Digital Evidence in Romanian Criminal Proceedings: Computational Challenges, Procedural Safeguards and Artificial Intelligence-Based Tools

Florentina-Anica Pintea[1*], Raluca-Mihaela Buculea[2]

[1]Assoc. Prof. PhD, Faculty of Computers and Applied Computer Science; Director, Multidisciplinary Computer Science Research Center (CCIM), "Tibiscus" University of Timișoara, Romania

[2]PhD Candidate, Faculty of Law and Public Administration, "Tibiscus" University of Timișoara, Romania

DOI: https://doi.org/10.51244/IJRSI.2026.1310000083

Received: 21 October 2026; Accepted: 26 October 2026; Published: 02 November 2026

ABSTRACT

Digital evidence is now present in almost every criminal case, yet it is volatile, easily altered and difficult to verify for a judge without technical training. The Romanian Code of Criminal Procedure requires computer searches to preserve the integrity of data, but the cryptographic safeguards it mentions, such as electronic signatures, remain optional. This article aims to translate the procedural guarantees of domestic and European law (Regulation (EU) 2023/1543, Directive (EU) 2016/680, and the case law of the European Court of Human Rights and of the Court of Justice of the European Union) into verifiable technical requirements. The methodology combines normative and case-law analysis with a review of digital forensics standards. On this basis, we propose a chain-of-custody model built on an append-only ledger chained through hash functions, electronic signatures, timestamps issued by a third party and a Merkle tree for data minimisation. The model was implemented as a Python prototype and evaluated on synthetic data. Internal verification of the ledger detected every alteration in 11 of 13 tampering scenarios, each tested in 1,000 trials. Truncation of the ledger and its complete rewriting by colluding operators were detected only when the final ledger value was anchored with an independent third party, in which case the detection rate reached 100%. The mechanism added about 0.75–0.80 s of computation per GiB of data, verification took about 0.19 ms per record, and Merkle proofs stayed below 640 bytes for one million files. We conclude that the integrity of digital evidence can be demonstrated rather than merely presumed, provided that data signing and external anchoring become mandatory. We also show that AI-based triage tools, which largely fall outside the high-risk category of the AI Act, create specific risks for the defence and should be recorded in the same chain of custody.

Keywords: Digital evidence, chain of custody, digital forensics, Merkle tree, artificial intelligence

INTRODUCTION

Digital evidence is no longer an exceptional category in criminal proceedings. Messages, files, location history and traffic data are now found in almost every case file, whatever the nature of the offence. The Grand Chamber of the European Court of Human Rights has expressly found that electronic evidence has become ubiquitous in criminal trials, but also that it is particularly vulnerable to destruction, damage, alteration or manipulation [29]. Taken together, these two findings describe the problem from which this article starts. Unlike traditional evidence, digital evidence cannot be perceived directly by the judge. It is always mediated by a device, by a program and, in most cases, by an expert. This mediation creates an asymmetry. Criminal investigation bodies have laboratories and specialised forensic tools, whereas the defence and the court receive the result of the processing, usually without the means to verify it independently. Under these conditions, the integrity of digital evidence tends to be presumed rather than demonstrated.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue X October 2026

Romanian positive law acknowledges this difficulty. The Budapest Convention on Cybercrime, ratified by Law no. 64/2004 [41], was transposed into the Code of Criminal Procedure through institutions such as the preservation of computer data and the computer search.

Art. 168(1) of the Code of Criminal Procedure (CCP) defines the computer search as a procedure carried out by adequate technical means and procedures capable of ensuring the integrity of the information [40]. The law does not, however, specify what these means are in concrete terms. The instruments that would make it possible to verify integrity, such as the electronic signing of data, are provided only as an option (Art. 143(2.1) and Article 170(2.1)–(2.4) CCP) [40]. The topic has particular relevance in the European context. Since 18 August 2026, Regulation (EU) 2023/1543 has applied, allowing judicial authorities to request electronic evidence directly from service providers established in other Member States [42], while Directive (EU) 2023/1544 requires providers to designate establishments and legal representatives for the receipt of such orders [23]. In Romania, the draft law transposing the directive was adopted by the Government in May 2026 [51], and the draft law on the implementation of the regulation (L272/2026) is under parliamentary debate [52]. The cross-border circulation of data multiplies the number of persons and systems through which a piece of evidence passes, and therefore the points at which the chain of custody may break.

Recent case law confirms that it is precisely these points that are contested. The Court of Justice of the European Union examined the conditions under which evidence obtained by intercepting the EncroChat platform may be transmitted through a European Investigation Order [18], [24], as well as the safeguards that must accompany police access to the data on a mobile phone [19]. At national level, the Constitutional Court has repeatedly examined the interferences with private life caused by the retention of traffic data and by technical surveillance [13], [14]. At the same time, artificial intelligence-based tools are entering investigations, especially for the triage of large volumes of data, and Regulation (EU) 2024/1689 subjects them to different legal regimes depending on the role they play [28].

