ISSN 1820-2969 (PRINT)
ISSN 2956-2198 (ONLINE)
UDK 343

JCCL

JOURNAL OF CRIMINOLOGY AND CRIMINAL LAW

REVIJA ZA KRIMINOLOGIJU I KRIVIČNO PRAVO

VOLUME 64/2026
NUMBER 1

SERBIAN ASSOCIATION FOR CRIMINAL LAW
THEORY AND PRACTICE

INSTITUTE OF CRIMINOLOGICAL
AND SOCIOLOGICAL RESEARCH

JOURNAL OF CRIMINOLOGY AND CRIMINAL LAW

REVIJA ZA KRIMINOLOGIJU I KRIVIČNO PRAVO

Belgrade, 2026

ISSN 1820-2969 (Print)
ISSN 2956-2198 (Online)
UDK 343
DOI 10.47152/rkkp

Publishers
Serbian Association for Criminal Law Theory and Practice,
Kraljice Natalije 45, Beograd
E-mail: sukp@sezampro.rs, Phone number: +381 11 26 58 019

Institute of Criminological and Sociological Research in Belgrade, Gračanička 18
E-mail: krinstitut@gmail.com, Phone number: +381 11 2625-424

Frequency of publishing:
Three times a year.
All articles and papers should be sent via online platform at https://rkkp.org.rs/

Abstract and indexing:
ERIHPLUS
Dimensions
HeinOnline Law Journal Library
Crossref
DOAJ
CEEOL

Financial support
Supported by the Ministry of Science, Technological Development and Innovation of Republic of Serbia

Prepress
Milka Raković

Print
Birograf Comp d.o.o. Beograd

Number of prints
200

Editor in chief
Marina MATIĆ BOŠKOVIĆ, PhD, Institute of Criminological and Sociological Research, Belgrade

Editor
Prof. Božidar BANOVIĆ, PhD, University of Belgrade, Faculty of Security Studies

Editorial Council
Prof. Zoran STOJANOVIĆ, PhD, University of Belgrade, Faculty of Law; Prof. Milan ŠKULIĆ, PhD, University of Belgrade, Faculty of Law; Prof. Vid JAKULIN, PhD, University of Ljubljana, Faculty of Law; Nenad VUJIĆ, minister of Justice of the Republic of Serbia; Prof. Natalija LUKIĆ, PhD, University of Belgrade, Faculty of Law; Prof. Đorđe IGNJATOVIĆ, PhD, University of Belgrade, Faculty of Law; Miroljub TOMIĆ, judge of the Supreme Court of the Republic of Serbia; Academician Igor Leonidovič TRUNOV, PhD, Russian Academy of Sciences in Moscow; Prof. Tatjana BUGARSKI, PhD, University of Novi Sad, Faculty of Law; Prof. Mladen MILOŠEVIĆ, PhD, University of Belgrade, Faculty of Security Studies; Prof. Vojislav ĐURĐIĆ, PhD, University of Niš, Faculty of Law.

Editorial Board
Prof. Stanko BEJATOVIĆ, PhD, University of Kragujevac, Faculty of Law; Prof. Dragana KOLARIĆ, PhD, University of Criminal Investigation and Police Studies, Belgrade; Jasmina KIURSKI, PhD, retired Deputy Republic Public Prosecutor; Prof. Veljko TURANJANIN, PhD, University of Kragujevac, Faculty of Law; Prof. Aleksandra ILIĆ, PhD, University of Belgrade, Faculty of Security Studies; Prof. Dragana ČVOROVIĆ, PhD, University of Criminal Investigation and Police Studies, Belgrade; Prof. Emir ĆOROVIĆ, PhD, Lawyer; Aleksandar TODOROVIĆ, PhD, lawyer; Ivana STEVANOVIĆ, PhD, Institute of Criminological and Sociological Research, Belgrade; Milica KOLAKOVIĆ-BOJOVIĆ, PhD, Institute of Criminological and Sociological Research, Belgrade; Ana BATRIĆEVIĆ, PhD, Institute of Criminological and Sociological Research, Belgrade; Anđela ĐUKANOVIĆ, PhD, Institute of Criminological and Sociological Research, Belgrade; Prof. Zoran PAVLOVIĆ, PhD, Faculty of Law for Commerce and Judiciary in Novi Sad; Prof. Gordana LAŽETIĆ, PhD, Ss. Cyril and Methodius University in Skopje, Faculty of Law "Iustinianus Primus"; Prof. Marina SIMOVIĆ, University of Banja Luka, Faculty of Legal Sciences of "Apeiron"; Chucha Sergey YUREVICH, PhD, Institute of State and Law of The Russian Academy of Sciences in Moscow; Prof. Mohammed AYAT, PhD, Vice President, UN Committee on Enforced Disappearances and member of International Society for Criminology; Prof. Horacio RAVENNA, PhD, School of Social Sciences University of Buenos Aires; Prof. Mario CATERINI, PhD, University of Calabria, Director of the Institute of Criminal Law Studies "Alimena"; Prof. Elizabeta IVIČEVIĆ KARAS, PhD, University of Zagreb, Faculty of Law; Prof. Rok SVETLIČ, PhD, Science and Research Centre Koper; Assoc prof. Mile ŠIKMAN, PhD, University of Banja Luka, Faculty of Security Science; Asst. prof. Yang CHAO, PhD, Beijing Normal University, College for Criminal Law Science; Prof. Angelina STANOJSKA, PhD, University "St. Kliment Ohridski" Bitola, Faculty of Law; Prof. Drago RADULOVIĆ, PhD, University of Montenegro, Faculty of Law; Prof. István László GÁL, PhD, University of Pécs, Faculty of Law; Prof. Shin MATSUZAWA, PhD, Waseda University, School of Law, Tokyo; Prof. Grażyna BARANOWSKA, PhD, Institute of Legal Studies of the Polish Academy of Sciences; Prof. Silvia SIGNORATO, PhD, University of Padua, Faculty of Law.

Editorial Board Secretary
MA Maša MARKOVIĆ, Institute of Criminological and Sociological Research, Belgrade

Editorial Board Technical Secretary
Nada ĐURIČIĆ, PhD, Faculty of Law for Commerce and Judiciary in Novi Sad

JOURNAL OF CRIMINOLOGY AND CRIMINAL LAW

VOLUME 64 / NUMBER 1 / 2026

CONTENT

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.

© 2026 by authors

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

Journal of Criminology and Criminal Law, 64(1), 31-42
Original Scientific Article
https://doi.org/10.47152/rkkp.64.1.2
UDK: 343.95:343.541
343.238

RECEIVED: 19 March 2026
ACCEPTED: 29 April 2026

Application of Bayes' theorem in assessing recidivism risk in a serial rapist: a case study

Valentina Baić[a], Milan Oljača[b], Marija Tasić[c]

The assessment of recidivism risk among sexual offenders represents one of the most challenging issues in criminological and forensic practice, particularly in cases involving multiple repeat offenders, where available data are often fragmentary and the degree of uncertainty is high. The aim of this paper is to demonstrate the application of Bayes' theorem in the analysis of criminal behaviour and in the formalised probabilistic assessment of the risk of rape reoffending through a case study of a serial rapist sentenced to a long-term term of imprisonment. The study is grounded in a Bayesian inferential framework, in which the recidivism hypothesis is operationalised as a binary outcome: the reoccurrence of rape within a three-year period following release (2029–2032). The individualised baseline probability (empirical prior) was estimated using a beta–binomial Bayesian model based on the offender's criminal history, due to the absence of domestic longitudinal recidivism rates for the specified time horizon. The evidence used for Bayesian updating comprised operationalised risk indicators, including repeated rape following previous releases, escalation of violence, the presence of antisocial personality disorder, impulsivity, and stable modus operandi patterns. Additional empirical data from a domestic study on rape recidivism were used to contextualise the findings. The results of the Bayesian analysis indicate that the posterior probability of recidivism within the three-year period remains exceptionally high (≈0.97–0.99), even under conservative assumptions regarding evidential strength. The findings suggest that the potential protective effects of age and long-term imprisonment, even when considered under a conservative scenario, do not outweigh the strong pattern of prior behaviour and the clinical-behavioural risk factors. In conclusion, the paper demonstrates that Bayes' theorem constitutes a methodologically transparent and practically applicable framework for individualised probabilistic reasoning in forensic risk assessment.

KEYWORDS: Bayes' theorem, rape recidivism, risk assessment, serial rapist, case study, forensic reasoning

[a] Full Professor, University of Criminal Investigation and Police Studies, Belgrade.
E-mail: valentina.baic@kpu.edu.rs; ORCID: https://orcid.org/0000-0002-3932-4593

[b] Assistant Professor, Faculty of Philosophy – Department of Psychology, University of Novi Sad.
E-mail: milanoljaca@ff.uns.ac.rs; ORCID: https://orcid.org/0000-0003-4628-4558

[c] Assistant Professor, University of Criminal Investigation and Police Studies, Belgrade.
E-mail: marija.tasic@kpu.edu.rs; ORCID: https://orcid.org/0000-0002-3755-4854

Introduction

Reasoning under conditions of uncertainty represents one of the key methodological challenges of contemporary science, particularly in forensic and criminological research, where decisions are made on the basis of limited, fragmentary, and heterogeneous information. In such a context, probability constitutes a particularly suitable concept for expressing the degree of belief in the truth of specific claims or hypotheses. In Bayesian statistics, it is interpreted as a degree of rational belief based on available information, rather than solely as the frequency of repeatable events (Taroni *et al.,* 2014; Gelman *et al.,* 2014).

This understanding of probability rests on the assumption that conclusions in real-world settings rarely arise from deductive necessity, but rather from plausible reasoning, in which evidence does not permit absolute certainty yet justifies changes in the degree of belief in a given claim. If such changes are required to be logically consistent and to incorporate all relevant data, probability theory may be viewed as a normative framework for rational reasoning under uncertainty (Jaynes, 2003).

The Bayesian approach to statistical inference is grounded in Bayes' theorem, which enables the formal and coherent updating of the probability of a hypothesis in light of new evidence. Within this framework, initial beliefs expressed through prior probabilities are systematically revised as new information becomes available, resulting in posterior probabilities and thereby ensuring a transparent and cumulative process of reasoning (Gelman *et al*., 2014). This approach is particularly well suited to domains characterised by a high degree of uncertainty and the need for individualised assessment, which is typical of forensic practice and the assessment of criminal recidivism risk.

The application of Bayesian reasoning in the assessment of criminal recidivism risk has already been recognised in the contemporary forensic literature. Mokros *et al.,* (2010) demonstrated that multivariate Bayesian classification enables an individually specific probabilistic assessment of violent recidivism risk, whereby combining multiple relevant predictors yields substantially greater predictive value compared with assessments based on single factors. A particular advantage of this approach lies in the explicit incorporation of the base rate of recidivism and the transparent updating of probabilities, which is crucial for informed decision-making in legal and forensic contexts.

Further research indicates that the application of Bayes' theorem is particularly important in the assessment of sexual recidivism risk under conditions of low base rates, where existing actuarial instruments exhibit serious limitations. Wollert (2006) demonstrates that even when discriminatory properties are satisfactory, actuarial models in such populations produce a high proportion of misclassifications and systematically overestimate risk. Under these circumstances, reliance on fixed group probabilities and tabular estimates becomes methodologically limited in individual forensic assessments, whereas the Bayesian framework enables rational and transparent reasoning through the integration of base rates, the evidential strength of available indicators, and the individual characteristics of the case.

This approach is of particular importance in legal and forensic systems in which standardised instruments for recidivism risk assessment and domestic normative guidelines for

their application are lacking. In the Serbian context, recidivism risk assessments are often made in practice without a formalised probabilistic framework, frequently relying on implicit clinical judgement. In this respect, the present paper does not introduce a new form of reasoning through Bayes' theorem, but rather enables the formalisation and transparent presentation of conclusions that are already made under conditions of uncertainty in practice, albeit without a clear separation of assumptions, evidence, and levels of belief.

This study

The aim of this study is to demonstrate the analytical and practical value of the Bayesian inferential framework in assessing criminal recidivism risk within a forensic context. The specific contribution of the paper lies in the formalisation of individual risk assessment under conditions of limited forensic data. The research is based on a detailed analysis of a case study of a serial rapist, in which available empirical and qualitative data are used to formally update the probabilities of relevant hypotheses. Rather than pursuing statistical generalisation, the focus is placed on individualised risk assessment under conditions of limited and fragmentary information.

Such an approach enables an explicit linkage between evidence, theoretical assumptions, and derived conclusions, while clearly distinguishing the inferential process from normative decision-making. In this way, the study illustrates how Bayes' theorem can be applied as a coherent methodological tool in the analysis of complex criminal behaviour under real forensic conditions.

In line with the stated objective, the paper deliberately relies on a limited number of theoretically and methodologically fundamental sources. The rationale for this selection lies in the fact that the aim of the study is not to provide a review of the existing literature on sexual recidivism, but to demonstrate the formal Bayesian framework of reasoning in a specific forensic context. The selection of references was guided by their relevance to the normative and methodological issues of probabilistic reasoning and risk assessment, rather than by the quantity of cited sources.

Consistent with these theoretical and methodological premises, the objective of this paper is to demonstrate the application of Bayes' theorem in the analysis of criminal behaviour and in the assessment of the risk of reoffending for rape, through a case study of a serial rapist sentenced to a long-term term of imprisonment.

Method

Research design

The study is designed as a case study in which a Bayesian inferential framework is applied to assess criminal recidivism risk and to analyse criminal behaviour. The aim of the research is not statistical generalisation to a population, but rather an individualised probabilistic assessment of relevant outcomes for a specific offender under conditions of limited and fragmentary data.

The Bayesian approach enables the transparent updating of the probability of a hypothesis in light of new information and explicitly distinguishes between: (a) initial assumptions (prior), (b) the evidential strength of the available information, and (c) the final posterior estimate. In this paper, the case study is treated as a formal framework for probabilistic reasoning about future behaviour, with clearly acknowledged limitations regarding external validity, rather than as an illustrative narrative.

Data sources

The study draws upon combined data sources:

1. Case study of a serial rapist (Baić and Lajić, 2017), including:

- sociodemographic characteristics,
- criminal history and recidivism pattern,
- modus operandi,
- level of violence, impulsivity, and ritualistic behaviours,
- temporal distribution of the offences.

2. Empirical data from a quantitative study (Baić *et al.,* 2026, in press), used as a reference empirical framework for contextualising the findings and for estimating the prevalence of selected characteristics across relevant groups. The sample comprises 560 individuals convicted of rape, classified into three reference groups:

- CSO-NR – individuals convicted of rape without recidivism,
- CSO-RnR – individuals who reoffended, but not through repeated rape,
- CSO-RR – individuals who repeated the offence of rape.

In the referenced sample, the majority of offenders were non-recidivists, while 12.7% were rape-specific recidivists and an additional 26.3% were recidivists for other criminal offences (Baić *et al*., 2026, in press). These rates are used in the present study for empirical contextualisation and for the selection of variables, but not as the basis for the primary prior, as the aim of the analysis is not population-level estimation but an individually informed risk assessment in an extremely high-risk behavioural trajectory. The aforementioned data were not used to quantify likelihood ratios nor to construct a population prior, but solely to provide theoretical and empirical grounding for the selection of relevant variables within the case study framework.

Hypotheses and operationalisation

The Bayesian analysis is based on the following hypotheses:

- A2(T): The offender will commit rape again within period T following release (after 2029).
- A3: The offender's modus operandi will remain consistent in the event of a subsequent offence.

In the analytical part of the paper, hypothesis A2 is operationalised for a three-year period following release and denoted as A2(3) (2029–2032). The outcome A2(3) is treated as binary (yes/no): the reoccurrence of rape at any point during the specified period.

The primary focus of the study is on hypothesis A2(3), whereas hypothesis A3 is used as a supplementary analytical dimension in interpreting the stability of the criminal behavioural pattern, without being directly incorporated into the quantitative Bayesian updating.

Evidence (B)

The evidence used for Bayesian updating is based on the case study (Baić and Lajić, 2017) and operationalised as a set of indicators:

- B1 (historical recidivism pattern): repeated commission of rape following previous releases, with behavioural escalation;
- B2 (clinical risk): diagnosed antisocial personality disorder, accompanied by pronounced auto-aggressive/suicidal behaviour during imprisonment;
- B3 (behavioural pattern and violence): high level of physical aggression, use of a knife and threats, impulsivity, and a ritualistic component of behaviour.

In light of findings from the reference sample (Baić *et al.,* 2026, in press) indicating that sociodemographic characteristics (e.g., education, employment, marital status) generally do not clearly differentiate rape recidivists from other groups, the Bayesian analysis prioritised historical, clinical, and behavioural risk markers, under the assumption of their limited mutual independence, which is further considered in the model sensitivity discussion.

Bayesian analytical procedure

The analysis was conducted using Bayes' theorem:

$$P(A \mid B) = \frac{P(B \mid A) \cdot P(A)}{P(B)}$$

where:

- P(A) denotes the prior probability of the hypothesis (the initial degree of belief before considering evidence B),
- P(B | A) denotes the probability of the observed evidence given that the hypothesis is true,
- P(B) denotes the overall probability of the evidence,P(A | B) denotes the posterior probability of the hypothesis after taking the evidence into account.

In the practical calculation, the odds form of Bayes' theorem is also used:

$$O(A \mid B) = O(A) \times LR(B)4$$

where:

[4] In the literature, the likelihood ratio may also be denoted as Λ(B) or LA(B). In this paper, the standard notation LR(B) is used, defined as the ratio P(B|A)/P(B|¬A).

$$O(A) = P(A) / (1 - P(A))$$

$$LR(B) = P(B \mid A) / P(B \mid \neg A)$$

The analysis is based on explicitly stated model assumptions, including the choice of the prior and the estimation of likelihood ratios, the sensitivity of which is examined in the interpretative section of the paper.

Results

Defining the prior for hypothesis A2(3) (Individually informed prior)

Given that available domestic sources do not provide longitudinal rape recidivism rates for a clearly defined three-year post-release period, the prior probability of hypothesis A2(3) was derived from the offender's individual criminal history using beta-binomial Bayesian updating.

In the case study, a pattern of repeated rape following three successive prior releases (1999, 2004, 2009) was documented, that is, 3 recidivism events in 3 relevant opportunities. Starting from a weakly informative prior Beta(1,1), the following is obtained:

$$p \sim Beta(1 + 3, 1 + 0) = Beta(4, 1)$$

This posterior beta distribution, obtained relative to the initial weakly informative prior, represents an individually informed prior for the subsequent Bayesian analysis and is based exclusively on the historical evidence of prior releases and repeated offending. It should be noted that the estimate is based on a limited number of observations (n = 3), resulting in a relatively wide posterior variance and requiring methodological caution in interpretation.

For the sake of methodological clarity, it should be emphasised that this posterior beta distribution pertains to the parameter *p* (the probability of recidivism following release) and is derived from the historical record of prior releases and recidivism. It is subsequently used as an informed prior for hypothesis A2(3) in the next stage of Bayesian updating (B1–B3), in the spirit of an empirically informed (empirical Bayes) approach.

The mean of the beta distribution is:

$$E(p) = 4 / (4 + 1) = 0.80$$

The obtained value of 0.80 is interpreted in this study as the informed prior P(A2(3)) for the subsequent Bayesian analysis, rather than as the final posterior probability after incorporating evidence B1–B3.

Bayesian updating of the informed prior with evidence (B1–B3)

To illustrate the Bayesian updating, the odds form was used:

$$O(A2(3) \mid B) = O(A2(3)) \times LR(B)1^{2}$$

[1] In the literature, the likelihood ratio is sometimes denoted using alternative notations, such as $\Lambda(B)$ or $L_A(B)$, where the subscript A explicitly refers to the hypothesis to which the evidence

where:

$$O(A2(3)) = P(A2(3)) / (1 - P(A2(3)))$$

$$LR(B) = P(B \mid A2(3)) / P(B \mid \neg A2(3))$$

Starting from the informed prior P(A2(3))=0.80, the initial odds are:

$$O(A2(3)) = 0.80 / 0.20 = 4$$

Given that B1 represents a highly discriminative piece of evidence, while B2 and B3 further strengthen the clinical-behavioural risk profile, the value of LR(B) was estimated through sensitivity analysis in order to avoid reliance on a single arbitrary point estimate. In this study, evidence B1–B3 is treated as an aggregated evidential set whose overall probative strength is expressed through a single LR(B).

The LR(B) values were selected as a plausible range of evidential strength based on the combined forensic significance of markers B1–B3 and are presented through sensitivity analysis. These values are heuristic in nature and do not constitute direct empirical estimates derived from a single reference study, nor do they purport to represent a point empirical estimate.

Sensitivity Analysis (LR Range)

Three evidential strength scenarios were considered:

- **Conservative**: LR(B) = 8
- **Moderate**: LR(B) = 14
- **High**: LR(B) = 20

The posterior probability was calculated as:

$$P(A2(3) \mid B) = [O(A2(3)) \times LR(B)] / [1 + O(A2(3)) \times LR(B)]$$

(1) Conservative scenario (LR = 8)

$$O(A2(3) \mid B) = 4 \times 8 = 32;\ P(A2(3) \mid B) = 32/33 = 0.9697 \approx 0.97$$

(2) Moderate scenario (LR = 14)

$$O(A2(3) \mid B) = 4 \times 14 = 56;\ P(A2(3) \mid B) = 56/57 = 0.9825 \approx 0.98$$

(3) High scenario (LR = 20)

$$O(A2(3) \mid B) = 4 \times 20 = 80;\ P(A2(3) \mid B) = 80/81 = 0.9877 \approx 0.99$$

Main Finding

Across all three scenarios considered, the posterior probability of hypothesis A2(3) remains exceptionally high, ranging from approximately 0.97 to 0.99. This indicates that, after combining the individually informed prior (based on the historical evidence of re-

pertains. In the present study, the notation LR(B) is retained in accordance with standard forensic statistical practice.

cidivism) with the evidential set B1–B3, the posterior estimate of the probability of rape reoffending in the period 2029–2032 remains very high, within the assumptions of the applied Bayesian model and the examined range of evidential strength.

Discussion

Interpretation of the key finding

The results of the Bayesian analysis indicate that the posterior probability of hypothesis A2(3) that is, the reoccurrence of rape within a three-year period following release (2029–2032) remains exceptionally high and relatively stable, ranging from approximately 0.97 to 0.99, even under conservative assumptions regarding evidential strength, within the assumptions of the applied Bayesian model. This finding derives from the combination of an individually informed prior, based on the offender's criminal history, and strong evidence encompassing repeated commission of the same offence, escalation of violence, and stability of the criminal behavioural pattern, which is consistent with research emphasising the central role of a history of violent behaviour in the assessment of sexual recidivism risk (Hanson and Morton-Bourgon, 2005; Andrews and Bonta, 2010).

It is important to emphasise that the high posterior probability of recidivism obtained in this study does not represent a methodological anomaly, but rather a logical outcome of formal probabilistic reasoning in situations where the available evidence is highly discriminative. Donaldson and Wollert (2008) note that thresholds in the range of 95% to 99% may be justified in contexts where risk assessment carries serious legal and public safety implications, analogous to the standard of "beyond reasonable doubt". In this respect, the Bayesian framework enables a transparent, verifiable, and rational expression of the degree of belief, provided that model assumptions and sources of uncertainty are explicitly stated, in contrast to implicit or intuitive clinical judgements.

In this case, the Bayesian analysis formalises a conclusion that is often reached implicitly in clinical-criminological practice: when a consistent pattern of repeated rape following prior releases is documented in the offender's history, the probability of future recidivism remains high, even in the presence of potentially protective factors. These findings are consistent with a substantial body of literature highlighting the central role of criminal history, stable behavioural patterns, and early onset of violent offending in the assessment of sexual recidivism risk (Hanson and Morton-Bourgon, 2005; Mann, Hanson and Thornton, 2010; Andrews and Bonta, 2017).

The role of individual criminal history in prior formation

A particular strength of this study lies in the manner in which the prior probability of the recidivism hypothesis was defined. In the absence of domestic longitudinal rape recidivism rates for a clearly specified three-year post-release period, the prior was not drawn from the general population nor from aggregated rates of sexual offenders, but was instead derived from the individual criminal history of the specific offender using beta-binomi-

al Bayesian updating. This approach is consistent with the Bayesian principle that prior experiential evidence should be treated as a relevant source of information for the initial probability of a hypothesis (Jaynes, 2003; Gelman *et al*., 2014), while acknowledging the limitations of estimates based on a small number of historical observations.

Such an approach is methodologically justified within a case study framework and accords with the position that Bayesian reasoning is meaningful only when initial probabilities are grounded in relevant and contextually justified assumptions. Donaldson and Wollert (2008) explicitly warn that uncritical reliance on population base rates in forensic contexts may lead to erroneous and normatively problematic conclusions, particularly in the assessment of extreme and high-risk criminal trajectories.

In this respect, the use of population base rates to assess risk in individuals exhibiting stable patterns of severe violent behaviour may result in substantial underestimation of risk. By contrast, reliance on the offender's individual criminal history allows prior behaviour of the same individual to be treated as empirically relevant information about future risk, without uncritical dependence on population averages. This approach is consistent with the principles of structured professional judgement and with contemporary criminological models of criminal careers (Andrews and Bonta, 2010; Douglas *et al*., 2013).

Age, long-term imprisonment, and the limits of the "aging-out" effect

One of the key issues in post-release risk assessment following long-term imprisonment concerns the potential effect of offender ageing ("aging out of crime"). Although theoretical models and part of the empirical literature suggest that age at release and sentence length may function as protective factors with respect to criminal recidivism (Andrews and Bonta, 2010; Lussier, Corrado, and McCuish, 2016), the results of the present analysis indicate that even a conservative reduction of the prior does not lead to a substantial decrease in the posterior probability of recidivism within the examined model and the assumed range of evidential strength.

The reason lies in the strong evidential weight derived from the historical pattern of repeated recidivism, clinical characteristics, and stable behavioural patterns. This finding suggests that the ageing effect is not universal and that, in individuals with prolonged and severe recidivistic trajectories, its impact may be considerably limited, which is consistent with findings from developmental and life-course studies of sexual offending (Hanson and Morton-Bourgon, 2005; Lussier *et al*., 2012).

Demographic variables versus behavioural and dynamic risk factors

Empirical data from the reference domestic study on rape recidivism indicate that sociodemographic characteristics do not clearly differentiate non-recidivists from rape recidivists (Baić *et al*., 2026, in press). This finding is consistent with the results of the Bayesian analysis in the present study, in which the greatest inferential weight was attributed to historical, clinical, and behavioural risk factors rather than to static sociodemographic variables.

Such results further highlight the limitations of actuarial instruments based on group probabilities, particularly with regard to their calibration and applicability to individual cases, as already documented in the international literature on the assessment of violent and sexual recidivism risk (Hanson and Morton-Bourgon, 2009; Rossegger *et al.,* 2014). In forensic and criminal justice contexts, these limitations carry significant implications, as the application of group averages to individual cases may lead to systematic underestimation or overestimation of risk, especially in extreme or atypical criminal trajectories.

Methodological implications of the Bayesian approach

The application of Bayes' theorem in this study demonstrates that the probabilistic framework enables a clear separation between initial assumptions (priors), the available evidence, and their effect on the final risk estimate, thereby increasing the transparency and verifiability of the reasoning process (Jaynes, 2003; Gelman *et al*., 2014). The sensitivity analysis further shows that the principal conclusion remains stable even under conservative assumptions regarding evidential strength, which additionally supports the robustness of the findings and reduces the risk of arbitrary assessment.

The Bayesian approach does not offer the illusion of certain prediction of future behaviour; rather, it enables rational and transparent reasoning under uncertainty, with explicit specification of the degree of belief and the assumptions on which the conclusions rest. This understanding is consistent with contemporary views of forensic probabilistic reasoning, according to which Bayes' theorem constitutes a normative framework for the integration of evidence and risk assessment, rather than a mechanism of deterministic prediction (Donaldson and Wollert, 2008; Taroni *et al.,* 2014).

Limitations of the Study

This study has several important limitations that must be explicitly acknowledged. First, it is a single-case study, which precludes statistical generalisation of the findings to the broader population of sexual offenders. The aim of the research was not generalisation, but rather the demonstration of the methodological framework and inferential logic of Bayesian reasoning in a forensically complex and high-risk case.

Second, due to the lack of domestic longitudinal rape recidivism rates for a clearly defined post-release period, the prior probability was derived from the offender's individual criminal history. This represents a deliberate methodological choice appropriate to a case study design, but it requires caution when interpreting the findings beyond this context, particularly given the limited number of historical observations on which the estimate is based.

Third, the estimation of likelihood ratios (LR) is based on a combination of empirical findings and sensitivity analysis rather than on precise population-level estimates, which further emphasises that the results obtained represent a rational probabilistic assessment rather than empirical proof of future behaviour.

Conclusion

Despite the stated limitations, the results of this study indicate that Bayes' theorem constitutes a methodologically coherent and practically applicable framework for recidivism risk assessment in forensically complex and high-risk cases, within explicitly defined modelling assumptions, which is consistent with contemporary understandings of probabilistic reasoning in the forensic context (Jaynes, 2003; Taroni *et al.,* 2014).

In the present case of a serial rapist, the combination of an individually informed prior, derived from a stable pattern of prior recidivism, and strong evidence encompassing historical, clinical, and behavioural risk factors, indicates that the posterior estimate of the probability of rape reoffending in the period 2029–2032 remains exceptionally high (≈0.97–0.99), even under conservative assumptions regarding evidential strength, with the methodological caveat that the estimate pertains to the specific model and the available evidence. This finding is consistent with empirical research indicating that criminal history and stable patterns of violent behaviour are among the strongest predictors of sexual recidivism (Hanson and Morton-Bourgon, 2005; Andrews and Bonta, 2010; Mann, Hanson and Thornton, 2010).

The Bayesian framework does not replace normative legal decision-making, but it provides a transparent, verifiable, and rational basis for reasoning under uncertainty, with a clear distinction between probabilistic risk assessment and decisions that carry legal consequences, in line with the standards of contemporary forensic expertise (Donaldson and Wollert, 2008; Douglas *et al.,* 2013). In this way, the present study demonstrates that Bayes' theorem is not only mathematically sound, but also a methodologically and normatively grounded framework with significant implications for forensic and criminal justice practice, particularly in contexts where standardised actuarial instruments exhibit limited calibration or reduced applicability to individual cases (Wollert, 2006; Rossegger *et al.,* 2014).

References

Andrews, D. A. and Bonta, J. (2010) *The psychology of criminal conduct* (5th ed.). New Providence, NJ: LexisNexis Matthew Bender. https://doi.org/10.4324/9781315721279

Andrews, D. A. and Bonta, J. (2017) *The psychology of criminal conduct* (6th ed.). New York: Routledge.

