital Evidence (I)', *Journal of Criminology and Criminal Law 63*(3), 7-30. https://doi.org/10.47152/rkkp.63.3.1

Ünver, A. (2018) *Politics of Digital Surveillance, National Security and Privacy*. Oxford: EDAM, CTGA & Kadir Has University.

Ünver, A. and Kim, G. (2016) 'Data privacy and surveillance in Turkey: An assessment of the draft law on the protection of personal data', *EDAM Policy Studies*, 1-20.

Van der Sloot, B. and Kosta, E. (2019) 'Big Brother Watch and Others v UK: Lessons from the latest Strasbourg ruling on bulk surveillance', *European Data Protection Law Review*, *5*(2), 252–261. https://doi.org/10.21552/edpl/2019/2/16

Weber, S. (1971) 'Habeas data: The right of privacy versus computer surveillance', *University of San Francisco Law Review*, 5, 358-377.

Yadin, G. (2017) 'Virtual reality surveillance', *Cardozo Arts and Entertainment Law Journal*, 35, 709-746.