The article seeks to answer three research questions. First: what procedural safeguards does the integrity of digital evidence require under Romanian and European law? Second: by what technical means can these safeguards be met, so that compliance with them can be verified by the court and by the defence? Third: to what extent does the use of artificial intelligence in processing evidence affect these safeguards?

The methodology is interdisciplinary, reflecting the background of the two authors, one a lawyer and the other a computer scientist. Normative and case-law analysis is combined with an analysis of digital forensics standards. On this basis, we propose a cryptographically verifiable chain-of-custody model, which we implement as a prototype and evaluate experimentally on synthetic data. The contribution of the article is fourfold: (i) a systematic mapping between procedural requirements and the technical responses that can satisfy them; (ii) a chain-of-custody model compatible with the procedural law in force, which also ensures data minimisation; (iii) the experimental finding that anchoring the ledger with an independent third party is a necessary condition for the integrity of the chain of custody, not merely an additional measure; (iv) a set of proposals on recording operations performed with artificial intelligence.

The article is structured as follows. The section on technical foundations explains the nature of digital evidence and the technical safeguards of integrity. It is followed by the mapping between procedure and technology, then by the proposed model and its experimental evaluation. The section on artificial intelligence analyses the European framework and the risks to procedural safeguards. The final sections discuss the recommendations and set out the conclusions.

TECHNICAL FOUNDATIONS OF DIGITAL EVIDENCE

The concept and characteristics of digital evidence

The Code of Criminal Procedure defines computer data as "any representation of facts, information or concepts in a form suitable for processing in a computer system" (Art. 138(5) CCP) [40].

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue X October 2026

Digital evidence is therefore information of evidentiary relevance that exists only as a sequence of bits interpreted by a program. Unlike a written document, it cannot be perceived directly by the judge: it is always mediated by a device and by the software that displays it. The specialised literature treats digital evidence as a distinct object of forensic science, with its own methods of identification and examination [8], [9].

Recent Romanian legal scholarship emphasises the high volatility and fragility of computer data, which can easily be modified, deleted or altered [5], as well as the central role of the computer search in proving offences committed in the digital environment [20]. Five characteristics follow from the nature of digital evidence, each with a procedural consequence (Figure 1): immateriality, volatility, fragility, exact duplicability and dependence on context and tools. Volatility explains the urgency of data preservation (Art. 154 CCP) [40]. The green box, exact duplicability, marks the only characteristic that favours the taking of evidence: it allows the analysis to be performed on a copy while the original remains untouched.