Baić, V. and Lajić, O. (2017) 'Analysis of the criminal behavior of multiple perpetrators of the crime of rape', *NBP – Journal of Criminalistics and Law*, *22*(1), 33-51. https://doi.org/10.5937/nabepo22-13316

Baić, V. *et al.* (2026) 'Recidivism of rapists: A retrospective analysis of static and dynamic risk factors', *Teme (in press).*

Donaldson, T. and Wollert, R. (2008) 'A mathematical proof and example that Bayes's theorem is fundamental to actuarial estimates of sexual recidivism risk', *Sexual Abuse: A Journal of Research and Treatment, 20*(2), 204-226. https://doi.org/10.1177/1079063208317734

Douglas, K. *et al.* (2013) *HCR-20V3: Assessing risk for violence – User guide.* Burnaby, BC: Mental Health, Law and Policy Institute, Simon Fraser University.

Gelman, A. *et al.* (2014) *Bayesian Data Analysis* (3rd ed.). Boca Raton, FL: Chapman & Hall/CRC.

Hanson, R. K. and Morton-Bourgon, K. E. (2005) 'The characteristics of persistent sexual offenders: A meta-analysis of recidivism studies', *Journal of Consulting and Clinical Psychology, 73*(6), 1154-1163. https://doi.org/10.1037/0022-006X.73.6.1154

Hanson, R. K. and Morton-Bourgon, K. E. (2009) 'The accuracy of recidivism risk assessments for sexual offenders: A meta-analysis of 118 prediction studies', *Psychological Assessment*, *21*(1), 1-21. https://doi.org/10.1037/a0014421

Jaynes, E. T. (2003) *Probability theory: The logic of science*. Cambridge University Press.

Lussier P., Corrado R. R. and McCuish E. (2016) 'A criminal career study of the continuity and discontinuity of sex offending during the adolescence-adulthood transition: A prospective longitudinal study of incarcerated youth', *Justice Quarterly*, *33*(7), 1123-1153. https://doi.org/10.1080/07418825.2015.1028966

Lussier P. *et al.* (2012) 'A developmental taxonomy of juvenile sex offenders for theory, research, and prevention: The adolescent-limited and the high-rate slow desister', *Criminal Justice and Behavior*, *39*(12), 1559-1581. https://doi.org/10.1177/0093854812455739

Mann, R. E., Hanson, R. K. and Thornton, D. (2010) 'Assessing risk for sexual recidivism: Some proposals on the nature of psychologically meaningful risk factors', *Sexual Abuse: A Journal of Research and Treatment, 22*(2), 191-217. https://doi.org/10.1177/1079063210366039

Mokros, A. *et al.* (2010) 'Assessment of risk for violent recidivism through multivariate Bayesian classification', *Psychology, Public Policy, and Law, 16*(4), 418-450. https://doi.org/10.1037/a0020939

Rossegger, A. *et al.* (2014) 'Replicating the Violence Risk Appraisal Guide: A total forensic cohort study', *PLoS ONE, 9*(3), e91845. https://doi.org/10.1371/journal.pone.0091845

Taroni, F. *et al.* (2014) 'Bayesian reasoning in forensic science', *Forensic Science International, 235*, 1-9. https://doi.org/10.1016/j.forsciint.2013.11.017

Wollert, R. (2006) 'Low base rates limit expert certainty when current actuarials are used to identify sexually violent predators: An application of Bayes's theorem', *Psychology, Public Policy, and Law, 12*(1), 56-85. https://doi.org/10.1037/1076-8971.12.1.56

© 2026 by authors

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

Journal of Criminology and Criminal Law, 64(1), 43-66
Review paper
https://doi.org/10.47152/rkkp.64.1.3
UDK: 341.49

RECEIVED: 5 December 2025
ACCEPTED: 20 January 2026

Historical development of international criminal courts

Darko Radulović[a]

This paper deals with the historical development of international criminal courts. The need for the establishment of an international criminal court has always been tied to armed conflicts and wars in which the most severe crimes had been committed - and the entire international community would be interested in the trials - so international justice would not be served if the adjudication was carried out by national courts. Beside a short introduction, the work is divided into four parts. The first part covers the period before World War Two, the second encompasses the period after World War Two, where the emphasis is put on the Nuremberg and Tokyo ad hoc tribunals, the third part is dedicated to the International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia (the Hague Tribunal) and the International Criminal Tribunal for Rwanda, whereas the fourth part addresses the permanent International Criminal Court. The establishment of the permanent International Criminal Court is undoubtedly one of the most significant events in the history of international criminal law. The creation of the last global institution of the 20th century implied at last the materialisation of the almost hundred-year-old idea of the establishment of a supernational court within whose jurisdiction would be the most severe international crimes.

KEYWORDS: International criminal law, court, crime, jurisdiction, proceedings, trial

[a] Assistant Professor, Faculty of Law in Podgorica, University of Montenegro.
E-mail: darko77@t-com.me; ORCID: https://orcid.org/0000-0002-7806-0973

Introductory remarks

What is especially important in the historical development of international criminal law is the issue of the historical development of international criminal courts as its significant constituents. On this path of development, two most significant issues - inextricably linked to each other - stand out. These include, on one hand, the codification of international criminal law, and on the other, the establishment of international criminal courts (Čejović, 2006, p. 50). The United Nations' efforts to form a permanent criminal court can, too, be followed in two aspects: the codification of the matter of international crimes and the work on drafting the statute of an international court (Cassese, 2005. p. 393; Bassiouni, 1998, p. 10). It is important to note here that international criminal justice did not develop in a straight line, and that its development could instead be followed in connection to some court or para-court cases and in certain historical circumstances, primarily linked with concrete wars and armed conflicts (Škulić, 2005, p. 25). These historical circumstances and the differentiation between the winning and the losing side in war were of vital importance when it comes to who would stand trial, whether there would be a trial at all and how the proceedings would be conducted. This is why it is difficult to talk about a single planned and continuous development of international criminal courts, let alone to say that since the very beginnings of the trials there already used to be an idea of the establishment of universal international criminal law and justice. We could rather say that this was a spontaneous process which mostly depended on the context of certain historical circumstances and relations among the political powers at the international level, with a prominent feature of all these processes: all of them, usually, came down to the winners of a war prosecuting the defeated (Škulić, 2005, p. 25). The literature states that the history of international criminal law - and of international criminal courts within its scope - is a history of political influence on its shaping and application, although this is the only obstacle for which science claims it had a twofold impact on international criminal law: as much as it is a burden for international criminal law, political influence is also necessary for its existence and activity (Ristivojević, 2012, p. 161).

Victor's justice could hardly be regarded as impartial and unbiased, insomuch as it could be universal in the application of law. We hope that there will be a breakthrough with the adoption, i.e. the acceptance of the Rome Statute on the establishment of the permanent International Criminal Court, regardless of the fact that its application is complementary in relation to the criminal legislation of the member states.

The idea of the formation of a single international criminal court has been present for a long time - it dates back to the 19th century - and it is the expression of an understanding of international courts as a means for the resolution of international disputes. The biggest obstacle to the embodiment of this notion was the concept of sovereignty as the basic characteristic of countries which prevented their subjugation to any government outside of their own borders (Milojević, 1997, p. 91). Having in mind the bumpy development of international criminal law and international criminal justice - we have observed on this path both periods of delay and periods of growth - the historical de-

velopment of international criminal courts shall be followed through several periods: 1) period before World War Two, 2) period after World War Two (Nuremberg and Tokyo ad hoc tribunals), 3) Hague Tribunal and Tribunal for Rwanda and 4) permanent International Criminal Court.

Period before World war two

Even though it is often stated how the history of international criminal justice began after World War Two, it should be said that the idea of the establishment of some kind of an international court emerged much earlier, as an expression of the need to sanction severe violations of humanitarian law. The roots of the laws of armed conflict and humanitarian law date back to Ancient History, where historical sources tell about crimes of such proportions which could be qualified as genocide today. In that context, there is the Roman destruction of Carthage and the slaughter of its inhabitants, then the Biblical description of the slaughter of the Canaanites after the Jews conquered Jericho and other events (Josipović, Krapac, Novoselec, 2001, p. 13). Parallel with the endeavour to humanise war, as the ultimate and inhumane means of conflict resolution, the idea evolved to create an appropriate judicial body with the task of establishing the criminal liability of persons who committed crimes in war. In that sense, during the Hundred Years' War (1337–1453), an idea came from the pope about a criminal court which would be competent for the prosecution of the perpetrators of the most gruesome crimes committed during wartime (Jovašević 2012, p. 112; Đurđić, Jovašević, 2003, p. 115). However, the first activities of such a court were recorded only in the 15th century. Namely, following the unprecedented crimes against the civil population in Breisach in 1474, the citizens of Breisach formed a multinational court comprising 28 judges, i.e. eight from said place and two from each of the surrounding regions (Alsace, Germany and Switzerland) where the Duke of Burgundy, Peter von Hagenbach, was put on trial, as the person responsible for the committed crimes "against natural law and the transgression of the laws of God and man," and was given a death sentence which was later carried out indeed (Bring, 2001, p. 12).

This trial - from the perspective of the criminal law standards of today - could hardly be called an international crime trial, but, as the literature points out, it certainly has a certain historical significance and it anticipated certain questions which play a highly important role in contemporary criminal law as well, especially in regard to superior orders, individual criminal responsibility and command responsibility (Škulić, 2005, p. 29).

The idea to establish a unique international criminal court is ascribed to the founder of the International Red Cross, the Swiss Gustave Moynier, who - horrified by the atrocities of the Franco-Prussian War - submitted in 1872 a proposal to the International Committee for Relief to the Wounded for the creation of an international court whose council would comprise five judges (one from each warring country and three from neutral countries). For that purpose, he prepared the draft rules of the International Criminal Court in 1878, whose jurisdiction would encompass the offences prescribed

by the Geneva Conventions of 1864 (Lombois, 1971, p. 23). This idea, like many before it, regardless of its noble nature, was not implemented, but there was a permanent effort in the commitment of individuals and professional institutions to bring the idea to fruition: the establishment of a permanent international criminal court. Obstacles that were in the way of implementing the idea to establish a permanent international criminal court were put there by the most influential countries which either refused to give their consent or avoided the ratification of already concluded treaties which provided for the establishment of such courts. The same fate befell the Hague Convention XII on the establishment of the International Prize Court in 1907, which was supposed to be a court of appeals against the judgments of national courts regarding the capturing of enemy property, i.e. the first-instance court if national courts would fail to resolve a case in two years. To make all this more absurd, all credit for the unsuccessful ratification of the Convention goes to the countries which got the main judicial positions in the court: Austria-Hungary, Germany, Russia, England, Japan and Italy (Radulović, 1999, p. 40).

The beginning of the 20th century brought new ideas aimed at the establishment of an international criminal court (Rascmany, 2001, pp. 608-625). A modified concept of warfare, radicalised to a terrifying extent, with the use of the latest technical achievements, often without a real military need, mobilised the international community to come up with a way and to find the resources to combat this evil (Palević, 2001, p. 195). Thus, following the end of World War One, at the Supreme Council Conference held on 4 December 1918 in London, England, France and Russia agreed to put the German Emperor Wilhelm II and a large number of accomplices, both military personnel and civilians, on trial before an international court. For that purpose, the so-called Commission of Fifteen was established at the Paris Peace Conference of 1919, whose task was to analyse all the materials and submit a report to the Conference. Because of the great powers' opposing opinions, the question of the above persons' responsibility became even more obscure, so Article 227 of the Treaty of Versailles of 28 June 1919 prescribed that "the Allied and Associated Powers publicly arraign William II, German Emperor, for a supreme offence against international morality and the sanctity of treaties." Despite the fact that Article 229 of the Treaty provided for the possibility to establish an international criminal tribunal, where each power would appoint one member, this didn't happen and the courts of the interested countries were pronounced competent. The Dutch government refused to extradite Wilhelm II who went into exile in the Netherlands following the abdication of 8 November 1918 (the Netherlands were not a party to the Treaty of Versailles). In doing so, it invoked two grounds: first, the offences for which his extradition was requested were not envisaged by the treaties which the Netherlands had with other countries and second, that the Netherlands, according to the legislation and tradition of the country, has always granted asylum to those defeated in international conflicts (Ignjatović, 1996, p. 46). Such a position of the Dutch government has been regarded as disputable, to say the least, because this concrete case deals with the obligations of a member of the international community towards that very community, and not with the relationship between individual countries on the basis of bilateral treaties on legal assistance (Vasili-

jević, 1968, p. 15). The only trial of war criminals whose guilt was significantly less severe in comparison to that of Wilhelm II was held before the Supreme Court in Leipzig, but only six persons were convicted in this trial (as many as the number of those who were exonerated), even though the Allies had compiled a list of 896 perpetrators.

Regardless of the poor results of the Treaty of Versailles regarding the delivery of justice, its importance must not be underestimated, because it emphasised several significant principles of international criminal law. In the first place, there is the emphasis on individual criminal responsibility, and not just the responsibility of the state as a legal entity, then the notion that war criminals should not only be tried before national courts, but also before the courts of those countries where the crimes had been perpetrated, and even before an international court if such court is formed, and finally that a person's position and function do not justify the crimes committed.

The question of the establishment of an international court was relevant even after the end of World War One because of the exceptional work of the League of Nations (as the predecessor of the United Nations Organisation), since Article 14 of the League's Covenant demanded the establishment of an international criminal court, which was also supported by professional organisations in the field of criminal law. However, these activities didn't result in either the formation of a separate international criminal court or the extension of the competences of the Permanent Court of International Justice so they could encompass criminal matters. Consequently, the Allies' attempt to sanction the persecution and murder of more than six hundred thousand Armenians in Turkey failed, despite the recommendation of the Committee formed by the Allies in 1919 to prosecute and punish the persons responsible for these actions. There was no prosecution because the USA was opposed with the explanation that crimes against humanity had not been recognised by international law at the time when these acts were committed. The Treaty of Sèvres, concluded on 10 August 1920 between the Allies and Turkey, which laid the basis for the establishment of criminal responsibility, was never ratified, whereas the Treaty of Lausanne of 1923 granted amnesty to Turkey (Radulović, 1999, p. 41).

Following the assassination of King Alexander I of Yugoslavia and of the French Foreign Minister Louis Barthou in Marseille in 1934, an expert committee appointed by the League of Nations prepared two draft conventions. One was aimed to prevent and combat terrorism, while the other referred to the establishment of an international criminal court against terrorism which would enforce the former Convention. Great Britain objected to the establishment of the court, with the excuse that the preconditions for that had not yet been met.

In addition, international professional associations such as the International Law Association, the International Association of Penal Law and others, which brought together the leading figures of the time (Bellot, Pella, Caloyanni), pushed for the establishment of a permanent international criminal court, but the implementation of this idea had always been thwarted by non-legal reasons. Politics is the culprit for the obstruction of these ideas, so the literature points out that all global - and especially European - policies,

along with historical circumstances, were dominantly responsible for the fact that "until a new end, a new world war and a new division between the victors and the vanquished" no trial for international crimes could proceed, i.e. there was no practical application of international criminal law, which represents another very illustrative indicator of the direct impact of international and political factors and of the real balance of power among countries on the situation in the field of international criminal law (Škulić, 2005, p. 36).

Period after World war two (Nurenberg and Tokyo Tribunals)

The unprecedented atrocities committed by the Nazis in World War Two prompted the four great powers (the USA, Great Britain, the Soviet Union and France) to establish, through the London Charter of 8 August 1945, the International Military Tribunal in Nuremberg before which the highest ranking war criminals of the European Axis countries would stand trial. This act was preceded by the Declaration regarding the defeat of Germany of 5 June 1945 (signed on 8 May in Reims), which also contained provisions on punishment for war crimes. In a similar fashion, for the crimes perpetrated in the Far East, by the decision of the commander of U.S. Army Forces in the Far East, General Douglas MacArthur, the International Military Tribunal for the Far East was formed on 19 January 1946, with its seat in Tokyo. The establishment of this court was preceded by the Potsdam Declaration of 1945, by which the representatives of the above stated four powers decided how Japanese offenders will be punished in addition to the Nazi criminals of Germany. It should also be noted that the issue of punishing war criminals had an important place at the meetings of the state and government leaders of the Allies even before the London Charter was concluded. So, already in 1942, the Allied Forces signed a declaration in St. James's Palace in London establishing the UN War Crimes Commission composed of seventeen representatives of the respective countries. This Commission compiled a list of 8,178 cases (files) about persons who had been suspected of the most severe international crimes committed during the war, as well as a list of crimes by 750 Italian war criminals, committed in Ethiopia during the short war starting from 1935 (Jovašević, 2012, p. 114).

The Moscow Declaration of October 1943, signed by the Governments of the United States, the Soviet Union and Great Britain, stipulates that war criminals would be tried in those countries where they committed their crimes according to the laws of said countries, while criminals who had no special geographical localisation would be tried on the basis of a special decision of the Allied Forces (United Nations, Collection of Documents 1941-1945, Second Edition, Belgrade, 1947). Shortly thereafter, at the conferences of the Big Three (the President of the US, the British Prime Minister and the Leader of the Soviet Union) held in Tehran from 28 November to 1 December 1943, in Yalta from 4 to 11 February 1945 and in Potsdam from 17 July to 2 August 1945, it was agreed that the major German war criminals need to be put on trial (Smith, 1982, p. 120).

And, as we have stated above, these decisions (conferences) were embodied in the signing of the London Charter by the great-power victors on 8 August 1945, which established

the International Military Tribunal to which the Charter of the International Military Tribunal was annexed, for the trial of war criminals whose offences have no particular geographical location. Regarding those crimes for which the International Military Tribunal was not competent, the proceedings against their perpetrators were regulated by Law No. 10 of the Control Council for Germany which was adopted on 20 December 1945. These crimes came under the jurisdiction of zone courts (Germany was divided into four zones: American, Soviet, British and French) and of German courts authorised for adjudication. It is interesting that there were proposals (coming from Great Britain) that, after Germany's defeat, it was sufficient to capture and execute (on summary conviction) those who were primarily responsible for the creation and enforcement of the Nazi policy and that no time should be spent on legal proceedings, while lower-ranking war criminals should be tried before specially established tribunals (Smith, 1982, pp. 31-35). The Americans did not agree with this, and were backed by the Soviets, so the International Military Tribunal was formed in order to establish guilt for offences which had no particular geographical localisation. Several reasons were stated in favour of the position to resolve even the most severe crimes before a court and not on summary conviction. First, although the victors are putting the defeated on trial, this must be done through legal proceedings, because resolving a crime without a trial would negate the basic rule that no one shall be held guilty until proven guilty in a fair trial. Otherwise, they would resemble the Nazis, who often killed innocent people on summary conviction. Second, facing the Nazi crimes before the Nuremberg Tribunal would have a strong effect on the global public opinion, so the gruesome crimes of the Nazi state could be witnessed by all of mankind. The third reason for the resolution of Nazi crimes before the International Military Tribunal arose from the desire of the Allied Forces to do something for posterity, because the crimes committed by the Third Reich and its Nazi officials were so heinous that some trace had to be left about them. This could be achieved through a court trial, which was also envisaged as a way to compose a file of historical documents which would have disappeared had the Tribunal not been formed, and consequently would not have been able to serve as a history lesson for future generations (Cassese, 2005, p. 389).

The International Military Tribunal convened in Nuremberg from 20 November 1945 to 1 October 1946 and this was the first time in history that a judgment was passed and sanctions imposed by an international court for crimes against peace, war crimes, crimes against humanity and for participation in the preparation or execution of a common plan or conspiracy for the accomplishment of said crimes. Out of a total of 22 defendants, 12 were sentenced to death by hanging, three to life imprisonment, four received prison sentences ranging from 10 to 20 years, while three were acquitted. These trials brought the individual responsibility for international crimes to the fore, which some believe is the greatest legacy of the Nuremberg Trials (Mettraux, 2011, p. 5).

The trial of Japanese war criminals commenced on 28 April 1948 in Tokyo. Twenty-five accused ministers, diplomats and military leaders were brought before the tribunal, five of which were sentenced to death, sixteen to life in prison and two received 7 and 20 years in prison, respectively.

Regarding the accused associations, i.e. organisations, the Nuremberg Tribunal pronounced the following as criminal: Nazi Party leadership, Gestapo and SS (independent Nazi Party units).

The work of the Nuremberg and the Tokyo Tribunals didn't have any major differences. One difference, for example, was the fact that the Tokyo Tribunal could not pronounce some organisation as criminal, and the period under the jurisdiction of this court was longer.

After World War Two, international criminal law was implemented on multiple levels: the highest level of implementation was before the Tribunals in Nuremberg and Tokyo, where major military and political leaders were tried, the medium level covered trials before Allied military tribunals in the occupation zones of Germany and before US military tribunals in the Far East, while the lowest level included trials before the national tribunals of individual states (Bassiouni, 2005, p. 119).

The experience after World War One demonstrated how international justice can be compromised because of political needs, whereas the experience following World War Two showed the opposite: how efficient 'international' justice can be when there is an appropriate political will and necessary resources (Cassese, 2005, p. 391). However, it should be stated that even during the Nuremberg Trials, and afterwards, opinions were divided on many questions connected to the Charter and the trials (Heller, 2011, pp. 107-138).

The importance of the London Charter and the Charter of the International Military Tribunal as its integral part, observed from its legal perspective, lies in the fact that this was the first document in the field of international criminal law which entered into force and had certain legal effects. The ruling of this tribunal represents the technical finish of what had been prepared for decades and the most important step towards the punishment of perpetrators of the most severe international crimes (Milojević, 2012, p. 46). This broke the 'monopoly' on criminal jurisdiction in the most severe criminal cases which had thus far been vested in national courts. The literature contains opinions that the Nuremberg and Tokyo Tribunals were not international (but tribunals of the winners instead), nor were they independent, because in their proceedings they were following the instructions of the countries which had appointed the judges (Krivokapić, 2007, p. 44). Appointing judges from neutral countries to the tribunals - as was proposed by prominent names of that time, such as Hyde and Kelsen - would have contributed to their better impartiality and objectivity (Ristivojević, 2012, p. 163). There are opinions that these trials would have been even more significant had the Allies mustered the strength to make persons from their own environment stand trial as well, since there were those among them who could have been charged with certain international crimes, for it is almost impossible to deny the criminal nature of the bombing of civilians, near the end of the war at that (Škulić, 2012, p. 134).

Among other things, there are remarks about the disproportionate, and even frantic bombing of Hamburg (1943) and Dresden (1945) by British and American forces, not to mention the bombing of Hiroshima and Nagasaki at the very end of the war when, as the

literature points out, Japan had already been on the brink of collapse (Krivokapić, 2012, p. 45). Although the opinion prevails that these were military tribunals established by the victorious great powers, where the judges were military personnel subject to military discipline, there are contrary views as well. So, we can find the opinion that this was not an international, but rather an inter-Allied tribunal, which on top of that wasn't of a military nature, because the judges, as well as their deputies - except for the Soviet representatives - were civilians, and what also allows the possibility of contesting the 'military' nature is the fact that not all defendants were members of the military, while some crimes they were charged with weren't primarily military crimes (Degan, Pavišić, 2005, p. 10).

Various arguments are given in defence of the international character of the International Military Tribunal. In that sense, it is underlined that the foundation for that tribunal had already been laid in the Atlantic Charter of 14 August 1941 which provided for the punishment of war criminals, followed on 1 January 1942 by the United Nations Declaration which confirmed the readiness of all nations gathered in the democratic coalition to restore peace and to completely recover "human rights and justice" (Marković, 1965, p. 30). In addition, the fact that the London Charter was signed by nineteen countries (Vasilijević, 1971, p. 68), and that the General Assembly adopted the principles recognised by the Charter and by the ruling of the Nuremberg Tribunal entirely and without reservations, confirms the international character of this tribunal (Glaser, 1958, p. 630).

The criticism expressed during the trials by the defendants, and later voiced by theoreticians, came down to several issues, such as the issue of the legal basis for the responsibility for crimes against peace, then the retrospective application of the law, which implies the violation of the known principles of criminal law nullum crimen sine lege, nulla poena sine lege, etc. (Marković, 1973, p. 424).

Notwithstanding any objection to the tribunals in Nuremberg and Tokyo which claims that these supported victor's justice, and that they breached the principle of legality, these trials undoubtedly had their justification and were a much better solution than treating the defeated on summary conviction (Kittichaisaree, 2001, p. 20 in relation to Stojanović, 2006, p. 172). The Charter of the Tribunal and the Nuremberg ruling promoted certain principles of international criminal law such as:

1. individual criminal responsibility for international crimes,
2. the fact that internal law does not impose a penalty for an act which constitutes a crime under international law does not relieve the person who committed the act from responsibility,
3. the fact that a person who committed an act which constitutes a crime under international law acted as Head of State or responsible government official does not relieve him from responsibility under international law,
4. the fact that a person acted pursuant to order of his superior does not relieve him from responsibility under international law, provided a moral choice was in fact possible to him,

5. any person charged with a crime under international law has the right to a fair trial on the facts and law,
6. the crimes hereinafter set out are punishable as crimes under international law:
   a) crimes against peace,
   b) war crimes,
   c) crimes against humanity.
7. complicity in the commission of these crimes is also a crime.

The United Nations General Assembly Resolution 95 (I) of 11 December 1946 confirmed the principles of international law recognised by the Charter of the International Military Tribunal and by the ruling of that Tribunal, which is the best evidence of their importance and international significance. The literature states that, from a practical perspective, the Nuremberg and Tokyo trials paved the road for the establishment of new international tribunals, both ad hoc ones and the permanent International Criminal Court (Krivokapić, 2012, p. 41).

Ad Hoc Tribunals for ther Former Yugoslavia and Rwanda

The tribunals in Nuremberg and Tokyo were ad hoc tribunals which fulfilled their mission and dissolved, but they were the bridge for the establishment of one universal international court. The overall efforts of both individuals and international organisations following World War Two were directed towards establishing a permanent international criminal court and no one even thought about forming new ad hoc tribunals. In that sense, there were proposals as to how to accomplish the creation of such a court. So, building upon the fact that the rule nullum forum sine lege applies both to the forming of international courts and to the forming of national courts, there were three options to establish this court: establishment through a review of the UN Charter, by a UN General Assembly Resolution and by an international treaty (Janković, 1957, p. 55). The advantages and shortcomings of each of these routes to a permanent international criminal court were discussed at length. And when it was just a matter of time when a permanent international criminal court would be established, following numerous preparatory activities, especially by the International Law Commission, the United Nations Security Council Resolution 827 of 25 May 1993 established the International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia (the Hague Tribunal). This demonstrated that a tribunal can be formed and a prosecution initiated even in cases when a military conflict has no winning and losing side (Crien et al., 2010, p. 133). A little over a year since the establishment of the Hague Tribunal, the Security Council Resolution 955 of 9 November 1994 established an ad hoc tribunal for Rwanda. The adoption of the Resolution on the establishment of the Hague Tribunal, which also implied the adoption of the Statute of the Tribunal, was preceded by a series of acts:

a) United Nations Security Council Resolution 780 of 6 October 1992 tasking the UN General Secretary with establishing an impartial Expert Commission to analyse the information "on serious violations of the Geneva Conventions and humanitarian law" in the territory of the former Yugoslavia.

b) General Secretary's Report to the Security Council (S/25274) of 10 February 1993, compiled on the basis of the Expert Commission's work on the violation of humanitarian law.

c) United Nations Security Council Resolution 808 of 22 February 1993 by which the General Secretary was requested to submit within 60 days a report on all aspects of the potential establishment of a tribunal and possible other options.

d) Finally, the General Secretary's Report (S/25704) of 3 May 1993 on the basis of which the Resolution on the establishment of the Hague Tribunal was adopted (Avramov, 1994, p. 443).

Since the very establishment of the Hague Tribunal, many questions were disputable and were met with different answers both among the professional and the general public. The primary disputable question was that of the legal grounds for the establishment of the Tribunal, i.e. whether Chapter VII of the UN Charter to which the Security Council refers gives the latter the authorisation to establish such an institution, whether it thereby assumes the competences of the 'legislative branch'. Furthermore, whether the tribunal can be a subsidiary organ to the Security Council in the context of Article 29 of the UN Charter, to what extent it can be independent and autonomous considering the manner of appointment of the tribunal's judges, how much it can contribute to restoring peace and preserving security, etc.

That the matter was not legally clear could be seen during the preparation of the Statute, because the already mentioned Resolution 808 of 22 February 1993 did not state the legal grounds and manner of establishment of the tribunal. Besides, in the already mentioned report (S/25704) of 3 May 1993, the General Secretary states: "The approach which, in the normal course of events, would be followed in establishing an international tribunal would be the conclusion of a treaty by which the States parties would establish a tribunal and approve its statute. This treaty would be drawn up and adopted by an appropriate international body (e.g., the General Assembly or a specially convened conference), following which it would be opened for signature and ratification."

Although the Resolution establishing the Hague Tribunal was adopted unanimously by the Security Council, the representatives of China, Brazil and Mexico made remarks regarding the legal grounds for its formation (Kokolj, 1995, p. 17; Matić, 1997, p. 477). The most heated discussion and the most divided opinions in the literature were generated by the issue of the legal basis of the Resolution on the establishment of the Tribunal. Before we set forth the differing opinions on this matter, we shall quote Article 29 of the UN Charter which prescribes that "The Security Council may establish such subsidiary organs as it deems necessary for the performance of its functions." Chapter VII of the Charter (Articles 39 to 51) is titled "Action with Respect to Threats to the Peace", and it

refers to the activities of the Security Council. Pursuant to Article 39 of the Charter, the Security Council is authorised to determine the existence of any threat to the peace and to take measures to restore peace and security in accordance with Articles 41 and 42 of the Charter. The measures prescribed by Article 41 exclude the use of armed force, and may be complete or partial interruption of economic relations and of rail, sea, air, postal and other means of communication, and the severance of diplomatic relations. Should the Security Council consider that these measures would be inadequate or have proved to be inadequate, it may take, pursuant to Article 42 of the Charter, such action by air, sea, or land forces as may be necessary to maintain or restore peace and security.

