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