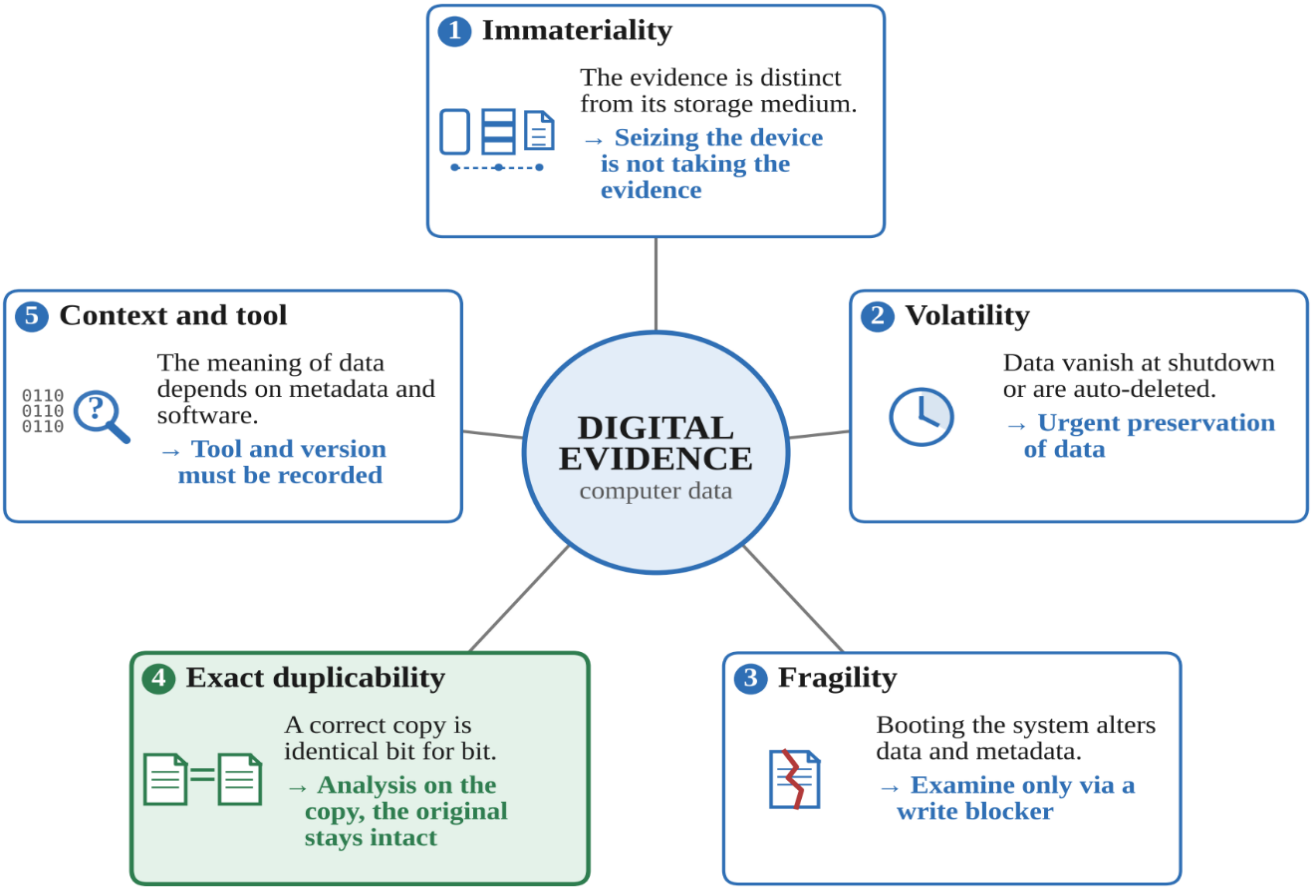


Figure 1. The characteristics of digital evidence and the procedural consequence of each

Data types and the order of volatility

From a technical point of view, data fall into three categories: data at rest (stored on a medium), data in transit (travelling across a network) and volatile data (existing only in working memory). The procedural regime broadly follows this distinction. The computer search (Article 168 CCP) mainly concerns stored data. Interception and access to a computer system (Article 138(1)(a)–(b) CCP) concern data in transit or remote access [40]. Regulation (EU) 2023/1543 applies only to stored data, not to real-time interception [42].

Forensic practice orders collection according to the order of volatility: first the data that disappear fastest (registers, memory, network connections), then the data on disk, and finally archives [6]. This rule sometimes conflicts with the procedural reflex of switching off and sealing the device. Switching off a computer with an encrypted disk may make the data permanently inaccessible.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue X October 2026

Three situations raise specific difficulties:

- Extraction may be logical (data accessible through the system interface), at file-system level, or physical (a full copy of the memory) [4]. Each level yields more data but requires a deeper intervention. The CJEU has held that even an attempt to unlock a phone constitutes processing of data subject to the safeguards of Directive 2016/680 [19], [22].
- The data are held on providers' servers, often in another state. The location of the data becomes uncertain, and access depends on judicial cooperation or, from 18.08.2026, on the European Production Order [42].
- The content is inaccessible without keys. Evidence obtained by compromising entire platforms (EncroChat, ByLock) raises problems of reliability and of defence access to the raw data, examined by the CJEU in Case C-670/22 [18], [44] and by the ECtHR in Yalçınkaya [29].

The digital forensics cycle

The ISO/IEC 27037 standard structures the handling of digital evidence in four initial stages: identification, collection, acquisition and preservation [38]. Analysis and interpretation are governed by ISO/IEC 27042, and the investigation process as a whole by ISO/IEC 27043. Similar process models are found in the NIST guidelines [39] and in those of the European Network of Forensic Science Institutes [26], and the methodology for the forensic investigation of computer crime has also been systematised in the Romanian literature [46]. The distinction between collection and acquisition has practical relevance. Collection means the physical seizure of the device. Acquisition means making a copy of the data, on site or in the laboratory.

The standard also sets out the principles against which the quality of the process is assessed: the relevance, reliability and sufficiency of the evidence, as well as the auditability, repeatability and reproducibility of the operations [38]. These principles have a direct procedural counterpart. Repeatability means that the same expert, using the same tool, obtains the same result. Reproducibility means that another expert, possibly one appointed by the defence, obtains the same result with another validated tool. Without reproducibility, adversarial debate on digital evidence remains a formality.