From the above quoted provisions, it can be concluded that the Security Council may form subsidiary organs to perform tasks and take actions within the competences of the Security Council, including those for the restoration of peace and security; that these measures are taken towards states, and not towards individuals. This is why the establishment of a tribunal, be it a permanent or ad hoc tribunal, as stated in the literature, cannot represent an enforcement measure for the preservation or restoration of peace (Radulović, 2000, p. 10). It is stated that the Security Council could even rather dissolve some country's parliament or dismiss some head of state if it deems that this country poses a threat to the peace, than establish a criminal tribunal (Stojanović, 1997, p. 26). The international justice system which was in force at the global level prior to the establishment of the Hague Tribunal was the product of contractual relations, because a tribunal's contractual character is an important precondition for the enforcement of sanctions and - what is most important for tribunals - the contractual character of tribunals in the international community is a guarantee that they will not be under the control of a single country, or a group of countries, but independent and impartial forums instead (Avramov, 1994, p. 454). Besides, in his Report S/25704 of 3 May 1993, the UN General Secretary points out how the real approach in establishing an international tribunal would lead through the conclusion of a treaty, which would have to be signed by the countries, but at the same time he expresses doubts that this would require a long period of time, and there is also no guarantee that the countries would ratify the treaty. Therefore, he proposes a (legally dubious) shortcut in which the Security Council would establish a tribunal with reference to Chapter VII of the UN Charter and this approach, as stated by the General Secretary, would have the advantage of being expeditious and of being immediately effective as all States would be under a binding obligation to take whatever action is required to carry out a decision taken as an enforcement measure under Chapter VII of the UN Charter (Račić, 1997, p. 54). For the purpose of preserving peace and security, the Security Council may take various measures, including measures of a legal nature, but it cannot establish a tribunal, because the notion of a tribunal cannot be equated with the notion of a measure (Čavoški, 1998, p. 24), since this would on one hand be logically absurd, and on the other, it is in a certain way offensive to the judicial function which has a general moral significance as well (Škulić, 2005, p. 54).

Article 29 of the UN Charter does not state which types of subsidiary organs the Security Council may form, but the question is posed whether a judicial body can be

a subsidiary organ in the sense of the above Article. Subsidiary organs perform tasks within the competences of the principal organ for the purpose of efficiency and expeditiousness in certain situations, but such organs, by their nature, are not and cannot be independent, nor can they act autonomously, but only under the instructions of and within the mandate given by the principal organ (Security Council).

If the principal organ does not have a judicial function—and according to the Charter, the Security Council doesn't have one—then the subsidiary organ cannot have such a function either, because it has been known since Roman times that one cannot transfer to another more rights than he has. The nature of the Hague Tribunal, as has been stated in the literature, does not correspond to the role of a subsidiary organ of the Security Council, because the judicial function cannot be a subsidiary function - in national as well as international law - but rather a form of power, independent of other forms of power (Đorđević, 1997, p. 157; Milisavljević, Palević, 2010, p. 278). There are opinions that there is no need to delve into the discussion of this matter from a legal perspective, because this is a political solution to political problems placed before the Security Council at a specific moment of time (Stojanović, 1999, p. 8).

Unlike the previously voiced opinions, there are also opposite viewpoints according to which the Security Council is authorised to establish a tribunal for the purpose of the preservation of peace and security (Vasilijević, 1997, p. 399; Paunović, 1997, p. 126), and the fact that Article 41 of the Charter does not explicitly provide for criminal prosecution measures does not mean that the authors of the Charter wanted to limit the Security Council regarding the choice of measures which are considered the most adequate and appropriate to the situation (Obradović, 1994, p. 13). It is further added that the Hague Tribunal is both legally grounded and credible to serve international justice (Pocar, 2010, p. 67). Additionally, the establishment of an international criminal tribunal by a Security Council resolution obliges all UN members, which could not be achieved if the tribunal was established by contractual means (Bantekas, Nash, 2007, p. 514). Some support the opinion of the General Secretary, expressed in the above mentioned Report of 3 May 1993, that the International Tribunal is established with reference to Chapter VII of the UN Charter as a subsidiary body for the performance of its tasks, because in the criminal and political context, this manner of establishing a tribunal is much more expeditious, not just in comparison to the contractual establishment of a tribunal, but also in comparison to a decision adopted by the General Assembly (Krapac, 1995, p. 23). The critics of this position state that references to criminal and political reasons cannot be valid in this case, and the matter of expeditiousness has no legal significance in this case, because the criterion of the need for swift action cannot compensate for the legal fallacies of a certain decision (Škulić, 2005, p. 53). Some justify this shortcut in the establishment of the Hague Tribunal by the fact that it can hardly be expected of national courts to prosecute and punish war criminals, so if the Tribunal was to be formed contractually, that would (strictly speaking) satisfy the law, but justice would be sacrificed, thereby negating the maxim - acknowledged since the time of Cicero - that the welfare of the people should be the supreme law (Aćimović, 1997, p. 197).

Article 92 of the UN Charter states that the International Court of Justice is the principal judicial organ of the United Nations, which - according to some opinions - points to the possibility of the existence of other UN judicial organs as well, among which the International Court of Justice would be the 'principal' one (Etinski, 2001, p. 158). It follows from the foregoing that the Security Council may establish an ad hoc tribunal, but not a permanent international criminal court (Degan et al., 2011, p. 477). Therefore, the International Court of Justice is the principal judicial organ of the UN, the successor of the Permanent Court of International Justice formed in 1921, and this court is, inter alia, competent to provide advisory opinions to the UN General Assembly or the UN Security Council on all legal matters, which is why the literature contains criticism as to why the Security Council didn't request this court's opinion before the establishment of the Hague Tribunal (Etinski, 2001, p. 157; Antić, 2002, p. 137). It is further added that the main protagonists of the establishment of the Hague Tribunal shied away from the court's opinion and, instead of striving towards the creation of a permanent international criminal court, whose jurisdiction would be limited neither in terms of time nor space, steps were taken to establish individual ad hoc tribunals, whose selection primarily depends on the leading powers in the Security Council (Đorđević, 1996, p. 4).

What can be said after these discussions on the legality of the Hague Tribunal? It is a fact that, in international trials, both factual and legal questions are extremely complex (Cassese, 2003, p. 398). Although there are disagreements regarding the legal basis of the decision on the establishment of this tribunal, no one disputes the imperative to punish war criminals in the territory of the former Yugoslavia, because that is the sacred duty of organised international justice. The question is posed: if there wasn't a permanent International Criminal Court already in place, what would have happened if the Hague Tribunal wasn't formed and if the national courts were entrusted with the prosecution of war criminals, or if the trial had to wait until the establishment of the permanent International Criminal Court (Boas, 2011, p. 52). Being aware of the circumstances in the countries of the former Yugoslavia, we believe that those who were charged before the Hague Tribunal would rarely be tried before the national courts. They might have even occupied important positions in their social and working environments. Besides, as far as we know, none of those who were charged before the Hague Tribunal had previously been charged with those crimes in their respective countries. Having all this in mind, irrespective of the fact that ad hoc tribunals cannot be freed from political influences, reasons of justice nevertheless justify the establishment of this tribunal, or in plain words: we are better off even with the Hague Tribunal than without it. History has shown that the trials of war criminals are always torn between legality and legitimacy, where legitimacy usually prevails.

What also faced criticism is Article 15 of the Statute of the Hague Tribunal, because this Article gave the tribunal 'legislative' authority as well, since it authorised it to adopt the Rules of Procedure and Evidence, which it did in February 1994, by adopting said rules which were amended on several occasions, even during proceedings, despite the fact that courts do not have the power and authority to create rules, but only to interpret

or apply them (Đorđević, 1995, p. 562). On the other hand, the criminal law provisions, as stated in the literature, do not have a constitutional character, but a declarative one, because they only confirm what had earlier been promoted by the Nuremberg principles and appropriate conventions (Kambovski, 1998, p. 389).

The Rwanda Tribunal was established by a Security Council resolution a little over a year after the establishment of the Hague Tribunal. Although it has many similarities with the Hague Tribunal, it is also specific in some ways, regarding the following: the manner in which it was established, its competences, the circumstances in which this tribunal operates and so on (Krivokapić, 1997, p. 79; Radulović, 1999, p. 166). Having in mind the limited space at our disposal, we shall in short outline the differences between these two tribunals. The Rwanda tribunal was established upon the request of the Government of Rwanda, albeit not the one which started the war, but the one which was the victim of genocide. As a result of the circumstances, Rwanda was at the time a non-permanent member of the Security Council, and even though it initiated the tribunal's establishment, it voted against (China abstained), because it reckoned that the Tribunal would be controlled by the Government in Rwanda, and also because it feared that it could be abused by those countries which supported the previous regime.

The jurisdiction of the tribunal (temporal, spatial and subject-matter) was defined differently than in the Statute of the Hague Tribunal. Articles 1 and 7 of the Statute of the Tribunal for Rwanda limit the temporal jurisdiction to the period from 1 January 1994 to 31 December 1994, i.e. to only one calendar year. The territorial jurisdiction is wider than is the case with the Hague Tribunal and spans not only the territory of Rwanda, but also the territory of neighbouring countries in regard to the serious violations of international humanitarian law committed by Rwandan nationals. The subject-matter jurisdiction has also been regulated differently. Article 3 of the Statute of the Tribunal for Rwanda, which defines crimes against humanity, does not require these crimes to be "committed in an armed conflict, international or internal in character", but it explicitly prescribes that crimes against humanity shall only be those acts which were "committed as part of a widespread or systematic attack against any civilian population on national, political, ethnic, racial or religious grounds." Since it began, the war in Rwanda has been treated as a civil war, so the competences of this Tribunal could not include serious violations of the provisions of the 1949 Geneva Conventions, since these are related to conflicts of an international character. Another difference between these two tribunals is the fact that prison sentences can be served in Rwanda as well, apart from the countries which have expressed their readiness to accept the convicts. Despite the stated differences between these two ad hoc tribunals, they have a common prosecutor and a common appeals chamber. This is, perhaps, an expression of the need for ensuring a certain degree of uniformity in the enforcement of international criminal justice.

Permanent International Criminal Court

The establishment of the International Criminal Court has been the long-standing idea of many individuals and professional organisations in the field of international criminal law. At the international level, it was first expressed in a normative manner in the Convention on the Prevention and Punishment of the Crime of Genocide of 9 December 1948, and was implemented fifty years later, on 17 July 1998, when the Statute of the International Criminal Court was adopted and opened for signature and ratification at the diplomatic Conference in Rome. The placement of the most severe international crimes within its jurisdiction is an expression of the belief that such crimes are contrary to the vital interests of the international community, and that justice cannot be served by relying on national jurisdictions only. The reasons why the formation of such a court had to wait for so long should primarily be sought in the lengthy and laborious process of creating a favourable international legal and political environment, because the political circumstances in the world had for a prolonged period of time not been inclined towards the implementation of this idea, because of the obstructions of some of the main actors in international relations. This is why it was easier to resort to the establishment of ad hoc tribunals with limited temporal and spatial jurisdictions, even though the International Criminal Court has significant advantages compared to ad hoc tribunals.

Apart from cost-efficiency reasons, the establishment of a single permanent court eliminates the influence of the Security Council - and thereby of the great powers - in assessing whether it is purposeful (in the political sense) to establish a tribunal in a concrete situation. In addition to that, the establishment of a permanent court whose Statute prescribes the crimes within its jurisdiction, the criminal sanctions which are imposed for such offences and the rules of procedure and evidence, leaves no room for discussions on the legality of the act, punishment and procedure, which ad hoc tribunals were criticised for, starting from the Nuremberg to the Hague tribunals (Radulović, 1999, p. 172). The literature states that, among other things, experiences gathered in the work of ad hoc tribunals had an influence on the establishment of the permanent International Criminal Court (Stojanović, 2006, p. 187; Cassese, 2005, p. 402; Babić, 2011, p. 193; Boas et al., 2011, p. 39). It is also added that the permanent International Criminal Court should rather be regarded as the beginning of the development of new international criminal law and new international legal practices, and not as some final product of previous experiences and previous case law (Škulić, 2005, p. 157). The principal body for the establishment of the permanent International Criminal Court following World War Two was the International Law Commission (ILC) founded by the UN General Assembly. This Commission even prepared draft Statutes in 1951 and 1953, but because of the situation regarding international relations, and because of the great powers' lack of interest, further work on these documents never materialised. This issue was reopened only in 1992 when the General Assembly requested that the Commission prepare a draft Statute of the permanent International Criminal Court, which the latter did and submitted to the General Assembly in 1993 the draft Statute which would soon, in 1994, be

revised after the suggestions and remarks of the governments of certain countries had been received. Later, the General Assembly established an ad hoc committee which concluded in 1995 that work on the Statute's text should be continued simultaneously with the preparations for the diplomatic Conference, which was also supported by the Sixth Committee (Legal) of the General Assembly. Afterwards, the General Assembly decided to establish the Preparatory Committee for the purpose of preparing the diplomatic Conference and adopting the final version of the Statute. The diplomatic Conference was held in Rome, from 15 June to 17 July 1998, and it adopted the Statute and established the permanent International Criminal Court, presenting it to the countries for ratification. The Rome Statute entered into force on 1 June 2002 after it had been ratified by sixty countries. The establishment of the permanent International Criminal Court was also supported by many international and regional organisations, starting from the European Union, to the Non-Aligned Movement (McGoldrick, 2004, p. 391).

This short overview of the activities en route to the establishment of the permanent International Criminal Court shows that it all implied many difficulties and evolved slowly, and the reason lies in the strong reluctance of governments to relinquish a part of their sovereignty in the field where they have always wished to maintain their exclusive internal jurisdiction. In that sense, the literature states that the field of criminal law is tightly connected to the sovereignty of a state, where this sovereignty is also reflected in the state's exclusive jurisdiction for offences committed in its territory (Crawford, 1995, p. 405).

At the diplomatic Conference which was held in such a complicated situation burdened by differing interests of individual countries, the Statute of the Court was adopted, which represents the result of difficult compromises made for the purpose of finishing the Conference's work. Credit goes, among others, to a group of prominent diplomats, and especially Canada's Philippe Kirsch, Chairman of the Committee of the Whole (Cassese, 2005, p. 404). Prior to the adoption of the final text of the Statute, three groups of countries could be distinguished during the work of the Preparatory Committee and at the diplomatic Conference. The first group, led by Canada and Australia, included countries which came forward with a proposal supporting a quite powerful court with wide and 'automatic jurisdiction', with an independent prosecutor who would be authorised to initiate proceedings before the court and a comprehensive definition of war crimes, including those committed in internal armed conflicts. The second group comprised permanent members of the Security Council. This group was against 'automatic jurisdiction' and the prosecutor's right to initiate proceedings, and it urged that the most important tasks be given to the Security Council, where it would be authorised to forward cases to the court for resolution, as well as to prevent the forwarding of cases to the court. They were opposed to the crime of aggression being listed among the crimes within the court's jurisdiction, and claimed that the use of nuclear weapons cannot be considered as a violation of humanitarian law, for which the court would also be competent. The third group mainly consisted of members of the Non-Aligned Movement which were against the Security Council having any role in connection to the court, and

promoted the inclusion of the crime of aggression among the crimes envisaged by the Statute. Some countries from this group proposed that the crimes of drug trafficking and terrorism be placed under the court's jurisdiction (Cryer, 2010, p. 147; Cassese, 2005, p. 403). Even after the Cold War ended, the threat to the peace remained because of international and internal conflicts, so the Security Council's influence on the work of this court could not have been excluded (White, Cryer, 2009, p. 455).

One of the most important questions for every court, including the International Criminal Court, is the question of its jurisdiction, and especially subject-matter jurisdiction. The basic subject-matter jurisdiction of this court is limited to the most serious crimes of concern to the international community as a whole. So, Article 5 of the Statute prescribes that the Court has jurisdiction with respect to the following crimes: a) the crime of genocide; b) crimes against humanity; c) war crimes; and d) the crime of aggression. Article 5 paragraph 2 of the Statute adds that the Court shall exercise jurisdiction over the crime of aggression once a provision is adopted in accordance with Articles 121 and 123 of the Statute (the provisions are related to the possibility of submitting and adopting amendments to the Court's Statute, as well as the possibility of its review) defining the crime and setting out the conditions under which the Court shall exercise jurisdiction with respect to this crime, provided that such a provision must be consistent with the relevant provisions of the Charter of the United Nations. The reasons for postponing the 'effective' jurisdiction of the Court for the crime of aggression are primarily of a political nature, because the issue of defining aggression is a highly sensitive one and, according to some opinions, the majority of other crimes against humanity and international law arise from a prior act of aggression (Škulić, 2005, p. 346).

A definition of aggression in international law was provided by the UN General Assembly in 1974 by the Resolution 3314-XXIX according to which aggression is the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, but the question was posed whether this definition of aggression could be applied to individual criminal responsibility. Twelve years after the adoption of the Statute of the permanent International Criminal Court and eight years after its entry into force, at the Review Conference of all signatories of the Statute held in Kampala (Uganda) from 31 May to 11 June 2010, the definition of aggression was adopted. So, the crime of aggression implies the planning, preparation, initiation or execution by a person, in a position effectively to exercise control over or to direct the political or military action of the State, of an act of aggression whose character, severity and scope constitute a manifest violation of the Charter of the United Nations (Simović et al., 2013, p. 426). Even when dealing with these most serious crimes, pursuant to Article 1 of the Statute, it is prescribed that the International Criminal Court shall be complementary to national jurisdictions and it is primarily up to the states to prosecute the perpetrators of the crimes referred to in Article 5 of the Statute, and if they fail to do so, then the International Criminal Court shall take over. This means, the principle of complementarity is of great importance for the operation of the International Criminal Court, because that principle, among other things, manifests itself as one of the key differences in relation to

ad hoc tribunals (Škulić, 2020, p. 64). One of the key reasons for the increasing reliance on national courts lies in the problems faced by the International Criminal Court, which is primarily because it does not have its own executive force or police (Vuletić, 2025, p. 337). This confirmed the basic rule of international law on national sovereignty, but the question arises whether the court will be able to fulfil its mission because of the efforts of states to preserve their sovereignty in the judicial branch as well (Çakmak, 2017, p. 213). Article 21 of the Statute prescribes which legal sources will be applied, with the note that the application and interpretation of the law pursuant to this Article must be consistent with internationally recognised human rights (Zeegers, 2016, p. 64).

Despite all efforts to eliminate the Security Council's influence on the work of the Court, this was not avoided, for the Security Council was authorised to initiate proceedings before the International Criminal Court, even without the limitations which apply in case a signatory state or a prosecutor initiate proceedings before the Court. In addition to this, maybe the Security Council's greater influence on the work of the Court was expressed in the provision of Article 16 of the Statute according to which the UN Security Council has the right, acting on the basis of Chapter VII of the UN Charter, to request the Court to defer an investigation or prosecution for a period of twelve months (Sanooshi, 2004, p. 110). This leaves room for the great powers - even if they become signatories to the Rome Statute - to avoid the prosecution of their citizens, even more so because the Security Council may repeat its request under the same conditions.

Conclusion

In the historical development of international criminal law, two issues stand out as the most significant. On the one hand, this concerns the codification of international criminal law, and on the other hand, the establishment of the International Criminal Court. Bearing in mind the history of warfare and wars, as well as the division into victors and the defeated, it is difficult to speak of a planned and continuous development of international criminal justice. However, the idea of establishing an International Criminal Court is an old one and was particularly pronounced in the twentieth century. Obstacles to the establishment of a permanent International Criminal Court were created by the most influential states, either by withholding consent or by avoiding the ratification of already concluded treaties. Instead of a permanent international criminal court, ad hoc tribunals were established, beginning with the International Military Tribunal for the trial of Nazis after the Second World War. Regardless of the objections raised against the tribunals in Nuremberg and Tokyo, these trials had their historical justification and promoted some of the most important principles of international criminal law.

And when it was believed that these would be the first and last ad hoc tribunals, as predecessors of a permanent International Criminal Court, the Hague Tribunal was established to prosecute war crimes committed in the territory of the former Yugoslavia. We have previously indicated all the controversial issues related to this tribunal, starting

with the questionable legal basis for its establishment, and here we merely emphasise that justice was not served through the proceedings before the Hague Tribunal, or rather that it was, to a significant extent, selective. The establishment of ad hoc tribunals represented an intermediate step toward the creation of a permanent International Criminal Court, which occurred at the Diplomatic Conference in Rome in 1998. The establishment of this court was met with a certain sense of relief and with expectations that it would achieve universal justice and that perpetrators of the most serious international crimes would be adequately sanctioned. In addition, it was expected that the existence of this court would have a preventive effect and serve as a serious warning to those who believe that by committing grave international crimes, they could evade punishment. Although more than twenty years have passed since the entry into force of the Rome Statute, the practice of the International Criminal Court remains very limited, despite the fact that wars and armed conflicts are taking place across the globe. This has led to disappointment among many, resulting in scepticism regarding the Court's ability, through its activities, to manifest the idea of universal justice and to exert a preventive influence on potential perpetrators of criminal offences. The future of this Court will depend on how the major powers relate to it, that is, whether they will accede to the Rome Statute. Unfortunately, the opposite process is occurring, with some states withdrawing from membership in this institution. Likewise, the future of the Court is also being called into question by the revival of the idea of establishing ad hoc tribunals, including those proposed for events in Ukraine.

References

Aćimović, Lj. (1997) 'Od ad hoc tribunala ka stalnom međunarodnom krivičnom sudu', *Jugoslovenska revija za međunarodno pravo,* 2-3, 193-199.

Antić, O. (2002) 'Antinomije Haškog tribunala', *Prava čovjeka,* 1-2, 128-145.

Avramov, S. (1994) 'Međunarodno krivično pravo i Povelja Ujedinjenih nacija', *Anali Pravnog fakulteta u Beogradu, 42*(5), 479-499.

Babić, M. (2011) *Međunarodno krivično pravo.* Banja Luka: Pravni fakultet u Banjaluci.

Bassiouni M.C. (2005) *The legislative history of the International Criminal Court.* Ardsley. https://doi.org/10.1163/9789004480124

Bassiouni M. C. (1998) *The Statute of the International Criminal Court - A documentary History.* New York, Ardsley: Transnational Publishers.

Bantekas, I., Nash, S. (2007) *International Criminal Law*. Third edition. London and New York: Routledge - Cavendish (Taylor i Francis Group).

Boas, G. *et al.* (2011) *International Criminal Procedure*. New York: Cambridge University Press.

Bring, O. (2001) *International Criminal Law in Historical Perspective - Comments and Material.* Stockholm: Juridiska Fakulteten.

Çakmak, C. (2017) *A Brief History of International Criminal Law and International Criminal Court.* Eskisehir Osmangazi University. New York: Springer Nature. https://doi.org/10.1057/978-1-137-56736-9

Cassese, A. (2003) *International Criminal Law*. Oxford University Press.

Crawford, J. (1995) 'The ILC Adopts a Statute for International Criminal Court', *American Jurnal of International Law*, 2, 404-416. https://doi.org/10.2307/2204214

Cryer, R. *et al.* (2010) *An Introduction to International Criminal Law and Procedure.* Cambridge University Press.

Čavoški, K. (1998) *Hag protiv pravde.* Beograd: IKP Nikola Pašić.

Čejović, B. (2006) *Međunarodno krivično pravo*. Beograd: Dosije.

Čučilović, I. (2025) 'Može li međunarodni krivični sud da „preživi" oružane sukobe u Ukrajini i Gazi?', *Izazovi međunarodnog krivičnog prava i krivičnog prava*. Beograd: Udruženje za međunarodno krivično pravo, 457-480. https://doi.org/10.51204/zbornik_umkp_25121a

Degan, Đ., Pavišić, B. (2005) *Međunarodno krivično pravo*. Rijeka.

Degan, Đ., Pavišić, B., Beširević, V. (2011) *Međunarodno i transnacionalno krivično pravo.* Beograd: Pravni fakultet Union i Službeni glasnik.

Đorđević, S. (1995) 'Međunarodno sudstvo - problemi i predlozi', *Pravni život,* 12, 561-577.

Đorđević, S. (1996) 'Međunarodno sudstvo i Jugoslavija', *Sudska praksa*, 1-2, 3-10.

Đorđević, S. (1997) 'Međunarodni krivični tribunal za prethodnu Jugoslaviju', in: Taboroši, S. (ed.) *Međunarodna krivičnopravna pitanja i Haški tribunal*. Beograd: Pravni fakultet u Beogradu, 157-177.

Đurđić, V., Jovašević, D. (2003) *Međunarodno krivično pravo.* Beograd: Nomos.

Etinski, R. (2001) 'Pojava specijalizovanih tribunala i pitanje ujednačene primjene međunarodnog prava', *Jugoslovenska kriza, pouke za* međunarodno pravo, 155-178.

Glaser, S. (1958) 'Les controverses du Droit international penal', *Revue de droit penal et de criminologie*, 6.

Heller, K. J. (2011) *The Nurnberg Military Tribunals and the Origins of International Criminal Law.* https://doi.org/10.1093/acprof:oso/9780199554317.001.0001

Ignjatović, A. (1996) *Genocid u međunarodnom i nacionalnom krivičnom pravu.* Beograd: Novinsko-izdavačka kuća-Vojska.

Janković, B. (1957) 'Osnivanje međunarodnog krivičnog suda', *Godišnjak Pravnog fakulteta u Sarajevu,* 47-75.

Jovašević, D. (2012) 'Principi međunarodnog krivičnog prava', in: Lopičić-Jančić, J. (ed.) *Od Nirnberga do Haga - pouke istorije.* Beograd: Beogradski forum za svet ravnopravnih.

Josipović, I., Krapac, D., Novoselec, P. (2001) *Stalni međunarodni krivični sud.* Zagreb: Narodne novine i Hrvatski pravni centar.

Kaseze, A. (2005) *Međunarodno krivično pravo*. Beograd: Beogradski centar za ljudska prava.

Kambovski, V. (1998) *Međunarodno kazneno pravo*. Skoplje: Prosvetno delo.

Kokolj, M. (1995) 'Međunarodni krivični sud za prethodnu Jugoslaviju (kome se sudi u Hagu)'. Beograd: Centar Marketing.

Krivokapić, B. (1997) 'Međunarodni krivični tribunal za Ruandu', *Jugoslovenska revija za međunarodno pravo*, 1, 73-89.

Krivokapić, B. (2012) 'Putevi i stranputice međunarodnih krivičnih sudova', in: Lopičić-Jančić, J. (ed.) *Od Nirnberga do Haga - pouke istorije*. Beograd: Beogradski forum za svet ravnopravnih.

Krivokapić, B. (2007) 'Razvoj međunarodnog krivičnog sudstva', *Strani pravni život*, 1-2, 39-61.

Krapac, D. (1995) *Međunarodni sud za ratne zločine na području bivše Jugoslavije*. Zagreb: Hrvatski Helsinški odbor za ljudska prava, Hrvatski pravni centar.

Lombois C. (1971) *Droit penal international*. Dalloz.

Marković, M. (1965) 'Međunarodna krivična dela', *Jugoslovenska revija za međunarodno pravo,* 1, 29-53.

Marković, M. (1973) 'Nirnberško suđenje, primena novih načela u međunarodnom krivičnom pravu', *Zbornik Instituta za kriminološka i sociološka istraživanja*, 2, 173-201.

Metraux, G. (2011) 'Trial at Nirnberg', in: Shabas, A.W. and Bernaz, N (eds.) *Routledge Handbook of International Criminal Law.* London and New York: Routledge (Taylor i Francis Group). https://doi.org/10.4324/9780203836897

Milisavljević, B., Palević, M. (2010) 'Razvoj međunarodnog humanitarnog prava, promenjena uloga oružanih sukoba i uloga ad hoc tribunala', *Pravni život*, 12, 265-283.

Milojević, M. (1997) 'Osnivanje međunarodnog krivičnog suda', in: Taboroši, S. (ed) *Međunarodna krivičnopravna pitanja i Haški tribunal*. Beograd: Pravni fakultet u Beogradu, 91-124.

Mitić, M. (1997) 'Odnos država prema Međunarodnom tribunalu za gonjenje lica za ozbiljne povrede međunarodnog humanitarnog prava na teritoriji bivše Jugoslavije, in: Taboroši, S. (ed) *Međunarodna krivičnopravna pitanja i Haški tribunal.* Beograd: Pravni fakultet u Beogradu, 145-162.

McGoldrick, D. (2004) *Political and Legal Responses to the ICC*. The Permanent International Criminal Court (Legal and Policy Issues). Portland: Hart Publising. https://doi.org/10.5040/9781472562944.ch-014

Obradović, K. (1994) 'O pravnoj osnovi konstituisanja ad hoc Međunarodnog krivičnog suda za bivšu Jugoslaviju', *Glasnik Advokatske komore Vojvodine*, *66*(10), 3-16. https://doi.org/10.5937/gakv9410003o

Palević, M. (2001) 'Istorijski razvoj međunarodnog krivičnog sudstva', *Zbornik radova Pravnog fakulteta u Prištini*, 1, 191-201.

Paunović, M. (1997) 'Međunarodni krivični tribunal za teške povrede međunarodnog humanitarnog prava na području bivše Jugoslavije', in: Taboroši, S. (ed) *Međunarodna krivičnopravna pitanja i Haški tribunal*. Beograd: Pravni fakultet u Beogradu, 125-144.

Pocar, F. (2010) *The International Criminal Justice (Law and Practice from the Rome Statute to Its Rewie)*. England: Ashgate Publising Limited.

Račić, O. (1997) 'Međunarodni sud i ovlašćenja Savjeta bezbjednosti: od savetodavnog mišljenja o Namibiji do slučaja Lockerbie', *Anali Pravnog fakulteta u Beogradu*, 1-3, 39-67.

Radulović, D. (2000) 'O legalitetu i legitimitetu Međunarodnog ad hoc tribunala u Hagu', *Jugoslovenska revija za kriminologiju i krivično pravo,* 1-2, 3-21.

Radulović, D. (1999) *Međunarodno krivično pravo*. Podgorica: Kulturnoprosvjetna zajednica.

Rascemany, Z.D. (2001) 'The Nationality of the ofender and the jurisdiction of the International Criminal Court', *The American Journal of International Law, 95*(3), 606-623, https://doi.org/10.2307/2668495

Ristivojević, B. (2012) 'Od Nirnberga do Rima preko Haga: Međunarodno krivično pravosuđe između prava i politike,' in: Lopičić-Jančić, J. (ed.) *Od Nirnberga do Haga - pouke istorije*. Beograd: Beogradski forum za svet ravnopravnih.

Sanooshi, D. (2004) 'The Peace and Justice Paradox: The International Criminal Court and the UN Security Council', in: McGoldrick, D, Rowe, P. and Donnelly, E. (eds) *The Permanent International Criminal Court (Legal and Policy Issues).* Portland: Hard Publishing, 95-120. https://doi.org/10.5040/9781472562944.ch-004

Simović, M. *et al.* (2013) *Međunarodno krivično pravo*. Sarajevo: Pravni fakultet u Istočnom Sarajevu.

Smith, Bradley F. (1982) *The American Road to Nurnberg - the Documentary Record 1944-1945*. Stanford, Calif.: Hoover Institution Press.

Stojanović, Z. (2006) *Međunarodno krivično pravo*. Beograd: Pravna knjiga.