Technical safeguards of integrity

The definition in Article 168(1) CCP requires the computer search to be carried out by "adequate technical means and procedures capable of ensuring the integrity of the information" [40]. Legal scholarship has identified the authenticity and integrity of electronic evidence as the main theoretical and practical challenges in taking it [2]. Forensic practice has developed three instruments that give substance to the legal requirement.

The original medium is connected through a hardware or software device that allows read-only access, so that the examination cannot modify the original. A bit-for-bit copy of the entire medium is made, including unallocated space, where deleted files may be found. The copy is kept in formats that also retain the acquisition metadata (for example, the raw dd format or the E01 format). Analysis is performed only on working copies of this image. A cryptographic hash function transforms any volume of data into a fixed-length value (256 bits for SHA-256) [48]. Any change, even of a single bit, produces a completely different value. Integrity is verified by comparison, and equality of the values implies, with a probability practically equal to 1, that the data are identical:

$$H(D_{copy}) = H(D_{original}) \Rightarrow D_{copy} = D_{original} \quad (1)$$

The choice of function matters. Collisions were demonstrated for MD5 as early as 2004–2005 [59], and a practical collision for SHA-1 was published in 2017 [55]. The current recommendation is SHA-256 or a stronger function [48], possibly computing two different functions.

Electronic signature. The hash value proves that the data have not changed, but it does not show who computed it or when. The electronic signature binds the hash value to an identified person. The CCP provides for this option in Article 143(2.1) and Article 170(2.1)–(2.4), using the wording extended electronic signature

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue X October 2026

based on a qualified certificate [40]. The terminology comes from the former Romanian law on electronic signatures, whereas the eIDAS Regulation uses the notions of "advanced" and "qualified" signature [30].

An observation that is important for the argument of this article: the CCP provisions state that the persons involved "may" sign the data [40]. Signing is not mandatory. The safeguard exists, but it is not imposed.

The digital chain of custody. The chain of custody is the uninterrupted documentation of all the persons and operations that have touched the evidence, from seizure to trial. For digital evidence, each entry in the chain should contain the identity of the operator, the date and time, the operation performed, the tool used (with its version) and the hash value before and after the operation.

The CCP retains an analogue model of custody: the storage medium is kept in a sealed envelope, at the prosecutor's office and then at the court registry (Art. 143(2) CCP) [40]. A physical seal protects the medium but proves nothing about the data on it. A medium may remain sealed while the working copies used in the case file differ from one another. The difference between a physical seal and the verifiable integrity of the data justifies the model proposed below.

Tool validation and defence access. The results of an extraction depend on the tool used, for example on commercial suites for mobile phones [4]. These tools are usually closed-source software, frequently updated, and different versions may extract or interpret data differently. The report must therefore indicate the tool, its version and the extraction method. Programmes such as NIST's Computer Forensics Tool Testing (CFTT) test such tools independently. In Yalçınkaya, the ECtHR stressed that the inability of the defence to access directly and test the integrity and reliability of electronic evidence requires national courts to examine such evidence more rigorously [29]. In technical terms, the defence needs three things: a copy of the forensic image, the reference hash value and the log of operations. With them, it can verify independently that the data in the case file come unaltered from the indicated source.

The Bridge Between Procedure and Technology

The previous section showed what the integrity of digital evidence means from a technical point of view. It remains to be established how these requirements translate into the categories of criminal procedural law: the lawfulness and fairness of taking evidence, the right of defence, the proportionality of the interference and the procedural sanction for non-compliance. The proposed mapping is summarised in Table 1.

Table 1. Mapping between procedural requirements and technical responses

Procedural requirement	Technical risk	Computational response
Lawfulness and fairness of evidence (Articles 101–102 CCP)	access beyond the limits of the warrant	logging of searches, filters based on the subject matter of the warrant
Data integrity (Article 168(1) CCP)	modification of the original during examination	write blocking, forensic image, hash before and after
Right of defence and equality of arms (Article 6 ECHR)	the defence cannot test the raw data	access to the forensic image and to the log, validated tools
Proportionality and private life (Article 8 ECHR, C-548/21)	collection of the entire content of the phone	minimisation, separation of irrelevant data
Nullity and exclusion of evidence (Articles 102, 280–282 CCP)	broken or undocumented chain of custody	immutable, signed ledger verifiable by the court

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue X October 2026

Lawfulness, fairness and the limits of the warrant

The principle of fairness in taking evidence and the rule excluding unlawfully obtained evidence (Art. 101–102 CCP) [40] also apply to digital evidence, but here they raise a specific difficulty.