Stojanović, Z. (1997) 'Međunarodni krivični sud, sukob prava i politike', *Jugoslovenska revija za kriminologiju i krivično pravo, 1*, 23-40.

Stojanović, Z. (1999) 'Ad hoc tribunal za bivšu Jugoslaviju i međunarodno krivično pravo', *Pravo - teorija i praksa*, 1, 8-14.

Škulić, M. (2005) *Međunarodni krivični sud*. Beograd: Pravni fakultet u Beogradu.

Škulić, M. (2012) 'Neke poruke suđenja u Nirnbergu', in: Lopičić-Jančić, J. (ed.) *Od Nirnberga do Haga - pouke istorije*. Beograd: Beogradski forum za svet ravnopravnih.

Škulić, M. (2020) 'Imaju li budućnost međunarodno krivično pravo i međunarodni krivični sud', in: Ignjatović, Đ. (ed) *Kaznena reakcija u Srbiji X deo*. Beograd: Pravni fakultet u Beogradu, 36-82.

Vasilijević, V. (1971) 'Suđenje pred Međunarodnim vojnim sudom u Nirnbergu i razvoj međunarodnog krivičnog prava', *Jugoslovenska revija za međunarodno pravo*, 3, 305-334.

Vasilijević, V. (1997) *Međunarodni krivični tribunal za prethodnu Jugoslaviju i kažnjavanje za teške povrede međunarodnog humanitarnog prava*. Beograd: Humanitarno pravo.

Vasilijević, V. (1968) *Međunarodni krivični sud*. Beograd: Institut za kriminološka i sociološka istraživanja.

Vuletić, I. (2025) 'Je li budućnost međunarodnog kaznenog prava nacionalna: osvrt na dosadašnji rad Međunarodnog kaznenog suda', *Izazovi međunarodnog krivičnog prava i krivičnog prava.* Beograd: Udruženje za međunarodno krivično pravo, 331-340. https://doi.org/10.51204/zbornik_umkp_25113a

Zeegers, K. (2016) *International Criminal Tribunals and Human Rights Law (Adherence and Confextualization)*. Amsterdam: Springer. Available at: https://link.springer.com/book/10.1007/978-94-6265-102-9. https://doi.org/10.1007/978-94-6265-102-9

White, N., Cryer, R. (2009) 'The ICC and the Security Council: An Uncomfortable Relationship', *The Legal Regime of the International Criminal Court*. Leiden – Boston: Martinus Nijhoff Publishers. 455-484. https://doi.org/10.1163/ej.9789004163089.i-1122.127

© 2026 by authors

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

Journal of Criminology and Criminal Law, 64(1), 67-82
Review paper
https://doi.org/10.47152/rkkp.64.1.4
UDK: 343.85
334.728:351.749

RECEIVED: 29 September 2025
ACCEPTED: 12 January 2026

The Role of Private Security in Crime Prevention

Jana M. Marković[a]

Contemporary security risks have led to the need for additional capacities that would support traditional institutions of formal control, primarily the police. In this context, the private security sector has assumed a significant role, not only in the protection of people and property, but also in proactive measures aimed at crime prevention in various social environments such as public spaces. For a long time, the central place in crime prevention was held by the police as a traditional, specialized subject of formal social control. However, numerous challenges faced by the public sector, including bureaucratization, an increase in crime, limited capacities, the burden of tasks, and high costs, contributed to the expansion of the role of private entities in the protection of people and property, i.e., control of criminal behavior, and led to a process that is often called 'privatization of security' in the literature, in which private entities take over tasks that traditionally belonged to public institutions. The paper starts from the assumption that private security actively contributes to the preservation of public security and investigates its evolving and increasingly complex role in crime prevention. The primary goal of the paper is to point out the significant role of private security in crime prevention, as well as to identify and interpret the key areas through which this role is realized in practice.

KEYWORDS: crime prevention, private policing, private security, public space

[a] Assistant professor, Faculty of Security Studies, University of Belgrade.
E-mail: jana.markovic@fb.bg.ac.rs; ORCID: https://orcid.org/0009-0003-0676-8213

Introduction

Over time, with urbanization and technological development, the security environment has become complex, making traditional public security models face significant challenges in terms of capacity and operational efficiency. In this context, private security is becoming a provider in the preservation of public order, especially in domains that include crime prevention. One study found that respondents believed that private security plays an important role in maintaining law and order in society, that it is as important as public police, and even that it should play a more significant role in public police work (Steenkamp, 2002, p. 52). Research also indicates that private security services are highly valued and relevant to public safety, and that their presence has significantly increased the effects of security (Stajić, 2015; Oyebambi, 2024).

To deal with the role that private security plays in crime prevention, it is first necessary to clarify what the concept of crime prevention entails. Being secure today means knowing vulnerabilities and taking measures to address those vulnerabilities. Starting from the fact that different entities participate in crime prevention, in the second part of the paper, special emphasis is placed on private security as one of those actors, which is in accordance with the theme of the paper. In this context, the process of the so-called privatization of security and the development of the concept of private police, i.e., private security, are discussed, with a more detailed definition of that term. By analyzing the activities that private security provides or can provide, attention is gradually directed towards the key issue of this work – the role of private security in crime prevention. This analysis does not mean only listing the existing services and tasks of private security, but aims at a deeper understanding of how it contributes to the general security environment. Formulating an answer to the above-mentioned issue is one of the main goals of the work, as it opens up space for further theoretical and practical reflection on the role and importance of private security in modern society.

Crime prevention

The history of crime prevention spans more than 200 years, and its basic principles still largely shape our preventive action today (Crawford and Evans, 2017, p. 798). Crime prevention, as a term, was first used in 1829 in the *Book of Instructions for the Metropolitan Police in London*, where it is stated that it is the first task of the police (Davidović, 2015, p. 346; Gilling, 1997, p. 1).

Van Dijk defined crime prevention as "the total of all policies, measures and techniques, outside the boundaries of the criminal justice system, aiming at the reduction of the various kinds of damage caused by acts defined as criminal by the state" (1990, p. 205). This definition includes the fear of crime that occurs as a consequence of crime, but also the policy of helping victims due to the consequences suffered. Similarly, Lab defines it in such a way that it "entails any action designed to reduce the actual level of crime and/or the perceived fear of crime" (2014, p. 27). Such a definition indicates that the actions taken are not limited to the efforts of the criminal justice system, but also include the activities of individuals and groups, both public and private. Crime prevention can be understood

basically as "the use of all means and measures aimed at preventing the occurrence of some form of crime" or "the use of all measures and means, for the mobilization of individuals, social groups, organizations and institutions, aimed at preventing those phenomena that are not in accordance with criminal legislation, and which by their essence cause harm to individuals, social groups or society as a whole" (Krivokapić, 2008, pp. 42-43).

Analyzing the literature on crime prevention, Gilling points out that the authors distinguish between situational and social prevention. The first focuses on "the management, design and manipulation of the built physical environment, to reduce the opportunity for crime to be committed and increase the risk of detection if deterrence fails", while the second seeks to "change criminal motives, which are seen to lie in people, not things, in the social environment". Authors like van Dijk or Graham and Rosenbaum introduce an additional form - community crime prevention, which includes a mixture of social and situational approaches, applied by individuals or groups (1997, pp. 5-7).[1] From the perspective of this study and the role of private security, situational crime prevention is of particular relevance, as it focuses on reducing opportunities and physical conditions conducive to criminal activity.

At the global level, there is a definition of crime prevention provided by the United Nations in the Crime Prevention Guide. In it, crime prevention includes "strategies and measures that seek to reduce the risk of crimes occurring, and their potential harmful effects on individuals and society, including fear of crime, by intervening to influence their multiple causes" (ECOSOC, 2002). At the level of the European Union, crime prevention is determined in the context of the elements that it should cover, which are: "all measures that are intended to reduce or otherwise contribute to reducing crime and citizens' feeling of insecurity, both quantitatively and qualitatively, either through directly deterring criminal activities or through policies and actions designed to reduce the potential for crime and the causes of crime". Furthermore, the subjects, "government, competent authorities, criminal justice agencies, local authorities and the specialist associations they have set up in Europe, the private and voluntary sectors, researchers and the public, supported by the media", have an active participation in crime prevention (Council Decision 2009/902/JHA, art. 2).

Crime prevention includes not only the practices of the criminal justice system, but also the practices of other social and public policies, as well as the practices of citizens and private organizations (Gilling, 1997, p. 2). Therefore, individuals, that is, different social subjects, are the ones on whom the implementation of crime prevention policies depends. Over time, private sector organizations have become proficient in prevention work, developing solutions to the problem of crime that can be sold to private consumers and public authorities, including law enforcement (Crawford and Evans, 2017, p. 805). More specifically, scientific and research literature, analysis of expert groups, resolutions, directives and recommendations of international agencies and institutions speak about the indispensable role of private security in crime prevention (Davidović, 2015, p. 353). Given that public police-private security partnerships carry unresolved issues related to "the appropriate balance of burdens, benefits, and controls that are allocated between the public and private

[1] See: Crawford, A. and Evans, K. (2017) 'Crime Prevention and Community Safety', in: Leibling, A., Maruna, S. and McAra, L. (eds.) *The Oxford Handbook of Criminology* (sixth edition). Oxford: Oxford University Press, 797-824.

sectors" (Joh, 2004, p. 51), the suggestion that private security should serve as a partner to public police in crime prevention must be viewed with caution. The issue of cooperation between private security and police, also known in the literature as public-private partnership, is increasingly relevant in both academic and professional circles, including in businesses. Especially after the privatization of critical infrastructure, an extensive body of literature has developed that examines public-private partnership in all contexts, including security. Public-private partnership was created as a paradigm that would use the capacities of both sectors in the best possible way, and today represents a "new value", which aims to achieve a specific goal or set of objectives through cooperation between these two sectors (Busch and Givens, 2012; Carr, 2016, p. 48; Radivojević, 2019, pp. XI, 120).

Members of private security do not focus on punishment but on preventive action, which includes "the plugging of security breaches in the future, the exclusion of likely offenders and ensuring that security is not compromised" (Crawford and Evans, 2017, p. 812).2 Hence, the private security sector is focused primarily on loss reduction and risk management, not on (criminal) law enforcement.

Evolution of private security

Industrialization and rising crime rates put a strain on the police, accelerating the development of private security, also known in the literature as private 'policing'.3 In addition to the historical practice of engaging mercenaries in armed conflicts (Avant, 2004, p. 153), states, driven by motives such as financial efficiency and technological supremacy, have increasingly involved private actors in the field of security. As one of the key drivers of the privatization of security, in addition to economic reasons (White, 2012), the position that the police were unable to meet the increased demands for security of both citizens and organizations is most often highlighted as it was overburdened and limited by its focus on crime control, as well as by existing laws on private property (Shearing and Stenning, 1983). Taking into account all of the above, we conclude that the state's behavior in combination with social, economic and political factors, including defendology factors (Vejnović et al., 2008, p. 13), accelerated the development of the private security sector.

Due to the newly established situation in which security affairs are performed by the entire system composed of "governmental, commercial and social bodies", there has been a 'fragmentation' or 'pluralization' of the police (Jones and Newburn, 2006, p. 1). Although there are authors who believe that the term 'multi lateralization' is more appropriate for this phenomenon (Bayley and Shearing, 2001, p. vii), the term 'privatization' will be used in the paper due to its wide representation in the literature.

---

[2] The evidence suggests that arrests and prosecutions are not necessary for crime control (Grunwald, Rappaport and Berg, 2024, p. 464).

[3] For more on the development of private policing and its impact on future governance in 'collective life', see: Kempa, M. et al. (1999) 'Reflections on the Evolving Concept of 'Private Policing", *European Journal on Criminal Policy and Research, 7*(2), 197-224; Davidović, D. (2007) 'Klasifikacije i tumačenje privatnog polisinga', *Zbornik Instituta za kriminološka i sociološka istraživanja, XXVI*(1-2), 389-397.

This so-called 'privatization' of security can be explained by means of Fiscal constraint theories and Pluralist (structuralist) theory (Jones and Newburn, 1998 according to Button, 2002, pp. 27-32). According to Fiscal constraint theories, the growth of private policing occurred due to the inability of the state to meet the demand for services, and the private sector emerged as an entity that fills the fiscal 'gap'. The radical direction of this theory sees the growth of private policing as an inevitable consequence of the crisis, where the state attracts the private sector to strengthen its legitimacy. The liberal-democratic perspective sees the growth of private policing as an inevitable consequence of demands that the police simply cannot satisfy. The pluralist (structuralist) perspective emphasizes the fragmentation of power that led to this that private corporations and local communities take over the 'reins of power'.

Consideration of the transformation of the security sector and the inclusion of non-state actors in the performance of security tasks can be analyzed analytically through the prism of Principal-agent theory (Avant, 2005). In this theoretical model, the 'principal' is the individual who delegates authority, while the 'agent' is the one who is delegated the authority. In addition to the mentioned approach, there is also an alternative application of this theory in the literature, which places the principal-agent relationship in the framework of the relationship between private security companies and subjects who pay for their services for the purpose of property protection or personal security. In this case, the principals are individuals, groups or organizations that have a need for security services, while the agents are private organizations that provide security services (Abrahamsen and Williams, 2011, p. 108). It is necessary to emphasize that this delegation model does not imply the marginalization or reduction of the role of the state in the security sector. On the contrary, it is possible that the presence of private security actors contributes to the strengthening and support of state authority. According to Abrahamsen and Williams (2007, p. 238), "authority is not necessarily a zero-sum game", which implies that the relationship between the state and private security can be seen as complementary instead of competitive.

According to some authors, the transfer of certain public functions to private security entities should not be viewed exclusively as a process of privatization, but as a "formalization of secondary activities of social control". This approach indicates that, due to the decline in the influence of actors who perform social control as a secondary activity (such as park guards, railway guards or conductors), there has been an intensification of primary forms of control — both through the strengthening of the role of the public police, and through the increase in the importance of private security structures (Jones and Newburn, 2002, p. 142). A group of authors pointed out that the mass production of private property led to the privatization of social control when the scope of this control was expanded by the so-called non-specialized security (Shearing and Stenning, 1983, p. 501). Under these circumstances, private security entities gained legitimacy to exercise social control.

Finally, the authors engaged with the concept of police nodalization, i.e., the diversification of policing and the creation of other nodes, as a result of which in the "age of nodal security management", policing is not limited to the police but includes "nodal groups such as the military and now the huge and growing private security sector" (Shearing, 2005, p. 58; Walby and Lippert, 2015, p. 241).

Conceptualizing private security

To more precisely define private security, it is necessary to refer to the term that is often used in literature as its synonym, 'private policing'. Policing is a term used to describe police action or work. As the primary protection responsibility shifted from the public to the private sector, policing, which was primarily related to the public sector, was basically divided into public – *Public policing* and private – *Private policing*.[4]

Private security is also referred to as *Private police* or *Private security industry*. Namely, numerous foreign authors choose the terms private policing and private police (Stenning, 2000, p. 326), with the fact that private security is not and cannot be a "private form of public police" (Shearing and Stenning, 1983, p. 495). The term Private Security is used to denote "a whole set of activities for securing property, persons and business performed by private legal entities for the provision of security services" (Davidović, 2011, p. 456; Kesić, 2009, p. 33). Pioneers of private security research in the United States indicate that it "starts where public policing leaves off and therefore does not encroach on public policing" (Shearing and Stenning, 1981, p. 220), because it undertakes what "public policing either does not do because of resource constraints or cannot do because of legal constraints" (Kakalik and Wildhorn, 1971, p. 19). A more detailed definition would refer to "employed individuals and organizations/legal entities that, for money, provide security services to clients, individuals or organizations that hire them or have employed them, with the aim of protecting the staff, private property and interests of those clients from various forms of threats" (Dempsey, 2010, p. 2). More comprehensively defined, private security is "a planned and organized independent or joint activity and function of individuals, organizations, private or professional agencies, aimed at their own protection or the protection of others, as well as the protection of appropriate persons, spaces, facilities, businesses or activities, which are not covered by the exclusive protection of state bodies" (Daničić and Stajić, 2008, p. 14).

Foreign and domestic authors have recognized as adequate the definition given by the American Society for Industrial Security, which defines private security as "the non-governmental practice of the private sector of protecting people, property and information, conducting investigations, and otherwise safeguarding the organization's assets" and which has a role in "helping the private sector to secure its operations and critical infrastructure, either from natural disasters, accidents or planned actions, such as terrorist attacks, vandalism..." (Strom et al., 2010, pp. 2-3; Keković and Dimitrijević, 2017, p. 235).

From the above definitions, it follows that the term private security means the performance of security tasks that do not fall under the jurisdiction of state authorities. These

[4] Academic literature identifies four categories of policing actors, differentiated by the extent of their public or private engagement: 1. public police bodies; 2. hybrid policing bodies: (central and decentralized public policing bodies, specialized police organizations and private policing (non-private security)); 3. voluntary policing and 4. private security (Button, 2002, p. 16). Division of private policing subjects see: Sparrow, K. M. (2014) *Managing the boundary between public and private policing.* New Perspectives in Policing Bulletin. Washington, DC: U.S. Department of Justice, National Institute of Justice. Compare with four groups of policing providers: 1) commercial security companies; 2) nongovernmental auspices acting as their own providers; 3) individuals and 4) governments (Bayley and Shearing, 2001, pp. 13-15).

jobs are carried out in two basic directions – for their own purposes or for the benefit of third parties, usually with monetary compensation, and are aimed at protecting individuals, property (space, facilities, information) and business activities from various forms of threats.

A very comprehensive classification of private security services was developed by experts who attended a symposium of the American Society for Industrial Security. They identified eighteen fundamental components of private security, encompassing physical and personnel security, information systems protection, investigative functions, risk and crisis management, legal frameworks, emergency preparedness, as well as strategies addressing crime prevention, counterterrorism, and workplace violence (ASIS Foundation, 2009, p. 4). Defining and classification of private security requires a careful approach, mostly because of the thin line of its distinction in relation to other related terms found in the literature.[5]

Private Security in Crime Prevention

Private security represents an important segment of the overall security system, especially in the domain of crime prevention and protection of people, property and information. The preventive function of private security is primarily achieved through various operational activities such as access and behavior control, physical presence (e.g. patrols, surveillance), securing facilities and persons, as well as implementing internal procedures and security rules. These activities are aimed at preventing and detecting various forms of criminal behavior, including unauthorized access, vandalism, theft, embezzlement, physical assaults, as well as violations of property rights and security procedures (United Nations Office on Drugs and Crime, 2014).

Classifications of private security services encompass a wide array of activities that reflect the sector's complexity and functional diversity. Based on classifications from the literature (CoESS, 2016; Radivojević, 2022, pp. 110-111), private security activities can be classified into four groups according to function: *preventive activities* (commercial manned guarding, beat patrols, in-house security services, public space patrolling, risk assessment and risk management, loss prevention, occupational safety and health, prevention of cyber and property-related crimes, workplace violence prevention, anti-terrorism measures, fire prevention and protection, urban security, critical infrastructure protection, screening procedures, alarm and CCTV monitoring, monitoring center operations, tracking and tracing services, integrated security solutions, front desk/reception and concierge services, security consulting, private security training, and canine (K9) services in their preventive role); *response/intervention activities* (mobile alarm response and call-out services, emergency medical response (first aid services), rapid response to alarms, canine (K9) services (active threat response)); *investigative activities* (corporate investigations); *operational activities* (event security and crowd control, door supervision, personal protection (bodyguarding), cash-in-transit (CIT) operations and transport of valuables, cash processing, aviation security, maritime security, protection of private residences); *logistical and support activities* (combined or

[5] See more: Marković, M. J. (2025) *Korporativna bezbednost kao element sistema nacionalne bezbednosti u zaštiti kritične infrastrukture Republike Srbije*. Doktorska disertacija. Beograd: Univerzitet u Beogradu, Fakultet bezbednosti.

integrated security services, tracking and tracing logistics, monitoring center operations).6 The mentioned activities and services are implemented across various domains of private security operations. At this point, the following key aspects warrant particular attention.

Engagement on public surfaces and in public space

Public areas such as streets, squares, parks and green areas, playgrounds and sports fields play a significant social and functional role in the daily life of individuals and communities. This category also includes closed spaces such as markets, fairs, bus and train stations. Designed to facilitate movement, gathering, and social interaction, these spaces often constitute environments in which various forms of criminal behavior may occur. They are frequently characterized by manifestations of social disorder related to "indecent or suspicious behavior, as well as some forms of social deviance such as homelessness, public drunkenness or consumption of psychoactive substances, excessive noise, unsupervised gatherings of young people, insults and insults, confinement in a closed space, physical and verbal conflicts in the neighborhood" (Marinković and Đurić, 2025, p. 57). Add to that urinating in a public place, begging or lighting pyrotechnic products or shooting, as well as criminal activities, more specifically, theft, fights and assaults, sexual harassment and sexual violence, destruction of public property, possession and sale of psychoactive substances or, ultimately, terrorism. Private security carries out its activity in crime prevention in public spaces primarily through physical direct presence, patrolling and visiting critical points, as well as monitoring certain areas and points through video security systems. Members of private security respond to suspicious or criminal actions, whereby, in addition to notifying the competent state authorities, they can secure the scene, temporarily detain certain persons or, in accordance with the law, apply physical force. A key part of their activity is communication with citizens, both for the purpose of providing information and guidelines, and for the purpose of resolving potentially conflicting situations.

In addition to the direct involvement of private security in crime prevention within public spaces, it is important to highlight other relevant aspects that further illustrate the sector's preventive role. Namely, when members of private security protect persons or property (objects, i.e., rooms, facilities and spaces in general), they can recognize and notice in their surroundings signs that indicate the planning or preparation of suspicious or specific criminal activity, as well as such activity itself, and immediately inform the police about it. For example, when visiting client locations, private security patrols may spot suspicious persons or vehicles, missing persons or they may witness potentially illegal activities. This aspect is particularly significant if we consider the claims that private security operates more in the commercial sector and business environment, and thus deters and prevents crime against individual clients, rather than against the society in which it operates (Muhammed and Musa, 2025). Although this

[6] This classification should be interpreted with caution. Firstly, it is derived from a selected set of activities referenced by other authors and does not encompass the full range of activities described in the broader body of literature. Secondly, the classification is organized according to the primary function of each activity, which implies that certain activities may be relevant to multiple functional categories and could reasonably be placed in more than one group depending on context.

claim may initially be acceptable, it would not be correct because by securing its clients, private security prevents criminal activities at both the micro and macro levels.

Taking into account that the transport of money, valuables, confidential documents and other values that represent high-risk assets is carried out in public space, the role of private security in crime prevention can be seen from that aspect as well. To provide these transports, trained personnel must be present, specialized vehicles must be used, and security procedures must be strictly defined. This method not only protects the property, but also decreases the chances of property crimes targeting those values. At the same time, this form of protection represents an important mechanism in the prevention and suppression of organized crime.

Private security plays a significant role in the control and prevention of crime during public gatherings such as music events, sports events, etc. Then, the main task is to prevent violent and criminal behavior before, during and after the gathering. Public gatherings represent complex security environments in which different forms of criminal behavior intertwine. As a rule, the most common forms of crime that occur under these circumstances are violent behavior, vandalism, bringing in illegal items such as weapons or pyrotechnics, property crimes, illegal trade including the distribution of alcohol and narcotics, sexual harassment. In these cases, private security can be used for security consulting, for material and technical equipment or for the engagement of members of private security who, performing their activities, will promptly detect and prevent any type of violation of security at the gatherings. Depending on the specifics of the gathering itself, the latter most often includes the provision, in the form of immediate presence, of the gathering at rest or in motion or the provision of a specific zone where the gathering takes place, including crowd control; access control – checking tickets or accreditation, inspection of individuals, vehicles and their items in order to prevent unauthorized entry of persons or the introduction of prohibited items; visitor movement control – directing the visitors; observation by direct presence or by technical resources7 in order to intervene or forward security-related information to relevant subjects; and in case of unexpected (harmful) events, conducting evacuation and directing the movement.

The operation of private security on public areas and in public spaces also has a wider preventive effect. Not only does their presence and activities contribute to a safer environment, but it also reduces citizens' fear of crime, thereby strengthening the perception and real sense of security.

Corporate security – Organizational security

Corporate security is distinguished here as part of private security. In fact, it can be understood as a form of private security that is established in an organization (profit and non-profit legal entity of a public and private nature) with the aim of protecting the basic values of the organization (people, property and business) and achieving organizational

[7] This primarily refers to the video security system. However, other surveillance and recording technologies, such as drones, are also being used, which contribute to reducing crime rates (Isbir Turan, Ali Tekine and Akincioğlu, 2020).

goals, which is achieved by proactive and reactive actions of its subjects. Basically, it encompasses every type of security of an organization and is responsible for every security activity carried out in it. The scope of its work can be seen through the following areas: physical and technical protection, data and information security, human resources and employee security, occupational safety and health, environmental protection, fire protection and disaster and emergency risk management (Marković, 2025).

Organizations can face various forms of criminal activity. Without a detailed analysis of each of them, the most significant are crimes against property and economy, computer crime, crimes against general security, diversion, sabotage and terrorism, crimes against the environment. Let's add to that abuse at the workplace, as well as various forms of deviant behavior that can be a prelude to criminal behavior. The task of corporate security is timely detection and prevention of all forms of crime. In this way, preventing criminal activity at the organizational level also prevents criminal activity in general. In this context, it can be concluded that corporate security affects the overall level of crime, reducing it through the actions of its subjects.

Public safety also includes the protection of critical infrastructure. It is highlighted here because it represents the basis for the functioning of the state and society, and the prevention of criminal acts that are in any way connected to it (whether they threaten the infrastructure from the inside, outside or combined) gains more importance. Networks, systems, facilities or their parts have been under the management of the private sector in recent years and even decades, which opens up special issues of its protection. One of these issues relates to the recognition of the private sector as key to the protection of critical infrastructure facilities (CoESS, 2016, p. 12). Looking at it from an organizational perspective, critical infrastructure is like any other organization that is exposed to risks from various forms of crime. Whether viewed in its basic form or as part of it (corporate security), private security plays a significant role in protecting and strengthening the resilience of critical entities, as well as ensuring their ability to provide services.8 It also implies improving security and strengthening the resilience of the entire community.

Emergency situations

From the previous classifications of private security activities and services, it can be concluded that private security can play a significant role in the management of emergency situations. Private security engagement can be conceptualized along two primary forms: as a response to an emergency occurring within the organization itself, and as a reaction to an emergency declared at the community level.9 Given the topic of the paper, we will limit ourselves to private security activities in the event of emergency situations and crime prevention activities.

[8] See more: Marković, M. J. (2023) 'Uloga korporativne bezbednosti u zaštiti kritične infrastrukture Republike Srbije', *Bezbednost, 65*(2), 197-214; Marković, M. J. (2024) 'Resursi privatne bezbednosti za zaštitu kritične infrastrukture u urbanim uslovima', u: Stanarević, S. i Đukić, A. (ur.) *Urbana bezbednost i urbani razvoj: Zbornik radova*, 471-485. Beograd.

[9] About the role of private security in emergency situations see: Cvetković, V. M., and Janković, B. (2020) 'Private security preparedness for disasters caused by natural and anthropogenic hazards', *International Journal of Disaster Risk Management, 2*(1), 23-33; Radivojević, N. (2022) 'Uloga

In an organization, certain forms of crime can be manifested by malicious actions or omissions by people. Extraordinary events caused by the malicious actions of people, such as terrorism, diversion or sabotage, are especially highlighted (Kešetović, 2017, p. 602). In this context, private security resources can be used both for prevention and early response, as well as for remediation of the consequences of those criminal activities. Proactive activities include risk assessment and preparation of documents (primarily assessment documents and action plans), detection of early warning signals, that is, signs that indicate planning or preparation of criminal activities. Reactive activities in the context of crime prevention would include securing the scene, controlling access, protecting property, as well as conducting an investigation, that is, providing assistance to the competent authorities, in order to discover the perpetrator of the crime.

On the other hand, when an emergency situation occurs at the community level (such as natural disasters or technical-technological accidents), there is an increased risk of criminal activities. Then, private security has a reactive role – in addition to engaging in evacuation activities, providing first aid, search and protection of persons, it also carries out other activities such as securing space, facilities and property, access control (identity check, recording presence, directing the people and vehicles), implementing technical or physical-technical protection, temporarily detaining suspects until the arrival of the police, etc. Activities to protect buildings and property in order to prevent potential criminal activities are particularly significant, because property becomes an 'easy target' for crime, in this case.

Conclusion

Although various formal and informal social control actors contribute to crime prevention, modern security challenges highlight the growing importance of the private security sector in this field. No longer limited to reactive protection of property and individuals, private security increasingly assumes a proactive role through activities such as surveillance, access control, and cooperation with local stakeholders. Within the broader process of security privatization, it emerges as a partner to public institutions, especially the police, not only complementing but at times also initiating measures to preserve public order and safety.

The research conducted in the paper yielded several findings. Private security fulfills its role in crime prevention through *operational activities*. Through access control, physical presence, patrols and surveillance, as well as securing facilities and persons, private security entities contribute to the reduction of incidents such as theft, vandalism, violence and other criminal acts. In this context, the preventive action of private security proves to be an effective mechanism in detecting and deterring illegal or deviant behavior. In the context of *public spaces*, the presence of private security in high-traffic locations – such as shopping malls, stations, parks and public events – significantly contrib-

privatnog obezbeđenja u upravljanju rizicima od katastrofa', u: Cvetković, M. V. (ur.) *Zbornik radova Naučno-stručnog društva za upravljanje rizicima u vanrednim situacijama*, Beograd: Naučno-stručno društvo za upravljanje rizicima u vanrednim situacijama i Međunarodnog instituta za istraživanje katastrofa, 110-120.

utes to the preservation of public order and peace. Video surveillance, physical patrols and quick interventions in the event of incidents enable timely response and increase the sense of security among citizens. In the segment of *protecting the transport of value*, private security resources enable the safe transfer of money and other valuables, which reduces the risk of value being compromised. This function represents an important component in the fight against organized crime, especially in the financial sector. Within *corporate (organizational) security*, private security enables comprehensive protection of persons, property and business processes, which contributes to the stability of both the organization and the business environment, as well as the overall reduction of security incidents at the micro and macro level. *Protection of critical infrastructure*, which includes energy, communication, transportation and other key systems, increasingly relies on private security capabilities. In this context, the private sector has a responsibility not only to protect, but also to improve the resilience of infrastructure against potential security threats. In *emergency situations*, private security has a dual role: prevention and early detection of threats within organizations (such as terrorism, sabotage, and diversion), as well as community-level emergency response (such as natural disasters), including evacuation, first aid, access control, and property protection. Finally, the *social aspect* of private security operations should not be neglected either. Its presence in the everyday life of citizens has a positive effect on the subjective sense of security and contributes to reducing the fear of crime, which indirectly encourages community cohesion and increases trust in protection systems.