In a house search, the limits of the warrant are physical: a room, a space, the objects sought. In a computer search, the same limits must be translated into search criteria applied to a volume of data that may cover several years of a person's private life. A judicial body examining a phone inevitably also sees data unrelated to the case. Compliance with the warrant can no longer be proved by describing the place searched, but only by documenting the searches performed: which criteria were used, which results were selected and what was done with the rest of the data. A first procedural conclusion follows: the log of operations performed on the evidence is not a mere technical document, but the means by which it can be verified whether the judicial body stayed within the limits of the authorisation. Romanian scholarship has analysed the stages of the computer search precisely from the perspective of the procedural and technical particularities of each [7], and recent literature insists on the deeply intrusive nature of this procedure [5].

Data integrity and evidence to the contrary

When the defence challenges the integrity of digital evidence, the court faces a difficult task. It must assess a technical assertion, namely that the data have not been modified, without being able to examine the medium directly. In current practice, the answer often comes down to finding that the medium was sealed and that the search report meets the formal requirements. As shown above, however, a physical seal does not prove the integrity of the data. If the hash value of the forensic image was recorded and signed at acquisition, verification becomes a simple and objective operation: the court or an expert recomputes the value and compares it with the recorded one. The defence's challenge thus moves from general assertions to a concrete verification whose outcome does not depend on the trust placed in either party.

The right of defence and equality of arms

Yalçınkaya illustrates the consequences of lacking access to raw data. The Court held that the defence had no real opportunity to test the reliability of the decisive electronic evidence and that this affected the fairness of the proceedings as a whole [29]. For Romanian law, the lesson is practical: the right to consult the case file has real content with regard to digital evidence only if the defence can obtain, under conditions ensuring confidentiality, a copy of the forensic image or at least of the relevant data, the reference hash value and the log of operations. In the closely related area of technical surveillance, Romanian scholarship has analysed the compatibility of this procedure with constitutional and Convention safeguards [60], as well as the controversies over the lawfulness of interceptions carried out through technical structures of the intelligence services [33].

Proportionality and private life

Access to the entire content of a mobile phone may constitute a serious, even particularly serious, interference with private life, and the CJEU has held that the safeguards of Directive 2016/680 already apply to an attempt to gain access [19]. Proportionality concerns not only the moment of authorisation but also how the data are subsequently stored and used. A technical solution that allows only the relevant data to be placed in the case file, while preserving proof that they come from the original evidence, directly serves this principle. It also meets the requirement that the judicial body seize only the objects and documents connected with the offence.

Expert examination and the preliminary chamber

In Romanian criminal proceedings, the review of digital evidence is concentrated at two moments. The first is the expert examination or the technical-scientific finding (Art. 172 et seq. CCP) [40]. Its value depends on the questions put by the judicial body.

For digital evidence, the objectives of the expert examination should include at least: identification of the original medium and of the hash value recorded at acquisition; verification that this value matches the copy examined; indication of the tools used, with their versions; a description of the criteria for selecting the relevant data; and a statement of the limits of the method and of any data that could not be extracted or interpreted.

The second moment is the preliminary chamber procedure, whose object includes reviewing the lawfulness of the taking of evidence by the criminal investigation bodies (Art. 342 CCP) [40]. Here, the existence of a verifiable custody ledger changes the nature of the review. The preliminary chamber judge is no longer forced to choose between the assertions of the prosecution and those of the defence, but can establish, on the basis of a simple technical check, whether the chain of custody is complete and whether the data have remained unchanged.

Guidance from case law and legal scholarship

The criminal procedure literature treats the computer search and the expert examination as distinct institutions, each with its own safeguards [49].

The article-by-article commentaries on the Code of Criminal Procedure, in turn, provide interpretive guidance for Art. 168 and for Art. 172 et seq. [57], [58]. Published case law shows, however, that defence challenges concerning digital evidence cluster around a few recurring questions. We present them briefly, because each corresponds to a piece of information that the proposed custody ledger makes verifiable.

The first question concerns the choice of evidentiary procedure. The Pitești Court of Appeal referred to the High Court of Cassation and Justice the question whether access to a computer system, governed by Art. 138 CCP, may be used when the storage medium is already in the possession of the judicial bodies, or whether a computer search is required in that situation; it also asked whether the choice of warrant falls within the discretion of the judicial body or is a matter of lawfulness reviewable by the preliminary chamber judge [37].

Legal scholarship has argued that any examination of the content of a computer or storage medium amounts to a computer search, not a mere finding, and that urgency cannot justify examining a phone without a warrant, since the device can be isolated from the network until authorisation is obtained [12].

The second question concerns technical operations preceding the search, such as unlocking a phone. In a recent case, the phone had been unlocked by a specialist who drew up a report under Art. 172(9)–(10) CCP; the High Court dismissed the appeal against the refusal to refer to the Constitutional Court a plea of unconstitutionality concerning Art. 168(2) and (12) CCP, finding that the plea was not connected with the resolution of the case [35]. For the subject of this article, the case shows that a technical operation that changes the state of the device may remain outside the debate, even though it forms part of the history of the evidence. In a custody ledger, such an operation would be recorded as a separate entry, with its author, time and the tool used.

The third question concerns the scope of the review exercised in the preliminary chamber over the acts of the judge of rights and liberties. It has been accepted that the preliminary chamber judge may review the lawfulness of acts relating to the taking of evidence [34], but may not reassess the merits of the measure ordered by the judge of rights and liberties [36]. The Constitutional Court, for its part, has found that an effective a posteriori review of technical surveillance measures is necessary [15], and the question of challenging these rulings in the preliminary chamber procedure continues to be discussed in the literature [47].

The fourth and best documented question concerns the exclusion of evidence obtained with the participation of bodies that did not have the status of criminal investigation bodies. Following Constitutional Court Decision no. 51/2016 [14], the courts declared null and excluded interceptions carried out with technical support from the intelligence service [56]. A case study of proceedings pending when the decision was published describes the exclusion, in the preliminary chamber, of both the transcription reports and the optical media on which the conversations were stored [3].

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue X October 2026

The solutions given in the preliminary chamber follow the structure of Art. 342–346 CCP [40]. The judge either dismisses the requests and objections and finds that the evidence was lawfully taken, or declares certain acts null and excludes the unlawfully taken evidence under Art. 102 CCP, with the consequence that it can no longer be taken into account at trial on the merits. In the case of relative nullity, the defence must also prove prejudice (Art. 282 CCP). This is where the verifiable ledger plays a practical role. It allows a distinction between a formal irregularity, which did not affect the data, and an irregularity that compromised their integrity. The former may cause no prejudice; the latter deprives the evidence of value, whatever its procedural classification.

As regards the computer expert examination, the difference between a general question and a verifiable one is essential. A formulation such as establish whether the seized phone contains data relevant to the case leaves the choice of method, tools and selection criteria to the expert, without these being subject to debate. A verifiable formulation asks instead whether the hash value of the examined copy is identical to the one recorded at acquisition; which tools, in which version, were used; which data could not be extracted or interpreted; and by which criteria the data placed in the case file were selected. The answers to these questions can be checked by the court and by the party-appointed expert, and the custody ledger provides them directly.

Proposed Model: A Cryptographically Verifiable Chain of Custody

Rationale and requirements

The analysis in the previous sections has revealed an asymmetry. Procedural law formulates the integrity requirement in general terms ("adequate technical means and procedures", Art. 168(1) CCP).

The instruments that would make it possible to verify it, such as the electronic signature, are only optional (Article 143(2.1), Article 170(2.1)–(2.4) CCP) [40]. The practical consequence is that the integrity of digital evidence is presumed instead of being demonstrated. The proposed model seeks to turn integrity from a presumption into a property that any participant in the proceedings can verify.

Building on the procedural safeguards analysed above and on the case law of the ECtHR and the CJEU, we formulate six requirements that a custody mechanism for digital evidence should satisfy (Figure 2). The first three concern the integrity of the chain of custody and rest on Article 168(1), Article 143(2.1) and Article 170(2.2) CCP [40]. The last three concern safeguards for the defence and for private life and derive from Article 6 ECHR, as interpreted in Yalçınkaya [29], from Article 8 ECHR and the CJEU case law in Case C-548/21 [19], and from Directive (EU) 2016/680 [22].