The paper pointed out the importance of precisely defining the role, functions and importance of private security, as well as the need for its strategic inclusion in the wider crime control system. Nevertheless, despite the positive tendencies, there remain numerous challenges. The first challenge is to develop a normative regulation that will define the competencies, obligations and limitations of private security and their cooperation with public institutions. Along with that comes the development of Public-Private partnerships as an institutional mechanism for the aforementioned cooperation. Through clearly defined responsibilities, information exchange and joint action, such partnerships contribute to a more effective response to security challenges. The next challenge would be related to standardization of work and professionalization of personnel. These prerequisites are necessary for both the public sector (police) and the private sector (private security), in accordance with the legal framework and adopted standards. It is also important to develop effective supervision mechanisms, as well as raise public awareness of the role of private security in crime prevention. Finally, there remains space for empirical research on the real effects of private security on the crime rate, citizens' sense of security, as well as on legal security and protection of human rights, which would fill gaps in knowledge and help in understanding the role of private security in crime prevention.

References

Abrahamsen, R. and Williams, C. M. (2007) 'Securing the city: private security companies and non-state authority in global governance', *International relations, 21*(2), 237-253. https://doi.org/10.1177/0047117807077006

Abrahamsen, R. and Williams, C. M. (2011) 'Power and governance: Global assemblages and the security field', in: Abrahamsen, R. and Williams, C. M. (eds.) *Security Beyond the State: Private Security in International Politics*. Cambridge: Cambridge University Press, 89-121.

ASIS Foundation. (2009) *Compendium of the ASIS Academic/Practitioner Symposium, 1997–2008*. Virginia: ASIS Foundation.

Avant, D. (2004) 'The privatization of security and change in the control of force', *International Studies Perspectives, 5*(2), 153-157. https://doi.org/10.1111/j.1528-3577.2004.00165.x

Avant, D. (2005) *The Market for Force: The Consequences of Privatizing Security*. Cambridge: Cambridge University Press.

Bayley, D. H. and Shearing, C. D. (2001) *The New Structure of Policing: Description, Conceptualization, and Research Agenda*. Washington, DC: National Institute of Justice.

Busch, N. E. and Givens, A. D. (2012) 'Public-private partnerships in homeland security: Opportunities and challenges', *Homeland Security Affairs*, *8*, art. 18.

Button, M. (2002) *Private policing*. London: Willan Publishing.

Carr, M. (2016) 'Public–private partnerships in national cyber-security strategies', *International Affairs*, *92*(1), 43-62. https://doi.org/10.1111/1468-2346.12504

Confederation of European Security Services (CoESS). (2016) *Critical Infrastructure Security and Protection: The Public-Private Opportunity*. Wemmel: CoESS General Secretariat.

Council Decision 2009/902/JHA of 30 November 2009 setting up a European Crime Prevention Network (EUCPN) and repealing Decision 2001/427/JHA. OG, L 321/44. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32009D0902

Crawford, A. and Evans, K. (2017) 'Crime Prevention and Community Safety', in: Leibling, A., Maruna, S. and McAra, L. (eds.) *The Oxford Handbook of Criminology* (sixth edition). Oxford: Oxford University Press, 797-824. https://doi.org/10.1093/he/9780198719441.003.0036

Cvetković, M. V. and Janković, B. (2020) 'Private security preparedness for disasters caused by natural and anthropogenic hazards', *International Journal of Disaster Risk Management*, *2*(1), 23-33. https://doi.org/10.18485/ijdrm.2020.2.1.3

Daničić, M. i Stajić, Lj. (2008) *Privatna bezbjednost*. Banja Luka: Visoka škola unutrašnjih poslova.

Davidović, D. (2007) 'Klasifikacije i tumačenje privatnog polisinga', *Zbornik Instituta za kriminološka i sociološka istraživanja, XXVI*(1-2), 389-397.

Davidović, D. (2011) 'Privatna bezbednost u Srbiji', u: Cvetković, N. V. (ur.) *Rizik, moć, zaštita – Uvođenje u nauke bezbednosti*. Službeni glasnik i Univerzitet u Beogradu, Fakultet bezbednosti, 452-467

Davidović, D. (2015) 'Prevencija kriminaliteta i sigurnost (lokalne) zajednice - mesto privatnog sektora bezbednosti', u: Hughson, M. i Stevanović, Z. (ur.) *KRIMINAL I DRUŠTVO SRBIJE: izazovi društvene dezintegracije, društvene regulacije i očuvanja* životne *sredine*. Beograd: Institut za kriminološka i sociološka istraživanja, 345-356.

Dempsey, S. J. (2010) *Introduction to private security*. Belmont: Wadsworth Cengage Learning.

Gilling, D. (1997) *Crime prevention: theory, policy and politics*. London: UCL Press Limited.

Grunwald, B., Rappaport, J. and Berg M. (2024) 'Private Security and Public Police', *Journal of Empirical Legal Studies, 21*, 428-481. https://doi.org/10.1111/jels.12393

Isbir Turan, A. A., Ali Tekine, M. and Akincioğlu, N. U. (2020) 'Modern usage areas of UAV Technology', *Journal of Criminology and Criminal Law 58*(3), 111-117. https://doi.org/10.47152/rkkp.58.3.8

Joh, E. E. (2004) 'The Paradox of Private Policing', *J. Crim. L. & Criminology, 95*(1), 49-132.

Jones, T. and Newburn, T. (2002) 'The Transformation of Policing? Understanding Current Trends in Policing Systems', *British Journal of Criminology, 42*, 129-146. https://doi.org/10.1093/bjc/42.1.129

Jones, T. and Newburn, T. (2006) 'Understanding plural policing', in: Jones, T. and Newburn, T. (eds.) *Plural policing, a comparative perspective*. London: Routledge, 1-11. https://doi.org/10.4324/9780203001790

Kakalik, S. J. and Wildhorn, S. (1971) *The Private Police Industry: Findings and Recommendations. Vol. I*. RAND Corporation study for the National Institute of Law Enforcement and Criminal Justice. Washington: Government Printing Office.

Keković, Z. i Dimitrijević, I. (2017). *Sistemi bezbednosti sa sistemom bezbednosti Republike Srbije*. Beograd: Univerzitet u Beogradu, Fakultet bezbednosti.

Kempa, M. *et al.* (1999) 'Reflections on the Evolving Concept of 'Private Policing'', *European Journal on Criminal Policy and Research, 7*(2), 197-224. https://doi.org/10.1023/A:1008705411061

Kešetović, Ž. (2017) 'Private security in emergency situations-Serbian experience', *Bezbednosni dijalozi, 8*(1-2), 595-609.

Kesić, Z. (2009) *Privatni sektor u kontroli kriminaliteta*. Beograd: Dosije studio.

Krivokapić, V. (2008) *Prevencija kriminaliteta: Teorijsko kriminalistički pristup*. Beograd: Nade Design; Narodno delo.

Lab, P. S. (2014) *Crime Prevention: Approaches, Practices, and Evaluations*. Waltham: Elsevier Inc

Marinković, A. P. i Đurić, S. (2025) 'Strah od kriminala i urbani nered', *Revija za kriminologiju i krivično pravo, 63*(2), 53-77. https://doi.org/10.47152/rkkp.63.2.3

Marković, M. J. (2023) 'Uloga korporativne bezbednosti u zaštiti kritične infrastrukture Republike Srbije', *Bezbednost, 65*(2), 197-214. https://doi.org/10.5937/bezbednost2302197M

Marković, M. J. (2024) 'Resursi privatne bezbednosti za zaštitu kritične infrastrukture u urbanim uslovima', u: Stanarević, S. i Đukić, A. (ur.) *Urbana bezbednost i urbani razvoj: Zbornik radova*, 471-485. Beograd. https://doi.org/10.5937/ubur24471m

Marković, M. J. (2025) *Korporativna bezbednost kao element sistema nacionalne bezbednosti u zaštiti kritične infrastrukture Republike Srbije*. Doktorska disertacija. Beograd: Univerzitet u Beogradu, Fakultet bezbednosti.

Markusen, R. A. (2003) 'The case against privatizing national security', *Governance, 16*(4), 471-501. https://doi.org/10.1111/1468-0491.00225

Muhammed, S. I. and Musa, A. U. (2025) 'The role of private security guard companies on crime prevention: a study of kano metropolis, nigeria', *International journal of social science research and anthropology, 7*(6), 211-234. https://doi.org/10.70382/tijssra.v07i6.031

Oyebambi, O. M. (2024) 'Role of private security firms in enhancing urban safety and crime prevention', *Fuoye journal of criminology and security studies*, *3*(2), 85-95.

Radivojević, N. (2019) *Javno-privatno partnerstvo u oblasti javne bezbednosti u razvijenim zemljama sa posebnim osvrtom na Republiku Srbiju*. Doktorska disertacija. Novi Sad: Univerzitet u Novom Sadu, Pravni fakultet u Novom Sadu.

Radivojević, N. (2022) 'Uloga privatnog obezbeđenja u upravljanju rizicima od katastrofa', u: Cvetković, M. V. (ur.) *Zbornik radova Naučno-stručnog društva za upravljanje rizicima u vanrednim situacijama,* Beograd: Naučno-stručno društvo za upravljanje rizicima u vanrednim situacijama i Međunarodnog instituta za istraživanje katastrofa, 110-120.

Shearing, C. (2005) 'Nodal security', *Police Quarterly, 8*(1), 57-63. https://doi.org/10.1177/1098611104267327

Shearing, D. C. and Stenning, C. P. (1981) 'Modern Private Security: Its Growth and Implications', in: Tonry, M. and Morris, N. (eds.) *Crime and justice: An Annual Review of Research, 3*, 193-245. http://dx.doi.org/10.2139/ssrn.2832664

Shearing, D. C. and Stenning, C. P. (1983) 'Private security: Implications for social control', *Social Problems, 30*, 493-506. http://dx.doi.org/10.2139/ssrn.2726577.

Sparrow, K. M. (2014) *Managing the boundary between public and private policing*. New Perspectives in Policing Bulletin. Washington, DC: U.S. Department of Justice, National Institute of Justice.

Stajić, L. S. (2015) 'Prevencija kriminala sa aspekta dizajniranja javnog prostora i uloge privatnog obezbeđenja', *Zbornik radova Pravnog fakulteta, Novi Sad*, *49*(1), 75-87. https://doi.org/10.5937/zrpfns49-8274.

Steenkamp, D. G. (2002) *The role of private security in crime prevention*. Doctoral dissertation. University of Zululand.

Stenning, P. (2000) Powers and Accountability of Private Police. *European Journal on Criminal Policy and Research, 8*(3), 325-352. https://doi.org/10.1023/A:1008729129953

Strom, K. *et al.* (2010) *The private security industry: A review of the definitions, available data sources, and paths moving forward*. US Department of Justice and National Criminal Justice Reference Service, Final Report.

Trivan, D. (2013) 'Vpliv korporativne varnosti na nacionalno varnost', *Sodobni vojaški izzivi, 15*(3), 69-98. https://doi.org/10.33179/BSV.99.SVI.11.CMC.15.3.5

UN Economic and Social Council (ECOSOC). (2002) UN Economic and Social Council Resolution 2002/13: Action to Promote Effective Crime Prevention, E/RES/2002/13. https://www.refworld.org/legal/resolution/ecosoc/2002/en/26450

Van Dijk, J. (1990) 'Crime Prevention Policy: current state and prospects', in: Kaiser, G. and Albrecht, H. J. (eds.) *Crime and Criminal Policy in Europe: Proceedings of the II. European Colloquium*, 205-220.

Vejnović, D. *et al.* (2008) D*etektivska djelatnost: teorijski i praktični aspekti po standardima Evropske Unije*. Banja Luka: Defendologija centar za bezbjedonosna sociološka i kriminološka istraživanja; Ljubljana: Detektivska zbornica Republike Slovenije.

Walby, K. and Lippert, R. (2015) 'The difference homeland security makes: Comparing municipal corporate security in Canada and the United States', *Security Dialogue, 46*(3), 238-255. https://doi.org/10.1177/0967010615570109

White, A. (2012) 'The new political economy of private security', *Theoretical Criminology, 16*, 85-101. https://doi.org/10.1177/1362480611410903

© 2026 by authors

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

Journal of Criminology and Criminal Law, 64(1), 83-102
Original Scientific Article
https://doi.org/10.47152/rkkp.64.1.5
UDK: 004.6:343.13(4–6EU)

RECEIVED: 22 January 2026
ACCEPTED: 15 April 2026

From admissibility to contestability: Structural opacity, encrypted-platform evidence, and the limits of adversarial review

Janko Munjić[a]

Digital evidence from encrypted platforms such as EncroChat and Sky ECC is increasingly treated as formally admissible across multiple jurisdictions, yet core questions of provenance, integrity, and attribution remain structurally resistant to adversarial testing. Existing scholarship has mapped the doctrinal and cooperation routes through which such datasets enter domestic proceedings, but has not sufficiently operationalised the conditions under which they remain genuinely contestable once admitted. This paper addresses that gap through a doctrinal analysis of selected EU, ECtHR, and domestic case law, combined with a normative analysis of Serbian criminal procedure and recent regional scholarship on digital evidence. It argues that structural opacity is sustained by cross-border procedural architecture, confidentiality constraints, and restrained legality review under mutual recognition, and that formal admissibility cannot by itself secure fair evidential use where the defence cannot test method-relevant premises. The paper makes three original contributions. First, it proposes a minimal contestability test structured around provenance, integrity, and attribution, together with a staged verification package designed to function under persistent secrecy. Second, it develops a tiered remedial model linking failed contestability to calibrated procedural consequences, from reduced weight and mandatory corroboration to exclusion where the material is sole or decisive. Third, it maps contestability onto the Serbian Criminal Procedure Code and shows how existing procedural levers can operationalise the framework without legislative change. The paper further argues that the EU AI Act is relevant only as an external traceability benchmark for algorithmically processed investigative outputs, but not as a direct source of evidentiary law.

KEYWORDS: encrypted-platform evidence, contestability, opacity, EncroChat, Sky ECC, adversarial principle, EU AI Act

[a] Senior judicial assistant, Appellate Court in Kragujevac; PhD candidate, Faculty of Law, University of Kragujevac; E-mail: munjicjanko@gmail.com; ORCID: 0009-0004-8649-2233

Introduction

Encrypted-platform evidence is increasingly treated as formally admissible in criminal proceedings across multiple jurisdictions. Courts admit EncroChat and Sky ECC material through familiar doctrinal categories and narrow cross-border legality review, and that process is by now well documented.

Recent regional scholarship has mapped how such datasets enter domestic proceedings through international legal assistance, including the Serbian context (Ilić, 2024, p. 409). Turanjanin (2025, p. 14) treats mutual recognition and mutual trust as the organising logic of cooperation, with the practical implication that the issuing State cannot replicate the executing State's legality control without weakening the European Investigation Order (EIO) framework. Bajović and Ćorić (2025, p. 248) identify the same stabilising pressure, but they also expose its central tension, namely that selective sharing of materials creates a permanent uncertainty about the legal nature and contestability of the datasets. The EncroChat experience has further exposed the absence of binding digital forensics standards and a mutual-trust setting in which the defence's position and scalable audit procedures remain underdeveloped (Stoykova, 2023, p. 1).

This literature is valuable, but it leaves a gap. It explains how encrypted-platform evidence becomes usable in court, but it does not sufficiently operationalise the conditions under which that evidence remains genuinely contestable once admitted. Contestability here refers to the defence's practical ability to test method-relevant premises through verifiable traces. The adversarial principle is a binding constraint on evidential use, not an optional aspiration (Lasagni, 2025, p. 146), and where the defence cannot test provenance, integrity, or attribution, that constraint is not met. The central question of this paper is under what conditions encrypted-platform evidence remains genuinely contestable after formal admission, and what procedural consequences should follow when it does not.

This paper adopts a doctrinal and normative legal method. It draws on selected EU, ECtHR, and domestic case law, together with regional scholarship and Serbian criminal procedure provisions, to examine how encrypted-platform material moves from formal admissibility to evidential reliance. It does not attempt an empirical reconstruction of all EncroChat or Sky ECC litigation, nor does it claim to identify universal technical features of every encrypted-platform case. Its purpose is to identify the procedural point at which formal admissibility becomes insufficient and to propose a court-usable framework for contestability under conditions of structural opacity.

The paper makes three contributions. First, it proposes a minimal contestability test structured around provenance, integrity, and attribution, together with a staged verification package designed to function under persistent secrecy. Second, it develops a tiered remedial model that links failed contestability to calibrated procedural consequences depending on the dataset's role in the case, ranging from reduced weight and mandatory corroboration to exclusion where the material is sole or decisive. Third, it maps contestability onto the Serbian Criminal Procedure Code and shows how existing procedural

levers, including evidentiary motions, expert examination, the exclusion-versus-weight distinction, and the reasoning duty, can operationalise the proposed framework without legislative change. The paper further argues that the EU AI Act serves as an external benchmark for traceability and documentation of algorithmically processed investigative outputs, but not as a direct source of evidentiary law.

The analysis proceeds through five substantive sections. Section II examines how admissibility is stabilised through doctrinal reclassification, restrained cross-border review, and categorisation. Section III analyses opacity as a structural constraint on adversarial review. Section IV proposes the contestability test. Section V applies it under the Serbian CPC. Section VI addresses AI-mediated processing as an additional contestability problem.

How encrypted-platform evidence becomes usable before it becomes contestable

Descriptively, admissibility in encrypted-platform cases is often secured before the court reaches the more complex questions about how the material was produced. Courts and cooperation frameworks make the dataset manageable by fitting it into familiar categories and by keeping cross-border legality review narrow. That keeps proceedings moving, but it shifts the real pressure point to contestability, where the defence needs a practical way to test provenance, integrity, and attribution.

Doctrinal reclassification

Doctrinal reclassification stabilises admissibility by recoding how courts describe the dataset. In the leading EncroChat appeal, the Court of Appeal treated the relevant material as stored data obtained from devices before encryption, not as communications in transmission, reducing the force of the strict interception exclusion (*A, B, D & C v R* [2021] EWCA Crim 128, paras. 66-67). The Investigatory Powers Act 2016 similarly distinguishes stored material from communications in transmission, with practical consequences for admissibility arguments (Griffiths and Jackson, 2022, p. 274; *Investigatory Powers Act*, 2016, s. 4; Smart and Mosley, 2021). These moves do not establish evidential reliability, but they make the dataset procedurally manageable. The result is that evidence may become usable for admission and early-stage reliance before the defence has a practical basis to test provenance, integrity, and attribution.

Restrained legality review across borders

Restrained legality review stabilises admissibility by narrowing the space for cross-border legality control. The German Federal Court of Justice notes that in the EIO and mutual legal assistance framework, the requesting State is not envisaged to review whether the executing State lawfully obtained already existing evidence under the requesting State's own procedural standards, and that any resulting deficits are addressed at the stage of evidential use (BGH 5 StR 457/21, 2022, para. 30(b)). The CJEU Encro-

Chat line complements this. Evidence already in the executing authority's possession may be transmitted under an EIO, but fundamental-rights compliance must be capable of subsequent judicial review, and courts may need to disregard evidence if the person concerned is not in a position to comment on it (CJEU, M.N. (*EncroChat*), Case C-670/22, paras. 130-131; Hoxhaj, 2025, p. 8). Recent commentary on that judgment argues that where the defence cannot meaningfully contest authenticity, legality, or reliability because key technical features remain undisclosed, exclusion may be the appropriate consequence rather than a purely formal admissibility outcome (Merkevičius, 2025, p. 551). These sources show that cross-border legality review is narrow and fairness is pushed to the evaluation stage, and that this architecture predictably entrenches opacity at the point where adversarial control should attach. Stoykova (2023, p. 11) similarly argues that mutual trust instruments such as the EIO structure cooperation around law enforcement, leaving defence and judges ill positioned to scrutinise the validity, integrity, and reliability of the resulting digital evidence. A similar normalisation of cross-border e-evidence flows appears beyond EU mutual recognition. The Second Additional Protocol enables direct orders to service providers and requires the order to carry basic case and offence information that can function as a minimum provenance record (*Second Additional Protocol*, 2022, Art. 7(3)(f) and 7(4)(a)).

Why admissibility becomes a category exercise

When admissibility is stabilised through doctrinal labels and restrained cross-border review, the judicial inquiry predictably shifts from reconstructing investigative method to placing the dataset into a manageable legal category. The practical question becomes whether the material can be treated as a recognised evidentiary type within the forum's procedural vocabulary, rather than whether the defence can scrutinise the full chain of technical and organisational steps that produced it. Courts effectively substitute technical verification with legal labelling, because the underlying method of production remains unscrutinised as long as the dataset fits a recognised evidentiary type. Article 6 of the European Convention on Human Rights does not lay down rules on admissibility as such, and the fairness inquiry centres on the proceedings as a whole, including whether the defence had a real opportunity to challenge authenticity and oppose use, even where the material is decisive in practice (*Khan v. the United Kingdom*, Application no. 35394/97, paras. 34, 37-38). The Court accepts that unlawfully obtained evidence is not excluded in the abstract and attaches weight to adversarial opportunities and the broader evidentiary setting, which makes "category plus opportunity" an attractive judicial shortcut when method-level disclosure is structurally unavailable (*Schenk v. Switzerland*, Application no. 10862/84, paras. 45-48).

These admissibility pathways describe how encrypted-platform evidence becomes court-usable, but they leave unresolved the question of what minimum conditions must be met before such evidence can be treated as genuinely contestable in adversarial proceedings. The next section examines why that question is structurally difficult to answer.

Structural opacity as the limit of adversarial review

Analytically, opacity in encrypted-platform cases stems from several interacting features that undermine adversarial testing. The analysis identifies recurring constraints in encrypted-platform cases without suggesting that each of them appears in every case. Cumulatively, these features shift the defence from testing method-relevant premises to reacting to a narrative that arrives pre-packaged, which is where adversarial review becomes formally available but practically thin.

Secrecy and the channelling of contestation

In Sky ECC cases, defence arguments for disclosure of decryption techniques have often been dismissed, partly on the basis that details are not relevant to lawfulness and partly because techniques must remain secret for future use. In evidentiary terms, secrecy does not merely restrict disclosure. It reallocates risk by requiring the court to rely on method-based premises that the defence cannot test. Oerlemans and Royer (2023, pp. 447, 453) argue that the absence of supervision and explicit reliability standards makes technical disclosure normatively difficult to avoid. One reason this secrecy posture persists is that, although technical standards exist (e.g., ISO/IEC 27037:2012 on the identification, collection, acquisition and preservation of digital evidence), there is still no binding EU-level procedural regime for cross-border criminal cases that would, in EIO practice, compel forensic-report exchange and demonstrable reliability criteria tied to Article 6-compatible evidence handling (Stoykova, 2023, p. 14).

The procedural difficulty arises when secrecy operates without substitute verification mechanisms that could keep adversarial review meaningful. Open-ended disclosure of investigative techniques would compromise operational capabilities and cross-border cooperation. But where secrecy blocks full disclosure, the question becomes whether a testable verification package, such as hash lists, chain-of-custody logs, and court-supervised independent forensic review, can bridge the gap as part of a procedural-accuracy approach requiring access to the chain of evidence and adequate forensic assistance (Stoykova, 2024, p. 1). Where such independent testing and counterbalancing safeguards are absent, secrecy can translate into a practical inability to mount a meaningful adversarial challenge to the underlying material (cf. *Matanović v. Croatia*, 2017, paras. 165-166; *Edwards and Lewis v. the United Kingdom*, 2004, paras. 74-81).

The ECtHR EncroChat applications illustrate how this plays out procedurally. The Court declared the applications inadmissible for non-exhaustion of domestic remedies, holding that the applicants should have pursued available remedies in France before seizing Strasbourg (*A.L. and E.J. v France*, 2024, paras. 145-147). The materials around Ruling 24-84.262 show the procedural fight over standing and the scope of review for measures linked to an EIO, including the applicant's argument that a person detained abroad on the basis of French-originating material may otherwise be left without any effective court to challenge it (Cour de cassation, 2025, 4°). These sources jointly show that the right to chal-

lenge is procedurally difficult to activate in a way that reaches the technical core. Contestation is formally redirected toward standing and jurisdiction, while the technical pathway that drives reliability remains largely insulated from adversarial inspection.

Early reliance and the routinisation of the review gap

Early procedural use of encrypted-platform material can precede meaningful adversarial inspection. Jocić (2025, p. 121) notes that in Serbian Sky ECC detention appeals the Appellate Court in Belgrade has relied on encrypted communications for reasonable suspicion while stating that it does not, at that stage, address the legal nature or legal validity of the obtained data. In decision Kž-Kre 11/2023 of 29 May 2023, the Appellate Court in Kragujevac treated decoded Sky Pin messages as probative for reasonable suspicion in extradition proceedings and noted that the material was obtained under the requesting State's law and was not contrary to international standards. Paunović (2025, p. 86) stresses that the issue is already live in ongoing proceedings before the Higher Court and the Appellate Court in Belgrade, although no final domestic judgment has yet been rendered on encrypted-platform material. These domestic sources support the narrower claim that early-stage reliance is possible despite limited adversarial traction on provenance and method. This creates path dependence, because once encrypted-platform material anchors reasonable suspicion, later procedural stages tend to inherit that starting point, even if the defence has not yet had a realistic chance to test provenance and attribution.

Adversarial participation must be effective, not merely formal (Lasagni, 2025, p. 146). In encrypted-platform cases, the defence can often comment on the incriminating narrative, but cannot meaningfully contest provenance, integrity, or attribution when key technical and cross-border steps are treated as non-disclosable. That is how opacity turns into a systemic feature rather than an isolated inconvenience. Once early-stage reliance is normalised, later review becomes path dependent, because courts tend to inherit the initial trust-based framing even when the evidentiary stakes increase. The practical result is that reasoning shifts from demonstrating reliability to repeating admissibility labels and cooperation premises, while the method-based premises remain largely unexamined.

The central issue therefore becomes which minimum premises must remain verifiable in order for the later evidential use of encrypted-platform material to remain genuinely contestable.

A minimal contestability test

What remains verifiable under structural opacity

Even under structural opacity, adversarial review need not collapse entirely. What remains verifiable is the evidential chain around the decryption technique. Courts can still require proof of provenance, meaning a traceable chain of custody from extraction to disclosure. They can still test integrity, meaning whether the dataset is stable, complete in the relevant sense, and consistent across copies through identifiers and logs of any

transformations. This demand is consistent with EU law enforcement data-processing standards, which treat logging as a basic accountability safeguard and require logs to be kept so that lawfulness and integrity can be verified (*Directive (EU) 2016/680*, Art. 25(1)). Courts are still able to scrutinise attribution, meaning whether messages are linked to the accused through independent anchors such as device seizure records, account identifiers, metadata, and corroboration. Where any of these three elements cannot be tested in practice, the court should recognise that deficit as an evidential constraint requiring procedural consequence, rather than dismissing it as a minor practical difficulty.

The test

Normatively, if opacity is structural, the corrective should be operational. This paper proposes a minimal contestability test centred on three method-relevant premises that must remain practically testable for Article 6 equality of arms under conditions of structural opacity. Provenance asks what the file is and whether it is complete. Integrity asks whether processing introduced material distortion, not just tampering. Attribution asks whether there are independent anchors linking the dataset to the accused. If these premises remain sufficiently testable, the remaining disputes can be handled through ordinary adversarial evaluation.

Provenance

The court should be able to trace the dataset through the cross-border chain of custody, including key processing stages. In digital forensics terms, provenance and integrity are closely linked through a traceable chain of custody that enables later reliability assessment (Stoykova, 2023, pp. 5-7). The court should require stable dataset identifiers, time stamps for each transfer, and a clear description of who controlled the material at each step, including any transformation prior to disclosure. A provenance showing is weakened where the file arrives as a selective extract or a curated compilation without a verifiable mapping back to the original capture set. Recent Italian proceedings confirm this pattern. In criminal proceedings in Imperia based on EncroChat material obtained through an EIO, a court-appointed forensic expert concluded that the data could not be regarded as original evidence, finding in particular that there was no evidence the dataset was complete, no evidence as to how conversations were attributed to individual users, and that the material appeared to be the result of a filtering process carried out by the French authorities (Fiorino, 2026). At minimum, the prosecution should be able to show how the disclosed subset relates to the source dataset, and that it allows the defence to assess context and completeness for the incriminating passages. Where such mapping is unavailable, the court should recognise those gaps as contestability deficits with evidential significance and should require either a disclosure remedy or a corroboration-based limitation on reliance. In practice, provenance requires reviewable artefacts capable of verification, including transfer logs, dataset identifiers, and documented extraction and filtering steps, rather than narrative assurances alone. The Eurojust monitor likewise links EIO transmission of already gathered evidence to subsequent fundamental-rights review by the trial court (Eurojust CJM 9, 2024, p. 10).

Integrity

The defence should be able to challenge reliability through access to limitations, error modes, and validation material, even if operational playbooks remain protected. Integrity must be assessed with regard to both message alteration and processing-induced distortions that may materially affect interpretation, including translation drift, merging of threads, or loss of metadata. Hash comparisons and forensic examinations can support integrity claims, while partial datasets and toolbox outputs raise distinct risks (Oerlemans and Royer, 2023, pp. 452-458). Courts should require a record of transformations, including decoding, formatting, filtering, and any automated enrichment, together with version identifiers for the tools used. Courtroom practice in the SKY ECC proceedings also illustrates that translation and interpreting constraints, especially drug argot and uneven access to preparatory materials, can operate as a non-trivial transformation of meaning rather than a neutral conduit (Elola-Calderón, 2024). This follows the BGH point that defence rights and a fair trial must be secured when evaluating EIO evidence in national proceedings (BGH 5 StR 457/21, 2022, paras. 49 and 51), and the CJEU point that evidence may need to be disregarded if effective comment is impossible (CJEU, Case C-670/22, para. 131; Hoxhaj, 2025, p. 8). Building on EncroChat, Janusz-Pohl reads the CJEU as attaching a nullity-based exclusionary consequence, grounded in effectiveness and fair-trial guarantees, where the defendant cannot effectively comment on or challenge the manner in which the evidence was collected or transmitted (Janusz-Pohl, 2025, pp. 749, 755). Where the defence cannot access even a minimal set of reliability material, the court should treat the evidence as method-dependent and should not permit the prosecution to convert that dependence into a presumption of accuracy.