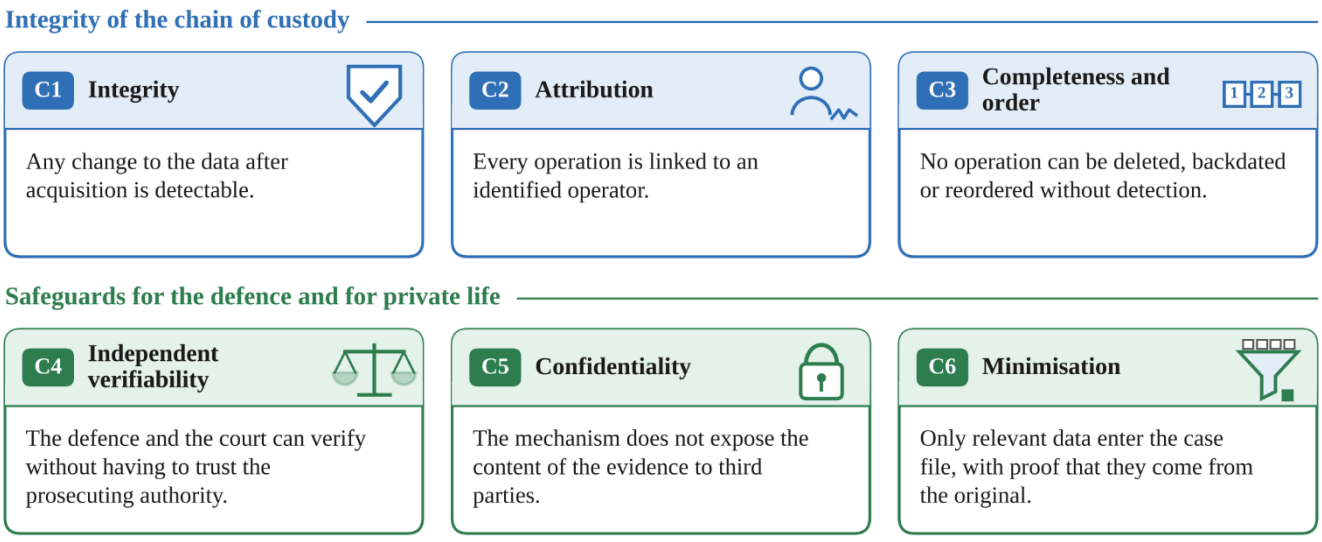


Figure 2. Requirements for the custody mechanism of digital evidence (C1–C6), grouped by their object.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue X October 2026

Requirements C1 and C2 are partly covered by positive law. Requirements C3, C4 and C6 currently have no explicit technical counterpart in Romanian procedural legislation and form the core of the contribution.

Architecture of the model

The workflow starts with the warrant for the computer search, issued by the judge of rights and liberties under Article 168 CCP [40]. At acquisition, a bit-for-bit image of the storage medium is created and its hash value (H0) is recorded. Every subsequent operation, from the analysis of the working copy to the signed expert report, is written to an append-only ledger together with the operator, the time, the previous hash value and a qualified signature (Figure 3).

At trial, the court or the defence recomputes the hash value and compares it with H0. If the values match, the integrity of the evidence is confirmed. If they differ, the evidence may be challenged and excluded under the rules on unlawfully obtained evidence (Art. 102 CCP) [40].