Attribution

The defence should be able to contest the link between a person and an identifier, device, or account, with disclosure sufficient to test alternative hypotheses. Attribution is central to equality of arms in encrypted-platform cases. Without it, adversarial review collapses into a one-sided contest about meaning (e.g., a shared handset, a compromised account, or a swapped device) rather than a test of method. This lack of transparency regarding the linkage mechanism can create a *de facto* burden-shifting effect, as the defence is pushed to disprove identity rather than test a prosecution case grounded in verifiable traces. The court should therefore require independent anchors, such as seizure records, device association evidence, account linkage material, and consistency with external corroboration, rather than relying on narrative coherence alone. Where attribution rests on probabilistic inferences or on investigative clustering, the defence must be able to inspect the basis of that linkage, at least through verifiable traces and a clear description of the inference steps. If the attribution showing fails this check, the court should order a verification package (e.g., logs, hash lists, chain-of-custody records, and independent expert review). Where meaningful verification remains impossible, the court should exclude the evidence or treat its probative value as minimal. Exclusion is warranted where the material is sole or decisive. Otherwise, independent corroboration by contestable evidence should be required.

The verification package

Where the three prongs cannot be assessed from the disclosed file alone, the court should order a verification package tailored to what remains verifiable under structural secrecy. The package should be staged. It could start with disclosure of non-sensitive artefacts that are directly probative of provenance, integrity, and attribution, such as chain-of-custody logs, transfer records, hash lists, dataset identifiers, and tool version information. Where the defence makes a specific, reasoned challenge that cannot be resolved on that basis, the court can move to controlled review of sensitive materials through in-camera inspection or a confidentiality regime, since any restriction must be strictly necessary and counterbalanced by judicial procedures (cf. *Jasper v the United Kingdom*, 2000, paras. 52-56; *Rowe and Davis v the United Kingdom*, 2000, paras. 61-63). A court-appointed expert can then test reproducibility and consistency, verify hash integrity, and report on whether the processing pathway contains gaps that prevent meaningful adversarial scrutiny, without exposing operational playbooks or technique details. The aim is to secure a court-managed minimum of reviewable traces that preserves contestability under conditions of secrecy.

Consequences if the test fails

Once contestability is defined through provenance, integrity, and attribution, the next question is procedural consequence. If the material fails to meet the contestability threshold, the court should recognise that deficit as an evidential constraint, with the consequence depending on the role the dataset plays in the case. Evidence that remains practically untestable after reasonable verification steps, including any court-ordered verification package, cannot be relied upon as sole or decisive proof. Non-decisive material may be admitted only with sharply reduced weight and an explicit requirement of independent, contestable corroboration that can carry the key inferences without the opaque pipeline. In pre-trial settings, the court should avoid determinative reliance on untestable material and should require a minimum showing on provenance and attribution before treating the material as sufficient for coercive measures. Across all stages, the court should record the failure of contestability in reasons and specify which prong failed and why. That discipline prevents opacity from becoming routine and forces a transparent link between what cannot be verified and what the court is prepared to infer.

Applying contestability under the Serbian CPC

Under the Serbian CPC, contestability may be operationalised through four procedural levers: evidentiary motions and judicial case management, expert examination and party technical participation, the distinction between exclusion and evidential weight, and the duty to give reasons where contested digital evidence is treated as sole or decisive. The mapping that follows is anchored in the CPC's core evidentiary architecture, including party-led proof with judicial steering (Art. 15 and Art. 395), free judicial evaluation combined with a legality constraint (Art. 16), and formal mechanisms for removing unlawful material from the case file (Art. 84, Art. 358, and Art. 407).

This section demonstrates the application of the contestability framework proposed in the preceding section through existing procedural tools, without requiring legislative change. While Serbian procedure does not directly implement EU e-evidence regulation, the forthcoming application of Regulation (EU) 2023/1543 reinforces the cross-border reality of digital evidence flows and highlights the importance of procedural tools that allow contestability at the evidentiary stage. By contrast, the US CLOUD Act addresses jurisdiction and provider-level conflicts at the production stage through comity-based mechanisms (18 U.S.C. § 2713; 18 U.S.C. § 2703(h)(2)-(3)), but it does not answer the courtroom question that drives this paper, namely how the defence can test provenance, integrity, and attribution once the material is repackaged for evidentiary use.

Evidence proposals and judicial case-management

Under the Serbian CPC, the contestability framework can be implemented through ordinary party-led proof combined with firm judicial steering. The prosecution bears the burden of proof, evidence is taken primarily on party proposals, and the court can still order supplementary evidence where the existing record is contradictory or unclear and needs to be fully tested, which is the natural procedural home for meta-evidence that goes to provenance, integrity, and attribution (Art. 15). The CPC also supports disciplined frontloading. After the main hearing is scheduled, parties proposing new evidence must specify which facts are to be proved and by which evidence (Art. 356), and throughout the main hearing they may propose new evidence until its close, while the presiding judge decides and must reject illegal evidence by a reasoned ruling, and may reject late proposals that were known earlier but not proposed without justification (Art. 395). These levers let the court distinguish between focused contestability requests that enable meaningful adversarial testing and diffuse requests that are either irrelevant or designed to delay, which the court has a duty to prevent (Art. 14). Domestic case law already shows that contestability disputes in digital cases often start as a classification dispute about the proper procedural route, including whether forensic extraction from devices is treated as a court-ordered search or as expert examination, which is precisely why contestability requests should be framed early and managed through focused evidentiary motions (cf. Appellate Court in Kragujevac, Kž2-465/23, 2023; Appellate Court in Kragujevac, Kž2-48/23, 2023). This route is especially important for integrity and attribution disputes, and it may also assist provenance review where the chain of technical handling is incomplete on the face of the file. Similar typology disputes arise with intelligence-type material, where courts debate whether such reports qualify as documentary evidence and how confidentiality claims interact with adversarial testing, which again supports treating contestability as a managed evidentiary issue rather than a late-stage narrative argument (cf. Appellate Court in Kragujevac, Kž2-402/22, 2022; Appellate Court in Kragujevac, Kž2-467/22, 2022).

In encrypted-platform cases, the practical point is that contestability should be litigated through targeted evidence proposals that seek verification steps rather than narrative debate. Bajović and Ćorić (2025, p. 255) note that in Serbia Sky ECC data is often

presented in Excel tables treated as documents obtained through international legal assistance, while the defence's ability to comment effectively is limited because such tables are easily manipulated and the collection method remains unknown. Official communications around Sky investigations in Serbia stress both the operational value of decoded datasets and the insistence that lawful acquisition is essential for indictment and conviction, which makes a court-facing contestability discipline all the more important (Government of the Republic of Serbia, 2023). Turanjanin's (2025, p. 12) synthesis of current litigation patterns identifies recurrent defence objections that track the same three pillars, including chain of custody and forensic integrity, and equality of arms concerns where technical methods remain classified, and he highlights that access to technical files remains a central unresolved issue. Against that background, CPC case management should treat contestability proposals as a structured request for a workable verification pathway within the case file and the hearing, such as chain-of-custody records, integrity checks where available, processing logs, and a court-supervised independent verification step under confidentiality, while using the CPC's refusal and anti-delay tools only against unfocused or unjustifiably late motions, not against the core minimum needed to make adversarial review real.

Expert evidence

Expert evidence is the CPC's most direct procedural route for converting disputes about integrity and attribution into reviewable facts when the prosecution relies on technical, method-dependent material. This framing also matches domestic appellate reasoning, which treats device-related disputes as belonging to the expert-evidence track rather than being automatically absorbed into the search regime, and it implicitly rewards method-recording in the expert file as the basis for later review (cf. Appellate Court in Kragujevac, Kž2-465/23, 2023). The defence should treat this as the natural procedural home of contestability by requesting expert examination and appointing a technical advisor, so the challenge is litigated inside the expert process rather than as abstract "trust" objections. The CPC defines the technical advisor and gives them concrete rights that track the verification needs identified in the preceding section, including being notified and attending the examination, inspecting the case file and the object of examination, proposing specific actions to the expert, submitting comments on the expert's findings, questioning the expert at trial, and being examined on the subject matter (Arts. 125 and 126). At trial, the expert is subject to adversarial questioning, and although the court may in limited situations proceed by reading the written report, it retains the option to order direct examination later if party comments show that fuller clarification is needed (Arts. 402 and 403). This matters practically because, as noted above, Sky ECC material in Serbia is often delivered through Excel tables whose collection method remains unknown, which narrows the defence's ability to comment effectively (Bajović and Ćorić, 2025, p. 255). Restricted defence access to technical files remains a central unresolved issue in EncroChat and Sky ECC litigation more broadly, which makes a court-managed, expert-mediated verification pathway a realistic counterbalance rather than a luxury (Turanjanin, 2025, p. 12).

Exclusion vs. weight

A contestability discipline under the CPC starts by separating two different questions that are often conflated in practice – illegality and reliability. If the defence challenge credibly targets illegality, the CPC's response is exclusion, because a judgment cannot be based on evidence that is unlawful in itself or unlawful by the manner of obtaining it (Art. 16(1)), and such material cannot be used in the proceedings (Art. 84(1)). A good illustration is domestic practice on covert recordings, where courts treat privately produced "surveillance-like" material as unlawful because citizens cannot replicate special evidentiary actions, so the response is exclusion rather than a mere discount in weight (cf. Appellate Court in Kragujevac, Kž2-434/22, 2022). The unlawfully obtained material must be physically separated from the file, and derivative illegality ("fruit of the poisonous tree") renders subsequent evidence unusable. The CPC provides a concrete procedural pathway for removing that material from the case file through formal rulings and separate custody, including exclusion during the investigation phase by the pre-trial judge (Art. 237), exclusion at trial by the presiding judge when unlawful minutes or notices remain in the file (Art. 358), and exclusion by the trial chamber with the possibility of a separate appeal, as well as the possibility to reverse an unchallenged exclusion decision before the end of the evidentiary stage if the chamber later concludes it was unwarranted (Art. 407).

Where the challenge is not about illegality but about contestability in the narrower sense, meaning the defence cannot practically test provenance, integrity, or attribution due to missing records, sealed methods, or non-reproducible processing, the issue is ordinarily weight, not automatic exclusion. But where contestability remains practically unrealised after reasonable verification steps and the dataset carries the key inferences as sole or decisive proof, the appropriate response may be non-reliance or exclusion, not a nominal discount in weight. The CPC imposes a strict reliability threshold through its evaluation rules. The court must assess evidence impartially, evaluate relevant evidence by free judicial conviction, and may base the verdict only on facts in whose certainty it is convinced, while doubts on decisive facts are resolved in favour of the defendant (Art. 16(2) to (5)). In that setting, an opaque item may remain formally admissible, but it should carry sharply reduced probative value unless the record contains a workable verification pathway, and it should not be used as sole or decisive proof where contestability remains practically unrealised after reasonable verification steps.

Reasoning duty for sole/decisive reliance

When a contested digital item is treated as the sole or decisive basis for a finding, the main safeguard under the CPC lies in a discipline of reasons that makes the court's reliance visible, reviewable, and open to challenge on the record. The CPC already demands reasons on every point of the judgment (Art. 428(8)). The court must state which facts it found proven or not proven, explain why it rejected party proposals, and assess credibility where the evidence conflicts.

A contestability discipline specifies what those reasons must cover when the dispute concerns method and provenance, alongside the apparent meaning of the message. The judgment should set out the verification pathway that was available and actually used. It should identify the records or traces that support provenance and integrity, explain how attribution was connected to the accused, and respond to the defence objections in a way that shows why they did not undermine reliability. A similar caution is visible in domestic practice. In a first-instance Sky case, the presiding judge reportedly accepted Sky messages as evidence, but stressed that they could not stand as "the only evidence" and had to be linked to other material proof (Parojčić, 2023). If the court cannot describe that pathway, then relying on the item as sole or decisive is an obvious weakness, because the CPC treats missing, unclear, or materially inconsistent reasons as a serious procedural violation that can make the decision non-reviewable. The same discipline matters on appeal, since a second-instance court must engage with the grounds of appeal and state the reasons it examined. A properly reasoned contestability analysis is therefore what links first-instance reliance to meaningful appellate review.

AI-mediated processing as an additional contestability problem

The contestability logic developed here also applies where the evidential chain includes processed outputs rather than only raw communications. Encrypted-platform material is increasingly translated, clustered, summarised, or otherwise structured by automated tools before it reaches the courtroom (cf. Turanjanin, 2025, pp. 13-14). Once that processing becomes part of the evidential chain, contestability has to cover method as well as content.

From raw chats to investigative product

Encrypted-platform material rarely reaches court as a neutral dump of raw chats. It usually arrives as an investigative product that has already been filtered and shaped, with messages translated, duplicates removed, threads grouped by people or themes, and sometimes enriched with timelines, entity extraction, link analysis, and scoring meant to signal urgency or risk (cf. Oerlemans and Royer, 2023, pp. 447-458). Each of those steps can be partly automated, and each can shift meaning and evidential weight. Translation can smooth over ambiguity or bake in an interpretation, grouping can stitch separate threads together or break up what was originally continuous, while scoring can steer attention toward certain messages, devices, and suspects, which then drives the next steps in the case.

Contestability extends beyond denying authorship or disputing what the chats appear to say. It also covers whether the defence can test the reliability and relevance of the processing that produced the version of the dataset the court is being asked to accept. When the file is already curated, summarised, or risk-scored, the court is no longer dealing with raw evidence in any strict sense, but with the output of a pipeline. That pipeline introduces additional method-based premises into the case, including the existence of the chat, its linkage to a device, and the assumption that processing did not materially distort content, context, completeness, or the identification of what matters.

A processed output therefore needs meta-evidence, meaning documentation and verifiable traces that make the processing steps reviewable. Without that, challenge turns into guesswork, and a court that relies on the output ends up relying on a method while treating it as mere content. This is consistent with domestic appellate control, where a decision can be set aside as non-reviewable when it lacks reasons on decisive facts, which is exactly what an under-described contestability assessment risks producing (cf. Appellate Court in Kragujevac, Kž2Po1-7/23, 2023). The same logic appears in soft-law guidance. The CEPEJ Ethical Charter insists on transparency through explainability and external auditability, and on keeping legal professionals in effective control of tools rather than deferring to prescriptive outputs (see CEPEJ, 2018, p. 7).

What the AI Act benchmarks and what it does not

Where algorithms sit between raw messages and what the court finally sees, the EU AI Act offers a useful external benchmark. The point is that the AI Act's traceability and documentation logic indicates the kinds of records that can make a processed output reviewable in court, without suggesting that the Act formally governs law enforcement workflows in these cases. The same direction is visible at treaty level, because the Council of Europe Framework Convention requires relevant information about AI-assisted decisions to be documented and made available in a form sufficient for individuals to contest decisions and seek remedies (Council of Europe AI Convention, 2024, Art. 14(2)(a)-(b)). The AI Act pushes record-keeping that lets someone later reconstruct what the system did, which version was running, what inputs it used, and what oversight applied (Artificial Intelligence Act, 2024, Arts. 11-14).

But the AI Act is not evidentiary law and therefore does not determine admissibility, probative value, or the remedies triggered by failed disclosure. It is mainly ex-ante and compliance-focused, shaping how systems are built and governed before they are used. Contestability is ex-post and case-bound, because it asks what must be verifiable in a specific file, under time pressure, after a measure has already happened, and often under secrecy limits. A dataset can meet regulatory duties and still be unusable in court if the method-based premises cannot be tested.

In practice, four types of records translate the governance idea into courtroom contestability. First, processing logs that allow the court and the parties to reconstruct the key processing steps, at least when data was ingested, how it was changed, and which filters or rules were used. Second, tool version records, so the defence can see which software, model, or pipeline version produced the output the prosecution relies on. A concrete domestic analogue of this minimum log logic appears in scholarship on algorithmically mediated outputs and is reinforced by Serbia's information security framework, which requires the keeping and review of event logs and treats an audit trail as a baseline condition for meaningful ex-post verification (cf. Munjić, 2025, pp. 86-88; *Law on Information Security*, Art. 2(33) and Art. 10(23); *Decree on the Detailed Regulation of Protection Measures for ICT Systems of Special Importance*, Art. 18). Third, validation

material, including internal checks, known error modes, and any configuration records or performance notes that exist for the task, whether that is translation accuracy, the stability of clustering, or the thresholds used for scoring. Fourth, records of human review, because courts can ask who checked what, whether outputs were tested against source material, and how exceptions or anomalies were handled.

The standard should shift with the kind of output the prosecution puts in issue. If it relies on raw, inspectable data, disclosure can focus on provenance and integrity. If it relies on curated or risk-scored outputs, the defence needs enough material to interpret the output and verifiable traces of how it was produced, otherwise the output starts to function as an authority claim. That is where exclusion becomes a principled option, which tracks the need for defence access to raw data, forensic tools, and validation studies, and for participation or audit trails at determinative processing stages (Stoykova, 2024, p. 2). Legal systems differ on how they treat unlawfully obtained evidence and on what the minimum threshold for courtroom use should be (Quattrocolo, 2020, p. 76). Where verification is impossible and the defence has no realistic route to contestation, exclusion may be justified because the proceedings cannot deliver effective adversarial control over the mechanism (Quattrocolo, 2020, p. 96). The core evidentiary point is that processed outputs require meta-evidence sufficient to make their processing pathway reviewable. Without that minimum, adversarial contestation of the underlying material remains incomplete.

Conclusion

Domestic scholarship has correctly documented how encrypted-platform evidence enters domestic proceedings through admissibility routes and the EU cooperation framework. But admissibility is only the entry point. The real safeguard is contestability, understood as the defence's practical ability to test the method-relevant premises on which evidential reliance depends.

This paper has argued that structural opacity in EncroChat and Sky ECC cases is sustained by cross-border procedural architecture, confidentiality constraints, and restrained legality review under mutual recognition. Where that opacity persists, formal admissibility alone cannot secure fair evidential use. The defence may comment on the incriminating narrative, but it cannot test provenance, integrity, or attribution when key technical and organisational steps remain sealed. Adversarial review then becomes available in form but hollow in substance.

On that basis, the paper has advanced three responses. First, a minimal contestability test structured around provenance, integrity, and attribution, together with a staged verification package that can function under persistent secrecy. Second, a tiered remedial model in which evidence that remains practically untestable after reasonable verification steps cannot serve as sole or decisive proof, while non-decisive material carries sharply reduced weight and requires independent, contestable corroboration. Third, an operationalisation of this framework through existing Serbian CPC tools, including evi-

dentiary motions, expert examination, the exclusion-versus-weight distinction, and the reasoning duty, without legislative change. The EU AI Act remains relevant only as an external benchmark for traceability and documentation of processed outputs.

Courts should address this problem through a discipline of verification applied at the point where evidential reliance begins and reflected in the reasons whenever that reliance is challenged. Admissibility without contestability is a procedural form without adversarial substance. Evidence that cannot be meaningfully tested on provenance, integrity, and attribution should not serve as the sole or decisive basis for conviction.

References

Appellate Court in Kragujevac, Kž2-402/22, 7 July 2022.

Appellate Court in Kragujevac, Kž2-434/22, 19 July 2022.

Appellate Court in Kragujevac, Kž2-467/22, 19 July 2022.

Appellate Court in Kragujevac, Kž-Kre 11/2023, 29 May 2023.

Appellate Court in Kragujevac, Kž2-48/23, 24 January 2023.

Appellate Court in Kragujevac, Kž2-465/23, 22 August 2023.

Appellate Court in Kragujevac, Kž2Po1-7/23, 7 April 2023.

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. https://doi.org/10.1163/15718174-bja10062

Bundesgerichtshof (BGH). (2022). *Beschluss vom 2. März 2022, 5 StR 457/21 (EncroChat)*.

Clarifying Lawful Overseas Use of Data Act (*CLOUD Act*) (2018) Division V of the Consolidated Appropriations Act, 2018, Pub. L. No. 115-141, 132 Stat. 348, 23 March 2018.

Council of Europe (2024) *Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law* (CETS No. 225).

Council of Europe (2022) *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* (CETS No. 224).

Cour de cassation (2025). *Challenging the regularity of measures carried out within the national territory pursuant to a European Investigation Order (Ruling 24.84.262)*. Criminal Chamber, 16 September 2025. Available at: https://www.courdecassation.fr/toutes-les-actualites/2025/09/16/challenging-regularity-measures-carried-out-within-national (Accessed: 27 December 2025)

Court of Appeal of England and Wales, *A, B, D & C v R* [2021] EWCA Crim 128.

Court of Justice of the European Union (Grand Chamber) (2024) *Criminal proceedings against M.N. (EncroChat)*, Case C-670/22, Judgment of 30 April 2024.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for law enforcement purposes, OJ L 119, 04 May 2016.

Elola-Calderón, T. (2024) 'L'argot de la drogue dans le procès SKY ECC en Belgique. Quels défis pour l'interprète français-espagnol?', *Traduire*, 251, pp. 14-23. Available at: https://journals.openedition.org/traduire/4302 (Accessed: 12 January 2026)

EUR-Lex, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (*Artificial Intelligence Act*), OJ L, 2024/1689, 12.7.2024.

Eurojust (2024). *Cybercrime Judicial Monitor*, Issue 9.

European Commission for the Efficiency of Justice (CEPEJ) (2018) *European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*. Strasbourg: Council of Europe.

European Court of Human Rights (Fifth Section) (2024) *A.L. v. France* (Application no. 44715/20) and *E.J. v. France* (Application no. 47930/21), 24 September 2024.

European Court of Human Rights (Grand Chamber) (2000) *Jasper v. the United Kingdom*, Application no. 27052/95, Judgment of 16 February 2000.

European Court of Human Rights (Grand Chamber) (2000) *Rowe and Davis v. the United Kingdom*, Application no. 28901/95, Judgment of 16 February 2000.

European Court of Human Rights (Grand Chamber) (2004) Edwards and Lewis v. the United Kingdom, Applications nos. 39647/98 and 40461/98, Judgment of 27 October 2004.

European Court of Human Rights (Plenary) (1988) *Schenk v. Switzerland*, Application no. 10862/84, Judgment of 12 July 1988.

European Court of Human Rights (Second Section) (2017) *Matanović v. Croatia*, Application no. 2742/12, Judgment of 4 April 2017.

European Court of Human Rights (Third Section) (2000) *Khan v. the United Kingdom*, Application no. 35394/97, Judgment of 12 May 2000.

European Union Regulation (EU) 2023/1543 on European Production and Preservation Orders for electronic evidence, OJ L 243, 29 September 2023.

Fiorino, D. (2026) *'SkyECC and EncroChat: Italian Court Developments Strengthening Defence Challenges to Digital Evidence'*, Joint Defense Team, 4 February 2026. Available at: https://www.joint-defense-team.com/post/skeyecc-encrochat-italy-defence-evidence-challenges (Accessed: 20 March 2026)

Government of the Republic of Serbia, '*Decoding of the Sky application contributed to detecting the most serious criminal offences*', 7 July 2023. Available at: https://www.srbija.gov.rs/vest/717873/dekodiranje-sky-aplikacije-doprinelo-otkrivanju-najtezih-krivicnih-dela.php (Accessed: 16 January 2026)

Griffiths, C. and Jackson, A. (2022) 'Intercepted Communications as Evidence: The Admissibility of Material Obtained from the Encrypted Messaging Service EncroChat', *The Journal of Criminal Law*, *86*(4), 271-276. https://doi.org/10.1177/00220183221113455

Hoxhaj, A. (2025) 'The CJEU ruled that the EncroChat data can be admissible evidence in the EU', *European Journal of Risk Regulation, 16*(4), 1567-1579. https://doi.org/10.1017/err.2025.10047

Ilić, A. (2024) 'Kriptovana komunikacija u svetlu međunarodne pravne pomoći u krivičnim stvarima', *Izazovi međunarodnog krivičnog prava i krivičnog prava* [Challenges of international criminal law and criminal law] (Tom 1), 393-409. https://doi.org/10.51204/Zbornik_UMKP_25117A

Investigatory Powers Act (2016), UK Public General Acts, 2016, c.25.

International Organization for Standardization and International Electrotechnical Commission (2012) *ISO/IEC 27037:2012 Information technology: Security techniques. Guidelines for identification, collection, acquisition and preservation of digital evidence*. Available at: https://www.iso.org/standard/44381.html (Accessed: 15 January 2026)

Oerlemans, J.J. and Royer, S. (2023) 'The future of data-driven investigations in light of the Sky ECC operation', *New Journal of European Criminal Law*, *14*(4), 447-458. https://doi.org/10.1177/20322844231212661

Janusz-Pohl, B. (2025) 'About Constitutive Rules once again, Deliberation Based on the Judgment of 30 April 2024 of the CJEU in the EncroChat Case', *Izazovi međunarodnog krivičnog prava i krivičnog prava* [Challenges of international criminal law and criminal law] (Tom 2), 745-757. https://doi.org/10.51204/Zbornik_UMKP_25169A

Jocić, M. (2025) 'Korišćenje dokaza pribavljenih sa kriptovanih aplikacija (SKY, ECC i drugih)' [Use of evidence obtained from encrypted applications (SKY, ECC and others)], *Bilten Vrhovnog suda Republike Srbije* [Bulletin of the Supreme Court of the Republic of Serbia], 1/2025.

Lasagni, G. (2025) 'Admissibility of Digital Evidence', in: Franssen, V. i Tosza, S. (eds.) *The Cambridge Handbook of Digital Evidence in Criminal Investigations*. Cambridge: Cambridge University Press.

Merkevičius, R. (2025) 'The significance of the Court of Justice of the European Union judgment of 30 April 2024 in case C-670/22 ("EncroChat") for the admissibility of evidence in criminal proceedings', *International May Conference on Strategic Management*, XXI(1), https://doi.org/10.5937/IMCSM25551M

Munjić, J. (2025) 'Veštačka inteligencija u fudbalu: krivičnopravni izazovi i perspektive', in Stanić, M. (ed.) *Srpski fudbal – uporednopravni izazovi i perspektive V* [Serbian football - comparative legal challenges and perspectives V]. Beograd: Institut za uporedno pravo, 63-88. https://doi.org/10.56461/ZR_25.SF.13

Paunović, B. (2025) 'Dokazna upotrebljivost podataka dobijenih sa kriptovanih aplikacija' [Evidentiary admissibility of data obtained from encrypted applications], *Bilten Vrhovnog suda Republike Srbije* [Bulletin of the Supreme Court of the Republic of Serbia], 1/2025.

Parojčić, S., '*Šariću šest godina zatvora za pokušaj diskreditacije svedoka saradnika*', KRIK, 31.08.2023. Available at: https://www.krik.rs/saricu-sest-godina-zatvora-za-pokusaj-diskreditacije-svedoka-saradnika/ (Accessed: 14 January 2026)

Quattrocolo, S. (2020) *Artificial Intelligence, Computational Modelling and Criminal Proceedings: A Framework for A European Legal Discussion*. Cham: Springer. https://doi.org/10.1007/978-3-030-52470-8

Smart, R. and Mosley, O. (2021) 'Cracking the Enigma Code: A, B, D & C and Regina [2021] EWCA Crim 128', *QEB Hollis Whiteman*. Available at: https://www.qebholliswhiteman.co.uk/site/library/articles/cracking-the-enigma-code-a-b-d-c-and-regina-2021-ewca-crim-128 (Accessed: 26 December 2025)

Stoykova, R. (2024) 'A New Right to Procedural Accuracy: A Governance Model for Digital Evidence in Criminal Proceedings', *Computer Law & Security Review*, 55, 106040. https://doi.org/10.1016/j.clsr.2024.106040

Stoykova, R. (2023) 'Encrochat: The Hacker with a Warrant and Fair Trials?', *Forensic Science International: Digital Investigation*, 46, 301602. https://doi.org/10.1016/j.fsidi.2023.301602

Turanjanin, V. (2025) 'EncroChat, Sky ECC and Regulation (EU) 2023/1543: towards a new standards of digital evidence (I)', *Revija za kriminologiju i krivično pravo* [Journal of Criminology and Criminal Law], *63*(3), 7-30. https://doi.org/10.47152/rkkp.63.3.1.

Uredba o uređenju mera zaštite informaciono-komunikacionih sistema od posebnog značaja [Decree on the Detailed Regulation of Protection Measures for ICT Systems of Special Importance] (2016) Službeni glasnik RS, br. 94/2016.

Zakon o informacionoj bezbednosti [Law on Information Security] (2025) Službeni glasnik RS, br. 91/2025.

Zakonik o krivičnom postupku [Criminal Procedure Code] (2011) Službeni glasnik RS, br. 72/11, 101/11, 121/12, 32/13, 45/13, 55/14, 35/19, 27/21 i 62/21.

© 2026 by authors

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

Journal of Criminology and Criminal Law, 64(1), 103-123
Review paper
https://doi.org/10.47152/rkkp.64.1.6
UDK: 343.14/.15
342.738
341.231.14(4)

RECEIVED: 11 January 2026
ACCEPTED: 19 March 2026

The Strasbourg Standards of Mass Surveillance of Communications

Miloš Biberdžić[a]

This paper examines the standards governing mass surveillance of communications under the European Convention on Human Rights (ECHR), as developed in the jurisprudence of the European Court of Human Rights (ECtHR). It aims to identify, analyse, and systematise the Strasbourg standards binding the Contracting States in regulating mass surveillance of communications under the ECHR. The central research question is whether the Strasbourg case law provides a coherent and operational framework capable of reconciling national security imperatives with the effective protection of fundamental rights and freedoms. The analysis proceeds from doctrinal scholarship on mass surveillance, through an interpretative reading of the Convention, to a systematic assessment of the ECtHR's jurisprudence, with cases selected for their role in shaping the scope, limits, and safeguards of bulk interception. The paper demonstrates that, under the ECHR, the ECtHR permits mass surveillance only conditionally and subject to strict safeguards. The analysis identifies five cumulative Strasbourg standards, articulated through corresponding safeguards, that structure the assessment of mass surveillance under the European Convention on Human Rights: legality, independent oversight, data protection safeguards, proportionality, and effective remedies. Rather than operating as isolated requirements, these standards function as interdependent elements of a coherent framework.

KEYWORDS: mass surveillance, bulk interception, Strasbourg standards, data protection safeguards, proportionality, European Convention on Human Rights, chilling effect

[a] PhD student, Faculty of Law, University of Belgrade. E-mail: milos.biberdzic@gmail.com.

Introduction

Mass (or bulk) surveillance[1] involves the large-scale interception and analysis of telephone and internet communications, often encompassing individuals who are not under any reasonable suspicion of criminal activity. It is proactive, aiming to identify potential risks, and therefore employed by intelligence agencies as a tool to safeguard national security. However, due to its broad scope, lack of proportionality, and indiscriminate nature, mass surveillance may also pose a serious threat to human rights and civil liberties.

The collection of data through mass surveillance can profoundly affect the relationship between citizens and the state. An imbalance in access to information may tip the scales of power, limiting citizens' ability to exercise democratic oversight and hold accountable those elected to represent them (Forcese and Freeman, 2011, pp. 481–484, as cited in Newell, 2014, p. 482). To address this inevitable asymmetry of power, it is necessary to develop legal frameworks that ensure the effective protection of human rights. The distinction between democratic and autocratic systems rests largely on how the state perceives its citizens: as trusted rights-holders or as potential suspects (Bernal, 2016, p. 259). This tension between trust and suspicion is particularly visible in the digital age, where the use of mass surveillance has made repression more efficient and enabled authoritarian regimes to consolidate control through selective and data-driven means (Xu, 2021).

In Europe, mass surveillance practices have often evolved within a constitutional vacuum, allowing executive authorities to expand their powers even after global disclosures of extensive rights violations (Celeste and Formici, 2024, pp. 428-429). To prevent a threat to collective security from being replaced by the threat of excessive surveillance carried out by unchecked executive power and to ensure the protection of human rights, legislation must timely keep pace with developments in digital technologies and remain consistent with international human rights instruments. Mass surveillance must be regulated within national legal systems in full compliance with international treaties that guarantee human rights.

The European Convention on Human Rights (hereinafter: ECHR) represents the most significant regional human rights instrument of this kind, binding nearly all European states.[2] Its provisions are largely abstract, functioning as guiding legal principles. Therefore, understanding and interpreting them requires familiarity with the case law of the European Court of Human Rights in Strasbourg (hereinafter: ECtHR), which has, through its judgments, given them substantive content and true meaning (Beširević *et al*., 2017, p. 14).

This paper aims to systematize and critically assess the Strasbourg standards governing mass surveillance of communications, identifying the safeguards required for its

[1] The term *bulk surveillance* is often used in academic writing and recent ECtHR case law (e.g. *Big Brother Watch and Others v. UK* [GC]) to describe the large-scale, indiscriminate interception of communications data, while earlier judgments, such as *Weber and Saravia v. Germany*, referred to *strategic surveillance*. In this paper, however, the term *mass surveillance* is preferred for its clarity and broader recognition in both legal and public discourse.

[2] With the notable exceptions of the Vatican City State and Belarus.

legitimacy. The central research question asks whether the jurisprudence of the ECtHR provides a coherent and predictable framework for reconciling mass surveillance with the protection of fundamental rights. Methodologically, the paper proceeds from a doctrinal analysis of contemporary legal scholarship, through a normative interpretation of the relevant Convention provisions, to a jurisprudential examination of the ECtHR's case law. The study focuses on landmark ECtHR cases concerning bulk interception, selected for their precedential value and contribution to the development of safeguards. Against this background, the following chapter introduces the key conceptual foundations and normative assumptions underlying mass surveillance of communications.

The Specificities of Mass Surveillance

A precise understanding of the distinction between mass and targeted surveillance, the legal significance of metadata in relation to the content of communications, and the role of effectiveness of bulk interception of communications is essential for a doctrinal analysis of mass surveillance.

Mass Surveillance and Targeted Surveillance: A Normative Distinction

Mass surveillance of communications typically involves the large-scale interception, storage, and algorithmic processing of data transmitted via telephone or internet networks. Such operations are generally conducted by intelligence services without individualized suspicion or prior judicial authorisation (Slobogin, 2015, pp. 518, 522). Their proclaimed objective is to protect national security by identifying emerging threats through the analysis of communication patterns rather than content.

In contrast, targeted surveillance refers to the interception of communications based on prior judicial authorisation and the existence of procedurally relevant degree of suspicion that a specific individual or group is involved in criminal activity. Its primary purpose is the collection of evidence within a framework of procedural safeguards that ensure judicial oversight, necessity assessment, and proportionality control. Unlike mass surveillance, it operates on a case-by-case basis and presupposes a concrete link between the person monitored and a legitimate investigative purpose.

The distinction between mass and targeted surveillance is therefore not merely technical but normative. Targeted interception is anchored in individualized suspicion and judicial oversight. Mass surveillance, by contrast, may treat all individuals as potential subjects of monitoring and relies on institutional safeguards rather than personalized suspicion. Accordingly, its legitimacy under the Strasbourg framework depends on whether states can demonstrate that bulk interception regimes are governed by strict and effective safeguards derived from, yet adapted beyond, those applied in targeted surveillance.

Metadata and the Content of Communications: Conceptual and Normative Significance

Another central conceptual distinction concerns the differentiation between the content of communications and metadata. Content refers to the essence of communications, such as text, a photo and video message, or an audio recording of a conversation. The information collected through bulk interception consists primarily of metadata - data generated automatically whenever a digital device is used. Metadata is often described as "data about data" (Newell, 2014, pp. 487-488), and includes information such as the identities of communicating parties, the time, duration, and frequency of interactions, as well as geolocation and device identifiers. While metadata does not reveal the substantive content of communications, it can nevertheless disclose extensive information about an individual's private life. Contrary to the assumption that metadata represents a lesser intrusion, scholars have emphasized that it can, in many contexts, be more revealing than content itself (Bernal, 2018, p. 176). Metadata analysis enables intelligence agencies to map social networks, infer personal relationships, and construct detailed behavioural profiles. Whether based on data from law enforcement and security agencies or on automated analysis, algorithmic surveillance creates categories of individuals, sometimes with no obvious connection, whose rights still require protection (Kosta, 2020, p. 213). Through algorithmic processing, individuals may be categorized along political, ethnic, or religious lines, raising concerns over compliance with human rights standards.

From an operational perspective, metadata is often preferred to content data. It can be processed automatically by software or artificial intelligence, whereas content analysis usually requires human interpretation. Moreover, content may be protected by encryption or coded language, while metadata, as a by-product of device usage, is almost impossible to conceal (Bernal, 2018, p. 176). This makes metadata both more precise and more reliable as a tool for surveillance, but also more intrusive in its implications for privacy and autonomy.

This distinction is therefore normatively relevant not because metadata is inherently less sensitive than content, but because its large-scale collection and analysis can generate comparable, and in some contexts even greater, interferences with individual rights.

Assessing the Effectiveness of Mass Surveillance

One of the most frequently invoked arguments in favour of mass surveillance is its effectiveness in preventing terrorism, serious crime, and threats to national security. Effectiveness is often presented as a self-evident justification, grounded in the assumption that broader data collection enhances the ability of authorities to detect unknown threats. However, from a normative perspective, effectiveness cannot function as an autonomous or conclusive justification. Broader data collection does not necessarily correlate with increased public safety, for at least two reasons. First, intelligence agencies may face analytical overload, reducing the efficiency of targeted surveillance measures that have proven operationally effective. Second, increased surveillance may fuel public interest in protecting privacy, prompting wider use of encrypted communications. Consequently, some states have intro-

duced lawful hacking powers to bypass encryption, raising important concerns regarding privacy protection and the security of information systems (Pisarić, 2022, pp. 70-71).

Some official reports point to benefits of bulk surveillance such as network mapping, pattern recognition, resource efficiencies, and retrospective analysis (Murray and Fussey, 2019, pp. 36-43). Yet, critics argue that expanding data collection may only deepen inefficiency. A commonly used metaphor for mass surveillance is "searching for a needle in a haystack" (Richards, 2019; Logan, 2017), and building a bigger haystack, they contend, only makes the needle harder to find.[3]

This critique underlines a central normative dilemma: whether extensive data collection genuinely contributes to security or merely amplifies the risks of overreach, arbitrariness, and rights violations. The answer, as reflected in the Strasbourg Court's jurisprudence, which will be examined in greater detail in the following chapters, does not rest on the scope of surveillance itself, but on the quality of the legal framework and the effectiveness of institutional safeguards designed to prevent abuse and ensure accountability.

Mass Surveillance through the Lens of the ECHR: Legal Framework and Affected Rights

Before examining the standards developed in the jurisprudence of the European Court of Human Rights, this chapter sets out the Convention framework governing mass surveillance of communications. It identifies the Convention rights most directly affected by large-scale interception and analyses key judgments illustrating how such practices interfere with their effective enjoyment.

The ECtHR's Four-Stage Framework for Assessing Interference with Convention Rights in Mass Surveillance

The ECtHR has accepted the establishment of mass surveillance systems for the purpose of protecting national security, but only if adequate and effective safeguards are in place to prevent abuse. Without such safeguards, there is a risk that, under the pretext of national security, democratic processes may be undermined (*Big Brother Watch and Others v. UK* [GC], § 339; *Centrum för rättvisa v. Sweden* [GC], § 253). The Court has emphasized that mass surveillance is not inherently less intrusive than targeted surveillance. Intercepted and retained metadata must be afforded the same level of protection as communication content (*Ekimdzhiev and Others v. Bulgaria*, § 394).

According to the ECtHR, mass surveillance is a gradual process in which the degree of interference with human rights increases as the process advances. The Court identifies four distinct phases (*Big Brother Watch and Others v. UK* [GC], §§ 325-329*; Centrum för rättvisa v. Sweden* [GC], §§ 239-243):

[3] Joint Committee on the Draft Investigatory Powers Bill (2016).

Interception Phase: Intelligence agencies intercept electronic communications involving a large number of individuals, the overwhelming majority of whom are not of interest. Filtering at this stage is minimal or absent.

Initial Search Phase: The data is subjected to preliminary searches using strong selectors (e.g., specific email addresses) and/or complex search queries to identify relevant individuals.

Analytical Phase: Selected communications are examined by analysts for the first time.

Utilization Phase: Intelligence services make use of the intercepted material, typically by producing intelligence reports, which may be shared with other domestic or foreign security services.

Considered jointly, these four stages illustrate a structured model of state interference, in which each subsequent phase entails a progressively deeper intrusion into individual rights and therefore requires correspondingly stricter legal safeguards.

Mass Surveillance as a Multi-Rights Interference under the ECHR

Mass surveillance can be indiscriminate, potentially affecting both individuals who may give rise to reasonable suspicion and those who do not. It can also be disproportionate, insofar as it may impose significant burdens on individuals and society relative to the security benefits achieved (Macnish, 2020, p. 2).

While the primary implications of mass communication surveillance may concern the right to respect for private and family life, its effects on the right to a fair trial, freedom of thought, conscience, and religion, freedom of expression, freedom of assembly and association, and the prohibition of discrimination must not be overlooked. A narrow focus solely on the right to privacy may lead to an incomplete understanding of the broader risks posed by bulk surveillance, not only for individuals, but also for democratic society. Moreover, such a limited perspective may result in the application of unduly lenient standards when assessing the legitimacy and lawfulness of surveillance measures (Bernal, 2016, p. 252).

Interference with the Right to Respect for Private and Family Life (Article 8 ECHR)

Mass surveillance raises issues under Article 8 of the Convention due to its capacity to enable systematic access to information concerning individuals' private and family life. The ECtHR has consistently held that the right to respect for private life and correspondence under the ECHR encompasses postal, telephone, and email communications (*Kennedy v. the United Kingdom*, § 118), as well as internet searches, even when conducted from a workplace (*Copland v. the United Kingdom*, § 41). The concept of "correspondence" must be interpreted in light of technological developments, meaning that all modern forms of electronic communication, such as Viber, WhatsApp, Telegram, Signal and similar services, should fall within the protective scope of Article 8.

Examining mass surveillance exclusively from the perspective of correspondence could, however, be an unjustified simplification for two reasons. First, there is significant

overlap between the right to correspondence and the rights to private life, family life, and home, making it difficult to identify which specific aspect of Article 8 has been infringed. In particular, bulk surveillance represents both an interference with private life and a violation of the confidentiality of correspondence. Second, mass surveillance potentially interferes more deeply with private and family life than with correspondence, given that nearly all aspects of modern private life are directly or indirectly exposed online. From the standpoint of legitimacy, the crucial question is not whether the information is private, but how it is collected, analysed, and for what purpose. While the right to respect for private life is not absolute, any restriction must comply with the strict safeguards prescribed by the Convention. States are under a negative obligation to refrain from unlawful interference and a positive obligation to ensure the effective enjoyment of this right, subject to the strict conditions laid down in the Convention.

Interference with the Right to a Fair Trial (Article 6 ECHR)

The right to a fair trial constitutes one of the most fundamental procedural safeguards, providing effective protection for other rights that underpin individual freedoms (Ilić, 2011, p. 229). Mass surveillance of communications may affect this right in multiple ways.

The presumption of innocence, a cornerstone of fair trial guarantees, can be undermined by mass surveillance. Its broad, indiscriminate scope may foster a social climate in which individuals are treated as suspects before there is any legally threshold of suspicion. The presumption of innocence is closely linked to the duty of impartiality, which itself is a prerequisite for ensuring the equality of arms between the parties (Miljuš, 2021, p. 86).

Mass surveillance may compromise the confidentiality of communication between clients and legal counsel, interfering with the right to an adequate defence. The essential role of lawyers would be undermined if client communications could not remain confidential (*Michaud v. France*, § 118).

In cases where surveillance measures do not meet statutory standards, questions may arise regarding the admissibility of evidence obtained through such means. The ECtHR has not established comprehensive rules on evidence admissibility nor rigid standards for evidence assessment.[4] In general, the admissibility and evaluation of evidence, including material derived from secret surveillance measures, remains primarily governed by domestic law and determined by national courts (Ilić, 2021, p. 124). The Court's role is not to act as a final court of fourth instance, but to assess whether the proceedings as a whole, including the manner in which evidence was obtained, were fair (*Jalloh v. Germany* [GC], § 95). Its function is primarily supervisory, occasionally corrective, and only rarely directive (Dajović and Spaić, 2019, p. 182). This could be particularly relevant in cases of bulk surveillance, where individuals may be unable to identify whether, and to what extent, intercepted material has been used against them in criminal proceedings.

[4] The only absolute exception concerns evidence obtained through torture, which is inadmissible under all circumstances (Ilić, 2015, p. 80).

Interference with Freedom of Thought, Conscience and Religion (Article 9 ECHR)

Individuals may be deterred from freely expressing their views or religious beliefs when they are aware that their communications may be subject to mass surveillance. This phenomenon, commonly referred to as the *chilling effect*, can suppress free expression by instilling fear of state scrutiny. Studies indicate that human behaviour changes when we know we are being observed, leading us to act less freely, which in effect means we are less free.[5] Pervasive surveillance and the analysis of intercepted information may amplify the influence of powerful social actors, such as security agencies, in shaping individuals' choices and actions (Nissenbaum, 2009, p. 83).

Mass surveillance that disproportionately targets specific groups may lead to self-censorship, the homogenization of thought and belief, and ultimately undermine the principles of pluralism of opinion and freedom of religion. If directed at religious institutions, such surveillance can also impair their autonomy and freedom to operate independently. In *Miroļubovs and Others v. Latvia*, the Court emphasized that state interference in the internal affairs of a religious community, including through measures of oversight and control, can violate the right to freedom of religion (§§ 80–82).

Interference with Freedom of Expression (Article 10 ECHR)

The chilling effect also extends to the freedom of expression. Awareness of being under surveillance may create a societal climate in which individuals hesitate to express their opinions freely, fearing repercussions. Mass surveillance can identify and track individuals or groups expressing dissent, thereby suppressing opposing views and undermining the free exchange of ideas.

Bulk surveillance can also compromise anonymity, vital for expressing unpopular opinions without retaliation. Journalists may self-censor if they fear state monitoring, undermining press freedom, particularly when sources and communications are insufficiently protected (*Big Brother Watch and Others v. UK* [GC], §§ 447–450).

Freedom of expression underpins whistleblower protection, which is necessary to preserve the transparent and accountable functioning of institutions, especially where secrecy surrounding mass surveillance limits public scrutiny. Whistleblowers are entitled to protection under Article 10 when disclosing information in the public interest.[6]

Interference with Freedom of Assembly and Association (Article 11 ECHR)

Freedom of peaceful assembly is a cornerstone of democracy and must not be interpreted restrictively (*Djavit An v. Turkey*, § 56). Mass surveillance tools can monitor groups regardless of unlawful activity, creating a chilling effect on the exercise of free-

[5] Snowden, J. (2014) *Snowden Answers Our Burning Data Collection Question: What's the Worst That Could Happen?* Available at: https://techcrunch.com/2014/01/23/snowden-answers-our-burning-data-collection-question-whats-the-worst-that-could-happen/ (Accessed: 01 September 2025)

[6] The ECtHR has rightly recognised that, in certain circumstances, the public interest may outweigh the confidentiality obligations imposed on civil servants (*Guja v. Moldova* [GC], §§ 70–73).

dom of assembly and association. The ECtHR in the case of *Glukhin v. Russia* illustrates the chilling effect that mass surveillance may have on the right to freedom of assembly, especially when combined with emerging technologies such as facial recognition. The Court emphasized that indiscriminate surveillance of peaceful protestors, particularly through facial recognition, fails to satisfy the Convention safeguards (§§ 86–89). Freedom of assembly is especially significant for minorities, who rely on it to express cultural identity and protect collective rights (*Gorzelik and Others v. Poland*, § 93).

Interference with Prohibition of Discrimination (Article 14 ECHR)

Rights under the ECHR must be secured without discrimination. Mass surveillance can generate large datasets, which, when analysed automatically, may classify individuals along protected characteristics (sex, race, colour, language, religion, political opinion, national or social origin, minority status, property, birth, or other status), potentially resulting in discriminatory profiling. Selective or disproportionate targeting based on these characteristics constitutes discrimination if it lacks objective and reasonable justification. Discrimination arises where the measure fails to pursue a legitimate aim or where the means are not proportionate to the aim. (*Okpisz v. Germany*, § 33). States enjoy a margin of appreciation regarding differentiation in otherwise similar situations. Large-scale data collection, notwithstanding the exercise of substantial caution, may still produce discriminatory effects through the inadvertent reliance on variables that are correlated with protected groups (Barocas & Selbst, 2016, p. 675).

Mass surveillance is particularly prone to resulting in indirect discrimination, which occurs when a seemingly neutral measure or policy has a disproportionately negative impact on a particular individual or group (Beširević *et al*., 2017, p. 364).

Considered jointly, these dimensions illustrate that mass surveillance can threaten not only the privacy of individuals but the institutional integrity. The Strasbourg approach therefore treats surveillance as a multi-rights issue, demanding systemic safeguards rather than *ad hoc* justification. The next chapter explores how the Court has articulated these safeguards through its evolving standards of legality, independent oversight, data protection safeguards, proportionality and effective remedies.

Strasbourg Standards Governing Mass Surveillance - An Analysis of the ECtHR's Jurisprudence under the ECHR –

The European Court of Human Rights has consistently emphasized that the rights guaranteed by the European Convention on Human Rights must be practical and effective, rather than theoretical or illusory (*Airey v. Ireland*, § 24). In the field of communications surveillance, this principle requires that national legal frameworks clearly reflect the Convention's requirements as interpreted by the Court. These standards are shaped both by the text of the ECHR and by the Court's case law, which together constitute *European human rights law* (Popović, 2011, p. 344).

The Strasbourg Court has repeatedly underlined that bulk interception of communications may represent interference with fundamental rights and therefore demands strict justification and robust procedural safeguards. On the basis of an analysis of the ECtHR's jurisprudence, the following cumulative standards may be identified: legality, independent oversight mechanisms, data protection safeguards, proportionality and availability of effective legal remedies. These standards function as safeguards against arbitrariness and abuse and must be cumulative fulfilled for mass surveillance to comply with the Convention.

Although these safeguards are examined separately for analytical clarity, the Court's case-law treats them as interdependent and mutually reinforcing, making some overlaps inevitable in their analysis in this paper. The following sections examine these standards in the way in which the ECtHR applies them to assess the compatibility of mass surveillance regimes with the Convention, concluding with cases that illustrate the increasingly blurred line between targeted and bulk interception, particularly in the monitoring of encrypted communications.

Legality as a Structural Safeguard in Mass Surveillance

A core element of legality in Strasbourg jurisprudence is foreseeability. The laws,[7] including those governing mass interception regimes, must be formulated with sufficient clarity to enable individuals to foresee the consequences of their actions and understand potential sanctions (*Kafkaris v. Cyprus* [GC], § 140). This does not require predicting specific interception instances, but it does demand clear criteria for when and under what conditions surveillance may occur (*Malone v. the United Kingdom*, § 67; *Weber and Saravia v. Germany*, § 93). Foreseeability does not necessitate an exhaustive enumeration of offences that may justify targeted interception. Laws should define categories of offences and persons subject to surveillance (*Kennedy v. the UK*, § 159). Vague or overly broad legislation fails this standard (*Iordachi and Others v. Moldova*, § 41). Bulk surveillance laws cannot be too detailed or too concrete, because the whole power of such surveillance relies on the use of flexible algorithms (Kosta, 2020, p. 220). However, warrants should define categories of selectors (*Big Brother Watch and Others v. UK* [GC], §§ 351–352; *Centrum för rättvisa v. Sweden* [GC], §§ 265–266). When selectors relate to identifiable individuals, heightened safeguards are required (*Big Brother Watch and Others v. UK* [GC], § 355; *Centrum för rättvisa*, § 269). Particular attention should be given to *contact chaining*, a technique for identifying individuals connected to a surveillance target through metadata analysis. As it risks extending surveillance beyond the original target, the law must clearly define its permissible scope, including limits on the number of "hops" and criteria for querying bulk data (Watt, 2017, p. 788). While foreseeability remains a key element of legality, in the field of mass surveillance its role has been partially reinterpreted. As mass surveillance is inherently secret, the ECtHR has shifted its focus from individual predictability toward structural safeguards capable of preventing abuse (Van der Sloot, 2020).

Accessibility is another integral element of the legality requirement, and ensures that the legal framework governing surveillance is open to public scrutiny. This requires that

[7] The ECtHR interprets "law" broadly, encompassing statutes, subordinate legislation, judicial practice (*Sunday Times v. the UK*, § 47), and even unwritten law (*Kafkaris v. Cyprus* [GC], § 139).

surveillance laws be publicly available, published online, and adopted by the legislature before entering into force (*Kennedy v. the UK*, § 157).

The Court's approach to legality was further clarified in the twin Grand Chamber judgments of *Big Brother Watch and Others v. the UK* and *Centrum för rättvisa v. Sweden*, where it affirmed that bulk interception may be compatible with the Convention, provided that strict safeguards are in place. These safeguards build upon the criteria first developed in *Roman Zakharov v. Russia* [GC], where the Court found that an abstract review of surveillance law was justified given its secret nature, broad scope, and lack of effective remedies. The Court held that the mere existence of a legal framework permitting secret surveillance, if it fails to provide adequate safeguards, may in itself amount to a violation of the Convention (§ 178).

Although the ECtHR's review in these cases has primarily been in abstracto due to the secrecy surrounding surveillance operations, the principle of legality remains the cornerstone of Convention-compatible surveillance, ensuring that state power is exercised within clearly defined limits. However, the availability of abstract scrutiny of mass surveillance does not by itself guarantee stronger protection of privacy in practice, as the ECtHR has been criticized for the limited enforceability of its judgments (Carpenter, 2021, p. 54). The Strasbourg Court acknowledges that legislation is drafted for general application and that legislative technique cannot achieve absolute precision. It therefore allows national courts to interpret laws in line with societal needs (Kononov v. Latvia [GC], § 185), while refraining from reviewing such interpretations unless there is flagrant non-observance or arbitrariness (Huhtamäki v. Finland, § 52). Overall, the Court's approach suggests that legality in mass surveillance functions primarily as a structural safeguard for organizing and reviewing surveillance powers.

Independent Oversight as a Constraint on Executive Discretion

To establish adequate and effective safeguards against abuse, it is essential to ensure independent oversight of the operation of mass surveillance regimes (*Weber and Saravia v. Germany*, § 117). The decisive criterion in assessing an oversight body is not its formal designation as a court or administrative authority, but the existence of substantive guarantees of independence and impartiality. Such guarantees include autonomy from the executive, objective and transparent procedures for the appointment and tenure of members, and effective protection against external influence or pressure (Mitsilegas *et al*., 2021, p. 197). In its jurisprudence, the ECtHR has developed two main models of oversight: judicial and non-judicial.

Judicial oversight provides the strongest guarantees of impartiality and independence. The rule of law requires the existence of an effective judicial system capable of providing redress in cases of violations of human rights and fundamental freedoms (Ilić, 2021, p. 120). Even in the context of espionage or counter-terrorism, states cannot exercise unfettered discretion to monitor individuals (*Klass and Others v. Germany*, §§ 48, 55). Accordingly, restrictions on the rights of citizens must remain subject to judicial review, which serves as a benchmark for the effectiveness of protective mechanisms internationally (Ilić, 2011, p. 228).

Non-judicial oversight can also provide effective protection, provided that the bodies entrusted with such tasks are vested with the competence and authority to exercise meaningful control (*Leander v. Sweden*). While prior judicial authorisation is an important safeguard, it is not absolute; bulk interception may be authorised by independent of the executive (*Big Brother Watch and Others v. UK* [GC], § 351; *Centrum för rättvisa v. Sweden* [GC], § 265). To prevent abuse, an independent authority should be informed of the purpose of the interception, targets, communication channels involved, including the choice of selectors (*Big Brother Watch and Others v. UK* [GC], § 352; *Centrum för rättvisa v. Sweden* [GC], § 266). The Court requires end-to-end safeguards, encompassing prior authorisation by an independent authority, continuous supervision, and *ex post facto* review of completed operations (*Big Brother Watch and Others v. UK* [GC], § 361; *Centrum för rättvisa v. Sweden* [GC], § 264).

Taken together, these requirements indicate that independent oversight functions as a structural constraint on executive discretion, ensuring that surveillance powers remain subject to ongoing institutional control.

Data Protection Safeguards as a Limitation on Data Use and Retention

Data protection constitutes a regulatory framework establishing a coherent set of rules and principles governing all forms of personal data processing, irrespective of whether such processing is carried out by automated means or otherwise (Lynskey, 2023, pp. 300, 302). In the context of mass surveillance, it requires that individuals be duly informed about the collection, processing, and storage of their personal data, and that appropriate safeguards ensure the preservation of privacy and data security. In *Rotaru v. Romania* the Court broadened the notion of "surveillance" to include the systematic collection and retention of personal data, even where the information is publicly available (§§ 43, 46).

The Strasbourg Court has articulated three core standards concerning data protection safeguards in the context of bulk surveillance activities. First, data may only be used for the purposes for which they were collected. Second, the possibility of sharing the collected data with other state authorities must be strictly limited. Third, personal data must be stored securely and destroyed once they are no longer necessary for the pursuit of a legitimate aim (*Weber and Saravia v. Germany*, § 116). When assessing the handling of material obtained through targeted interception, the Court has further held that the law should strictly limit the number of persons to whom such material may be disclosed, require an appropriate level of security clearance for those with access, and prescribe that disclosure should occur only on a "need-to-know" basis (*Kennedy v. the UK*, § 163).

Recent judgments, such as *Pietrzak and Bychawska-Siniarska and Others v. Poland*, reiterated that the widespread retention of communications data by service providers, and their subsequent processing by the authorities, must be accompanied, *mutatis mutandis*, by safeguards and protective measures against abuse comparable to those applicable to targeted secret surveillance (§ 250). The Court observed that retained metadata enable the creation of an "intimate portrait" (*un portrait intime*) of the person concerned, revealing

social interactions, movements, browsing habits, and communication patterns, and therefore amount to an interference with the individual's private sphere (§ 253). More recently, the ECtHR emphasized in *Podchasov v. Russia* that the mere existence of laws requiring service providers to decrypt end-to-end encrypted communications, without any individualized suspicion or prior justification, constitutes a disproportionate interference that compromises user security and violates the right to respect for private life.

As mass surveillance often involves transnational data exchange, the absence of clear international rules on cross-border transfer and use of intercepted data creates an additional challenge. Without such regulation, states may indirectly circumvent domestic restrictions, weakening both accountability and the protection of individual rights. In this regard, the *Big Brother Watch* Grand Chamber judgment represents a pivotal development, as it was the first to address international intelligence sharing under the Convention. The Court adopted a cautious and deferential stance, accepting that states may exchange information obtained through mass surveillance provided that adequate safeguards are effectively implemented (Zalnieriute, 2022).

In this sense, Court's jurisprudence suggests that data protection safeguards in the context of mass surveillance function as limitation on the use, retention, and circulation of intercepted data, rather than as a barrier to data collection as such.

Proportionality in Bulk Interception Regimes

According to the principle of proportionality, derogations and limitations on the protection of human rights must be applied only to the extent that they are strictly necessary and accompanied by minimum safeguards providing individuals with sufficient guarantees to effectively protect their rights against abuse (Vogiatzoglou, 2019). However, mass surveillance is by its very nature difficult to reconcile with this principle, as it involves the collection of data whose necessity cannot be demonstrated, or even assessed, prior to their acquisition (Rojszczak, 2021, p. 57). In the context of mass surveillance, proportionality therefore requires that any measure be both necessary and proportionate with the legitimate aim pursued. Where such measures exceed what is required to address the threat at issue, they risk undermining fundamental rights through excessive monitoring. The Strasbourg Court found a system of targeted surveillance to be "excessively used" where domestic courts had granted virtually all prosecutorial requests for interception warrants over a three-year period (*Iordachi and Others v. Moldova*, § 52).

Legislation permitting secret monitoring may be necessary and proportionate when aimed at safeguarding national security and preventing crime (*Weber and Saravia v. Germany*, § 148). States are therefore required to assess necessity and proportionality at every stage of a bulk surveillance operation (*Big Brother Watch and Others v. UK* [GC], § 350). When assessing proportionality, states enjoy a margin of appreciation in determining whether interferences with individual rights are necessary to protect national security (*Weber and Saravia v. Germany*, § 106). This margin rests on the premise that national authorities are better placed to evaluate how Convention provisions are to be

applied within their domestic legal systems (Popović, 2008, p. 110). However, given that broad discretion in the conduct of bulk surveillance may *ab initi*o compromise proportionality, strict compliance with the other Strasbourg standards remains indispensable.

The proportionality requirement also mandates that the law clearly define the maximum duration of surveillance measures and the conditions for their extension. Targeted interception should be limited in time; extensions may be granted only upon a fresh request that complies with statutory conditions. Once the grounds for surveillance no longer exist, the measure must be terminated without delay (*Weber and Saravia v. Germany*, § 116). Although these temporal safeguards were initially formulated in the context of targeted interception, they are equally applicable to bulk surveillance, where the risks of prolonged and disproportionate interference with privacy are even greater. The ECtHR confirmed this approach emphasizing that the same fundamental safeguards, including strict temporal limits, must govern both targeted and bulk interception (*Big Brother Watch and Others v. the UK* [GC], §§ 314–317). Some flexibility may be permitted, depending on the complexity of an investigation, but only if adequate procedural and institutional safeguards are in place (*Kennedy v. UK*, § 161). In assessing proportionality, the Court also considers the fairness of the procedure, the availability of less intrusive means to achieve the legitimate aim, the existence of a pressing social need, and the extent to which the essence of the right was impaired (Paunović and Carić, 2006, p. 20).

Overall, the ECtHR's approach indicates that proportionality in mass surveillance extends beyond the initial authorization and depends on the combined operation of temporal limits and procedural guarantees.

The Right to an Effective Remedy

Everyone whose rights and freedoms guaranteed by the ECHR have been violated is entitled to an effective remedy before national authorities, even where the interference results from acts of public officials performed in an official capacity, including in the context of mass surveillance.

A defining feature of both mass and targeted surveillance is secrecy. Since the effectiveness of such measures depends on confidentiality, the ECtHR has held that a remedy must be available once the existence of secret measures is disclosed to the individual concerned (*Segerstedt-Wiberg and Others v. Sweden*, § 117). In this field as well, the Court has developed a set of general safeguards applicable to mass surveillance.

The Court requires that the totality of remedies under domestic law be effective (*Leander v. Sweden*, § 77). Several individually ineffective remedies cannot cumulatively amount to one effective remedy (*Leander v. Sweden, partly dissenting opinion of judges Pettiti and Russo*). A constitutional complaint may also qualify as an effective remedy (*Marinković v. Serbia*, § 59), making its use a necessary precondition for access to Strasbourg.

An effective remedy must be capable of rectifying an alleged violation and offer a reasonable prospect of success, without requiring certainty of a favourable outcome (*Lorse and Others v. Netherlands*, § 96). Remedies cannot exist merely in abstract terms; they

must also function effectively in practice, and it is for the state to demonstrate this (*Iovchev v. Bulgaria*, § 142).

Importantly, in the context of bulk interception, the Court has recognised that remedies not dependent on notification of the subject may still be effective and may even provide stronger safeguards than systems that rely on *ex post facto* notification (*Big Brother Watch and Others v. UK* [GC], § 358; *Centrum för rättvisa v. Sweden* [GC], § 272).

The Court's jurisprudence indicates that the right to an effective remedy in the context of mass surveillance is primarily ensured through the existence of institutional mechanisms capable of independent review and correction, rather than through individual notification and participation. In this sense, the right to an effective remedy completes the system of Strasbourg safeguards by linking legality, oversight, data protection, and proportionality to mechanisms of review and accountability.

Viewed together, these standards form a coherent legal framework through which the ECtHR assesses the legitimacy of mass interception regimes. Yet, as technology evolves and surveillance techniques grow more sophisticated, the distinction between targeted and bulk interception becomes harder to sustain in practice, as illustrated by the Court's recent jurisprudence. Accordingly, the following section briefly considers cases in which technological developments have blurred this distinction, challenging the traditional boundaries of lawful surveillance.

The Blurred Line Between Mass and Targeted Surveillance

The rapid evolution of digital technologies is increasingly challenging the traditional dichotomy between targeted and mass surveillance. Encryption, anonymization tools, and the global flow of data have made conventional distinctions based on scope, selectivity or purpose increasingly blurred. In several recent cases, the ECtHR has confronted surveillance practices that, while formally targeted, relied on mass interception or algorithmic filtering of vast data sets to identify potential threats. Such techniques effectively merge preventive intelligence gathering with individualized monitoring, resulting in a hybrid form of surveillance.

Cases involving the surveillance of encrypted communications illustrate how the line between targeted and mass surveillance can quickly become blurred. They reveal broader structural challenges, including the fragmentation of procedural safeguards, the tension between investigative efficiency and the protection of fundamental rights, and the limitations of existing instruments such as the European Investigation Order (Turanjanin, 2025, p. 10). Investigations initially aimed at specific individuals or entities may ultimately affect thousands of users. One illustrative example is the EncroChat platform[8], where criminal proceedings against the company led to the interception of communications from thousands of users, subsequently triggering large-scale prosecutions (See more in: Bajović, 2022).

[8] EncroChat was an encrypted communication service primarily used via modified smartphones, marketed as a secure platform for private messaging. It was dismantled in a joint law enforcement operation in 2020, revealing widespread criminal use of the network (Europol, 2020).

The ECtHR addressed the surveillance of encrypted communications in *Yüksel Yalçınkaya v. Turkey [GC],* where the applicant's conviction was based on his use of the ByLock messaging app. Turkish authorities treated all users as members of the "Gülen movement," creating an almost irrebuttable presumption of guilt and denying individuals the chance to challenge the evidence. The Court found systemic violations of several Convention rights and ordered general measures on the judicial assessment of ByLock evidence (§§ 414, 416). However, it did not rule on the broader legality of encrypted communication surveillance (Škulić, 2024, pp. 38-39). The judgment illustrates the Court's cautious approach toward surveillance of encrypted communications, focusing on due process guarantees rather than on establishing broader principles governing state access to encrypted data.

When bulk interception tools are used to extract or analyse the communications of specific individuals, procedural safeguards designed for targeted surveillance must apply with equal rigor. Conversely, when targeted measures rely on large-scale data collection, states must ensure that prior judicial authorisation is obtained, that a procedurally relevant degree of suspicion exists linking a specific individual or group to criminal activity, that temporal limits are clearly defined, and that the necessity and proportionality of the measure are subject to continuous oversight throughout its implementation.

The Convention framework is designed to balance the imperatives of collective security with the protection of individual rights. However, the emergence of advanced surveillance technologies increasingly strains its capacity to preserve this equilibrium. Ensuring effective human rights protection therefore depends on the consistent application of Strasbourg standards of legality, independent oversight, data protection safeguards, proportionality and effective remedies to all emerging forms of surveillance, irrespective of their technical configuration.

Conclusion

The analysis demonstrates that, under the European Convention on Human Rights, mass surveillance of communications is permitted only conditionally and subject to a set of strict and cumulative Strasbourg standards developed in the jurisprudence of the European Court of Human Rights. Rather than rejecting bulk interception as such, the Strasbourg Court has articulated a framework within which its compatibility with the ECHR depends on the fulfillment of multiple interrelated standards, operationalised through corresponding safeguards.

Five core standards emerge consistently from the Court's case law: legality, independent oversight, data protection safeguards, proportionality, and effective remedies. These standards are cumulative rather than alternative; each loses meaning if not supported by the others. Legality structures the exercise of surveillance powers within a clear, accessible, and foreseeable legal framework. Independent oversight constrains executive discretion through mechanisms of authorization, supervision, and review. Data protection safeguards limit the collection, use, retention, and dissemination of intercepted data. Proportionality requires

that all measures remain necessary and strictly limited to the legitimate aim pursued. Finally, effective remedies ensure that surveillance measures are subject to mechanisms of institutional review and accountability capable of identifying, correcting, and, where appropriate, redressing unlawful interferences, even in the absence of individual notification.

Taken together, these standards, reflected through a set of cumulative safeguards, constitute a systematic model of human rights compliance under the Convention. Their interdependence implies that weaknesses in one dimension (e.g. oversight) cannot be compensated by the formal strength of another (e.g. legality). Strasbourg case law thus offers not only a catalogue of standards but a functional framework for assessing whether national surveillance regimes respect the essence of the right to privacy.

The findings further indicate that compliance with Strasbourg standards depends not only on their formal recognition in domestic law, but also on their effective implementation in practice. The operation of independent supervisory bodies, the quality of judicial review, and the institutional capacity to enforce data protection requirements play a decisive role in determining whether surveillance frameworks function in a Convention-compliant manner. In this respect, the Court's case law highlights structural risks that may arise where safeguards remain declarative rather than operational. At the international level, the lack of harmonized rules governing cross-border access to and exchange of intercepted data presents additional challenges for the effective application of Convention standards. Differences between national legal regimes may create gaps in oversight and accountability, particularly in relation to metadata processing and international intelligence cooperation.

Overall, Strasbourg case law offers a structured set of safeguards for assessing mass surveillance under the Convention, which form cumulative standards according to which such measures can be considered compatible with the rights and freedoms protected by the Convention.

References

Bajović, V. (2022) 'EncroChat i Sky ECC komunikacija kao dokaz u krivičnom postupku', *CRIMEN*, *13*(2), 154-179. https://doi.org/10.5937/crimen2202154B

Barocas, S. and Selbst, A.D. (2016) 'Big data's disparate impact', *Calif. L. Rev.*, 104, 671-732. https://doi.org/10.2139/ssrn.2477899

Bernal, P. (2016) 'Data gathering, surveillance and human rights: recasting and debate', *Journal of Cyber Policy*, *1*(2), 243-264. https://doi.org/10.1080/23738871.2016.1228990

Bernal, P. (2018) *The Internet, warts and all: Free speech, privacy and truth*. Cambridge: Cambridge University Press.

Beširević, V. *et al*. (2017) *Komentar Konvencije za zaštitu ljudskih prava i osnovnih sloboda*. Beograd: Službeni glasnik.

Carpenter, C. (2020) 'Privacy and proportionality: Examining mass electronic surveillance under Article 8 and the Fourth Amendment', *International and Comparative Law Review*, *20*(1), 27-57. https://doi.org/10.2478/iclr-2020-0002

Celeste E. and Formici G. (2024) 'Constitutionalizing Mass Surveillance in the EU: Civil Society Demands, Judicial Activism, and Legislative Inertia', *German Law Journal*, *25*(3), 427-446. https://doi.org/10.1017/glj.2023.105

Dajović, G. and Spaić, B. (2019) 'Doktrina "četvrte instance" i pravo na obrazloženu presudu u praksi Evropskog suda za ljudska prava', *Anali Pravnog fakulteta u Beogradu*, *67*(3), 158-185. https://doi.org/10.5937/AnaliPFB1903166D

ECtHR, *Airey v. Ireland*, no. 6289/73, Judgment of 9 October 1979 (*Airey v. Ireland*)

ECtHR, *Big Brother Watch and Others v. UK*, nos. *58170/13, 62322/14 and 24960/15*, Judgment of 25 May 2021[GC] (*Big Brother Watch and Others v. UK* [GC])

ECtHR, *Centrum för rättvisa v. Sweden*, no. 35252/08, Judgment of 25 May 2021 [GC] (*Centrum för rättvisa v. Sweden* [GC])

ECtHR, *Copland v. UK*, no. 62617/00, Judgment of 03 April 2007 (*Copland v. UK*)

ECtHR, *Djavit An v. Turkey*, no. 20652/92, Judgment of 20 February 2003 (*Djavit An v. Turkey*)

ECtHR, *Ekimdzhiev and Others v. Bulgaria*, no. 70078/12, 11 January 2022 (*Ekimdzhiev and Others v. Bulgaria*)

ECtHR, *Glukhin v. Russia*, no. 11519/20, Judgment of 4 July 2023 (*Glukhin v. Russia*)

ECtHR, *Gorzelik and Others v. Poland*, no. 44158/98, Judgment of 17 February 2004 (*Gorzelik and Others v. Poland*)

ECtHR, *Guja v. Moldova* [GC], no. 14277/04, Judgment of 12 February 2008 [GC] (*Guja v. Moldova* [GC])

ECtHR, *Huhtamäki v. Finland*, no. 54468/09, Judgment of 6 March 2012 (*Huhtamäki v. Finland*)

ECtHR, *Iordachi and Others v. Moldova*, no. 25198/02, Judgment of 10 February 2009 (*Iordachi and Others v. Moldova*)

ECtHR, *Iovchev v. Bulgaria*, no. 41211/98, Judgment of 2 February 2006 (*Iovchev v. Bulgaria*)

ECtHR, *Jalloh v. Germany*, no. 54810/00, Judgment of 11 July 2006 [GC] (*Jalloh v. Germany* [GC])

ECtHR, *Kafkaris v. Cyprus*, no. 21906/04, Judgment of 12 February 2008 [GC] (*Kafkaris v. Cyprus* [GC])

ECtHR, *Kennedy v. UK*, no. 26839/05, Judgment of 18 May 2010 (*Kennedy v. UK*)

ECtHR, *Kononov v. Latvia*, no. 36376/04, Judgment of 17 May 2010 [GC] (*Kononov v. Latvia* [GC])

ECtHR, *Leander v. Sweden*, no. 9248/81, Judgment of 26 March 1987 (*Leander v. Sweden*)

ECtHR, *Lorse and Others v. Netheralands*, no. 52750/99, Judgment of 4 February 2003 (*Lorse and Others v. Netheralands*)

ECtHR, *Malone v. UK*, no. 8691/79, Judgment of 2 August 1984 (*Malone v. UK*)

ECtHR, *Marinković v. Serbia*, no. 5353/11, Judgment of 22 October 2013 (*Marinković v. Serbia*)

ECtHR, *Michaud v. France*, no. 12323/11, Judgment of 6 December 2012 (*Michaud v. France*)

ECtHR, *Miroļubovs and Others v. Latvia*, no. 798/05, Judgment of 15 September 2009 (*Miroļubovs and Others v. Latvia*)

ECtHR, *Okpisz v. Germany,* no. 59140/00, Judgment of 25 October 2005 (*Okpisz v. Germany*)

ECtHR, *Pietrzak and BychawskaSiniarska and Others v. Poland,* nos. 72038/17 and 25237/18 Judgment in French of 3 February 2022 (*Pietrzak and BychawskaSiniarska and Others v. Poland*)

ECtHR, *Podchasov v. Russia*, no. 33696/19, Judgment of 13 February 2024 (*Podchasov v. Russia*)

ECtHR, *Roman Zakharov v. Russia*, no. 47143/06, Judgment of 4 December 2015 [GC] (*Roman Zakharov v. Russia* [GC])

ECtHR, *Rotaru v. Romania*, no. 28341/95, Judgment of 4 May 2000 (*Rotaru v. Romania*)

ECtHR, *Segerstedt-Wiberg and Others v. Sweden,* no. 62332/00, Judgment of 6 June 2006 (*Segerstedt-Wiberg and Others v. Sweden*)

ECtHR, *Sunday Times v. UK*, no. 6538/74, Judgment of 26 April 1979 (*Sunday Times v. UK*)

ECtHR, *Weber and Saravia v. Germany*, no. 54934/00, Judgment of 29 June 2006 (*Weber and Saravia v. Germany*)

ECtHR, *Yüksel Yalçınkaya v. Turkey*, no. 15669/20, Judgment of 26 September 2023 [GC] *(Yüksel Yalçınkaya v. Turkey* [GC])

Europol (2020) *Dismantling of encrypted network sends shockwaves through organised crime groups across Europe*. Available at: https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe(Accessed: 15 September 2025)

Ilić, G. P. (2011) 'Pravo na obrazloženu sudsku odluku', *CRIMEN*, *2*(2), 227-244.

Ilić, G. P. (2015) 'O nezakonitim dokazima u krivičnom postupku', *Kaznena reakcija u Srbiji*, 5, 75-87.

Ilić, G. P. (2021) 'Arbitrarna primena prava i pravo na pravično suđenje', *Kaznena reakcija u Srbiji*, 11, 120-138.

Joint Committee on the Draft Investigatory Powers Bill (2016) *Oral Evidence: Draft Investigatory Powers Committee*. Available at: https://www.parliament.uk/globalassets/documents/joint-committees/draft-investigatory-powers-bill/oral-evidence-draft-investigatory-powers-committee.pdf (Accessed: 17 September 2025)

Kosta, E. (2020) 'Algorithmic state surveillance: Challenging the notion of agency in human rights', *Regulation & Governance,* 16, 212-224. https://doi.org/10.1111/rego.12331

Logan, S. (2017) 'The needle and the damage done: Of haystacks and anxious panopticons', *Big Data & Society*, *4*(2), 1-13. https://doi.org/10.1177/20539517177345

Lynskey, O. (2023) 'Complete and effective data protection', *Current Legal Problems*, *76*(1), 297-343. https://doi.org/10.1093/clp/cuad009

Macnish, K. (2020) 'Mass surveillance: A private affair?', *Moral Philosophy and Politics*, *7*(1), 9-27. https://doi.org/10.1515/mopp-2019-0025

Miljuš I. (2021) *Načelo jednakosti "oružja" u krivičnom postupku*. Doktorska disertacija. Univerzitet u Beogradu.

Mitsilegas, V. *et al*. (2023) 'Data retention and the future of large scale surveillance: The evolution and contestation of judicial benchmarks', *European Law Journal*, *29*(1-2), 176-211. https://doi.org/10.1111/eulj.12417

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

Newell, B. C. (2014) 'The massive metadata machine: Liberty, power, and secret mass surveillance in the US and Europe', *ISJLP*, *10*(2), 481-522.

Nissenbaum, H. (2010) *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press. https://doi.org/10.1515/9780804772891

Paunović, M. and Carić, S. (2006) *Evropski sud za ljudska prava osnovna načela i tok postupka*. Beograd: Pravni fakultet Univerziteta u Beogradu.

Pisarić, M. (2022) 'Communications encryption as an investigative obstacle', *Revija za kriminologiju i krivično pravo*, *60*(1), 61-74. https://doi.org/10.47152/rkkp.60.1.4

Popović, D. (2008) *Evropski sud za ljudska prava: između 11. i 14. dodatnog protokola uz konvenciju za zaštitu ljudskih prava i osnovnih sloboda*. Beograd: Službeni glasnik.

Popovic, D. (2011) 'Uticaj Evropske Konvencije za zaštitu ljudskih prava i osnovnih sloboda na srpsko zakonodavstvo i sudsku praksu', *Pravni Zapisi*, *2*(2), 343-357. https://doi.org/10.5937/pravzap1102343p

Richards, J. (2019) 'Needles in haystacks: law, capability, ethics, and proportionality in big data intelligence-gathering', *Secret Intelligence*, 2, 422-431. https://doi.org/10.4324/9780429029028-28

Rojszczak, M. (2021) 'Extraterritorial bulk surveillance after the German BND act judgment', *European Constitutional Law Review*, *17*(1), 53-77. https://doi.org/10.1017/S1574019621000055

Škulić, M. (2024) 'Dokazni značaj informacija iz komunikacije ostvarene aplikacijama/modifikovanim uređajima za kriptovanje - kao što su Sky ecc i Enchrochat', *CRIMEN*, *15*(1), 3-55. https://doi.org/10.5937/crimen2401003S

Slobogin, C. (2015) 'Standing and covert surveillance', *Pepperdine Law Review*, *42*(3), 517-548.

Snowden, J. (2014) *Snowden Answers Our Burning Data Collection Question: What's the Worst That Could Happen?* Available at: https://techcrunch.com/2014/01/23/snowden-answers-our-burning-data-collection-question-whats-the-worst-that-could-happen/ (Accessed: 01 September 2025)

Turanjanin, V. (2025) 'EncroChat, Sky ECC and Regulation (EU) 2023/1543: towards a new standards of digital evidence (I)', *Revija za kriminologiju i krivično pravo*, 62(1), 7-30. https://doi.org/10.47152/rkkp.63.3.1

Van der Sloot, B. (2020) 'The quality of law: How the European Court of Human Rights gradually became a European Constitutional Court for privacy cases', *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 11, 160-185.

Vogiatzoglou, P. (2019) 'Mass surveillance, predictive policing and the implementation of the CJEU and ECtHR requirement of objectivity', *European Journal of Law and Technology*, *10*(1).

Watt, E. (2017) 'The right to privacy and the future of mass surveillance', *The International Journal of Human Rights*, *21*(7), 773–799. https://doi.org/10.1080/13642987.2017.1298091

Xu, X. (2021) 'To repress or to co-opt? Authoritarian control in the age of digital surveillance', *American Journal of Political Science*, *65*(2), 309-325. https://doi.org/10.1111/ajps.12514

Zalnieriute, M. (2022) 'Big brother watch and others v. the United Kingdom', *American Journal of International Law*, *116*(3), 585-592. https://doi.org/10.1017/ajil.2022.35

© 2026 by authors

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

Journal of Criminology and Criminal Law, 64(1), 125-128
Book Review

Baranowska, G. & Kolaković-Bojović, M. (2025) *Enforced Disappearances: On Universal Responses to a Worldwide Phenomenon.* Cambridge University Press

Marina Matić Bošković[a]

Published by Cambridge University Press in March 2025, and edited by Professor Grażyna Baranowska and Dr. Milica Kolaković-Bojović the book *Enforced Disappearances: On Universal Responses to a Worldwide Phenomenon* discusses the UN human rights (both treaty bodies and special procedures) response to the key challenges of missing persons and enforced disappearances, including search and identification, reparations, family rights, involvement of non-state actors, the role of NGOs as well as migrations and armed conflicts as contexts of disappearances. A pioneer project in this field, the book resulted from joint work of two editors (who are in parallel coauthors of two chapters) and eleven authors,[2] where all of them are experts in this issue working across a global range of juris-

[a] PhD, Senior Research Fellow, Institute of Criminological and Sociological Research, Belgrade. E-mail: maticmarina77@gmail.com; ORCID: https://orcid.org/0000-0003-1359-0276

[1] IVAN JOVANOVIĆ is Transitional justice and rule of law consultant; MARIA CLARA GALVIS, PhD is Professor at the Externado University of Colombia and American University - Washington College of Law and former member and the Vice President of the United Nations Committee on Enforced Disappearances; REINER HUHLE, PhD is Human right expert, co-founder of the Nuremberg Human Rights Center and former member and the Vice President of the United Nations Committee on Enforced Disappearances.

GABRIELLA CITRONI, PhD is Professor of International Human Rights Law at the University of Milano-Bicocca, Italy, Member of the United Nations Working Group on Enforced or Involuntary Disappearances, an International Legal Advisor for the Latin American Federation of Associations for Relatives of the Detained-Disappeared (FEDEFAM) and Senior Legal Advisor for TRIAL International; ARIEL DULITZKY, PhD is Clinical Professor of Law and the Director of the Human Rights Clinic at the University of Texas, the Director of the Latin America Initiative and the former member of the United Nations Working Group on Enforced or Involuntary Disappearances; HORACIO RAVENNA, PhD is Human Rights professor, School of Social Sciences University of Buenos Aires and member of the United Nations Committee on Enforced Disappearances; LENE GUERCKE, PhD is an Independent human rights researcher and consultant; BARBARA LOCHBIHLER is member and the former Vice-President of the United Nations Committee on Enforced Disappearances; EVA NUDD is Legal Adviser at the Danish Institute Against Torture and former legal advisor in REDRESS; JASMINKA DŽUMHUR, PhD, Human Rights Ombudsperson of Bosnia and Herzegovina, a Vice President of the UN Committee on the Protection of the Rights of All Migrant Workers and Members of their Families, and a Member of the UN Commission of Inquiry on Ukraine; Former member and the vice chair of the UN Working Group on Enforced or Involuntary Disappearances; KOJI TERAYA, PhD is Law Professor, Tokyo University; Member of the United Nations Human Rights Committee and former member of the United Nations Committee on Enforced Disappearances.

dictions, including, but not limited to the membership in the UN treaty bodies and special procedures, NGO, academia and a research community. The book has been divided in two parts and ten chapters, where the first part deals with the horizontal issues associated to enforced disappearances worldwide, such as enforced disappearances in armed conflicts, strategies and means to improve the process of search and identification or to ensure access to social and economic rights for victims. In the second part, the book also includes several illustrative case studies from Latin America, Africa, Mexico, Western Balkans, and the Asia-Pacific region, which demonstrate the current challenges and problems relating to enforced disappearances in domestic or regional settings.

This title is available as a hardcopy, but also through the open access on Cambridge Core.[2]

The first part of the book is consisted of the five chapters:

In their coauthored, the introductory chapter, *Dealing with Uncertainty: On Addressing Enforced Disappearances Universally,* the editors used the notion of uncertainty as a highlight, underlining that „this simple word does not sound strong enough to describe all the seriousness and gravity of the consequences of an enforced disappearance." The editors further elaborate on the legal, economical and psycho-social consequences caused by enforced disappearances to the direct victims and their family members. This chapter also explores the regional and global developments from the pilot steps towards legal recognition of enforced disappearances to the present mechanisms of international human rights law and international criminal law. The chapter further elaborates on the International Convention for the Protection of All Persons from Enforced Disappearance (ICPPED, Convention) and the role of the UN Committee on Enforced Disappearances and the UN Working Group on Enforced or Involuntary Disappearances.

Chapter 2*, Enforced Disappearances in Armed Conflict through the Lenses of the International Convention for the Protection of All Persons from Enforced Disappearance,* written by Ivan Jovanović, explores the differences between enforced disappearances and the term 'missing persons' existing in international humanitarian law. It also demonstrates how the ICPPED fills gaps in IHL, highlighting the advantage of an international treaty in contrast to customary law, - in particular for practitioners -, as well as the potential of the continues nature of enforced disappearances for accountability efforts. Furthermore, limitations of the ICPPED in the context of armed conflict are shown, particularly not including non-state actors among the potential perpetrators. The author underlines that the fact that victims of enforced disappearances are a narrower group within the broader category of missing persons should not exclude large numbers of families of missing persons from access to support and reparation. Chapter 3, exploring the origins and assessing the impact of the Guiding Principles on the Search for Disappeared persons adopted in 2019, was written by Maria Clara Galvis Patiño and Rainer Huhle. The chapter explores the impact the Guiding Principles have during their first 4 years of existence (2019-2022) in the

[2] Available in open access: https://www.cambridge.org/core/books/enforced-disappearances/DE76D4C043ABF8E3F299032AE055041B#fndtn-information (Accessed: 27 February 2026)

public policies, but also in the case law, legislation, academic literature, and civil society. It connects a broad and comprehensive consultative process that preceded the adoption of the Guidelines with their strong impact on the practice, but also recognises an importance of the involvement and activities of families of disappeared persons, who were involved in the consultation process and are now demanding the Guiding Principles to be implemented domestically. Chapter 4, *New technologies and enforced disappearances*, written by Gabriella Citroni explores both: opportunities and challenges in this area. In addition to the presentation of the main findings from the work of UN Special Procedures on new technologies, including the WGEID, the author addresses the connection between a use of modern technologies and enforced disappearances. The chapter further explores how the WGEID could better engage with new technologies in its work, especially during its country visits. It reflects upon a need to find the balance in use of (still necessary) traditional approaches and techniques and the new technologies. The author also sheds some light on the perspectives to improve UN CED work through the use of modern technologies. Chapter 5 of the book, titled *The Fate and Whereabouts of Social Rights in the Practice of the Committee on Enforced Disappearances*, written by Ariel Dulitzky, addresses the access to property, health care, education, religious facilities, and other social and cultural rights for direct victims and their family members. The chapter analyses both: positive aspects in the CED's approach to social rights, as well as showcases gaps. It also comprehensively discusses approaches of the WGEID, Inter-American Court of Human Rights, UN treaty bodies and special procedures, and offers the proposal on how to use these approaches to change the restrictive interpretations applied so far by the CED. The second part of the book comprises of the five chapters that analyse the universal challenges from regional or domestic perspectives (in Latin America, Africa, Mexico, Western Balkans and Asia). Chapter 6, written by Horacio Ravenna addresses *NGO Contributions to Eradicate Enforced Disappearances in Latin America* brings valuable testimony of the author who actively participated in the struggle of the family members (mothers and grandmothers) of those disappeared in Argentina during the dictatorship. The author describes the causes and roots of the movement born in Argentina, as well as its growth, evolution and fight for the global legal recognition and eradication of enforced disappearances. This chapter is also of the greatest importance for a proper understanding of NGOs' role nowadays when enforced disappearances occur in different contexts such as migration or armed conflicts. Chapter 7, *Contemporary Disappearances in Mexico* by Lene Guercke discusses a challenging topic of contexts and modalities of enforced disappearances in Mexico as well as legal issues arising from them. It especially focuses on unprecedented increase disappearances associated to organised crime and drug trafficking, discussing how these practices fits to the concept of enforced disappearances, taking into account 2023 CED's statements on non-state actors. The chapter puts into the focus whether a failure to identify dead bodies can be a form of enforced disappearances, and under which circumstances impunity can be assessed as form of acquiescence. Chapter 8, *Disappearances of Migrants in Africa,* written by Eva Nudd and Barbara Lochbihler shed a light on migration as a context of disappearances focusing on African region where the widespread disappearances occurring

to migrants and refugee seekers. Authors reflects upon the problem of missing migrants in Africa and the impact on their families adopted by the African Commission in 2021 and discuss practical challenges, such as the lack of understanding of the very concept and distrust in authorities. Chapter 9, *Enforced Disappearances and the Right to Reparation in Western Balkans*, written by Milica Kolaković-Bojović and Jasminka Džumhur, both researchers and practitioners from the Western Balkans, presents an in-depth analysis of the complex legal situation on reparation in the region associated to the consequences of massive armed conflicts occurred in 1990's where over 40.000 of people went missing. The authors underline the results of the search and identification processes resulted in clarified faith and whereabouts of more than 30.000 people but emphasise underdevelopments when it comes to granting reparation to victims. The chapter brings comparative analysis of the challenges in Bosnia and Hercegovina, Croatia and Serbia where a common denominator is the absence of the crime of enforced disappearances, which appears particularly surprising in a region where the violation was so widespread. It also analysing the capacities of EU accession processes to foster and shape reform processes in the region, including access to reparation for victims of armed conflicts in the region. Chapter 9, *The Strategies to Increase the ICPPED Ratification with Special Attention to the Asia-Pacific Region,* by Prof. Koji Teraya, focuses on the region with a lowest ICPPED ratification rate and explores causes, roots and challenges associated with the ratification. The author also underlines that a seriousness of enforced disappearances requires for to arrange symptomatic treatments, along with suggesting possible strategies to increase the number of ratifications in the Asia-Pacific Region. A broad thematic scope coupled with in depth analysis of a number of highly relevant issues done by the most respective authors in the field, but in the manner which makes it understandable for different groups of audiences, makes this book a great choice not only for academic and research communities, but also for practitioners in the field, students and human rights activist. A plenty of recommendations on how to improve legislation and practices makes it also being a valuable source of inputs for policy makers on international, regional and national level.

© 2026 by authors

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

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

343

REVIJA za kriminologiju i krivično pravo = Journal of Criminology and Criminal Law / editor in chief Marina Matić Bošković. - Vol. 41, br. 1 (2003)- . - Beograd : Serbian Association for Criminal Law Theory and Practice : Institute of Criminological and Sociological Research, 2003- (Beograd : Birograf Comp). - 24 cm

Tri puta godišnje. - Glavni stvarni naslov od br. 1 (2023) Journal of Criminology and Criminal Law. - Je nastavak: Jugoslovenska revija za kriminologiju i krivično pravo = ISSN 0022-6076. - Drugo izdanje na drugom medijumu: Revija za kriminologiju i krivično pravo (Online) =

ISSN 2956-2198
ISSN 1820-2969 = Revija za kriminologiju i krivično pravo

COBISS.SR-ID 116488460

Institute of Criminological
and Sociological Research

Serbian Association for
Criminal Law and Practice

ISSN 1820-2969

www.rkkp.org.rs