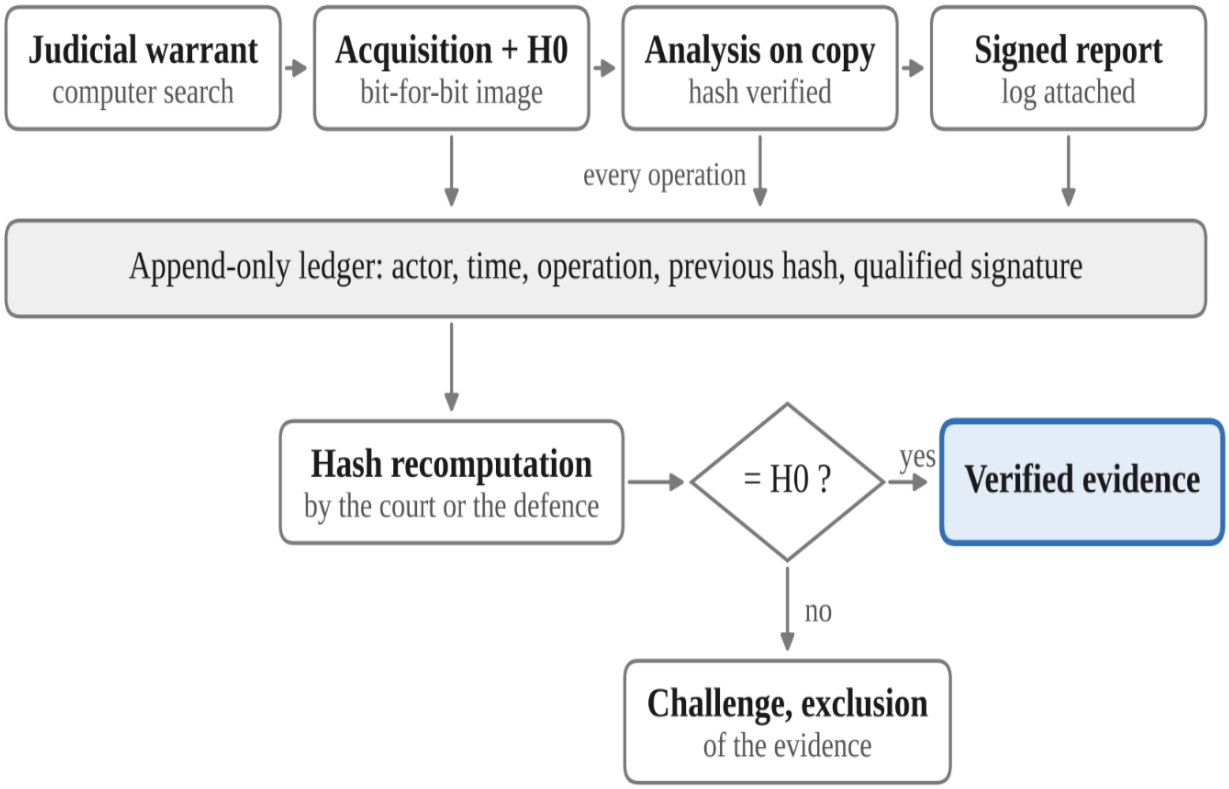


Figure 3. The proposed chain of custody: each stage writes a signed entry to the ledger

The choice of standardised components (hash functions, qualified signatures and qualified timestamps) is deliberate. An evidentiary mechanism must be capable of being explained and challenged.

Solutions based on established technologies are easier for a court-appointed expert to assess than proprietary solutions.

Record structure and chaining

Each operation on the evidence (acquisition, copying, analysis, transmission, handover to the court) generates a record with the fields listed in Table 2.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue X October 2026

Table 2. Fields of a custody ledger record

Field	Content	Requirement covered
no	sequence number of the record	C3
case_id	identifier of the case and of the act authorising the operation (warrant, prosecutor's order)	C1, C6
operator	identity and capacity of the person acting	C2
operation	type and description of the operation	C3
tool	name and version of the tool used	C4
data_hash	hash value of the data after the operation	C1
prev_hash	hash value of the previous record	C3
timestamp	timestamp issued by a third party	C3
signature	electronic signature of the operator over the fields above	C2

The link between records forms a chain of hash values. Denoting by r_i the content of record i (without the signature) and by H the hash function, the value linking a record to the previous one is:

$$h_i = H(h_{i-1} \| r_i), \quad h_0 = H(H0 \| \text{case identifier}) \qquad (2)$$

where ‖ denotes concatenation (Figure 4). The idea of tamper-evident audit logs based on cryptographic chaining is not new in computer science [53], [21]. The contribution of this article lies in linking the mechanism to Romanian and European criminal procedural safeguards.

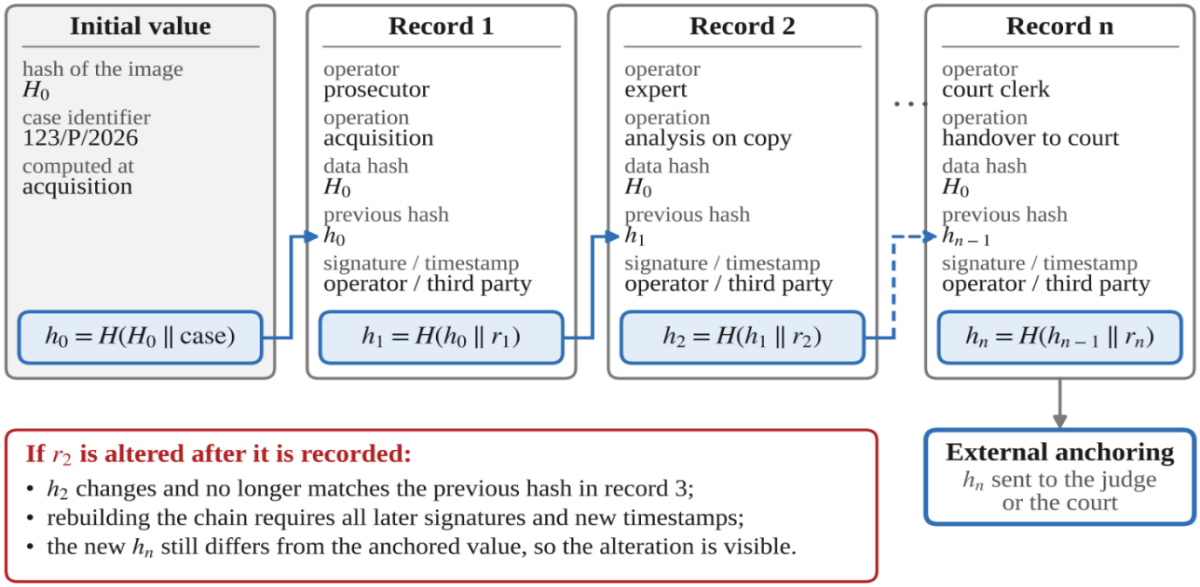


Figure 4. The hash-chained custody ledger

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue X October 2026

Each record contains the hash value of the previous record, is signed by the operator and receives a timestamp from a third party; the final value is anchored externally, so that any later alteration becomes visible. The essential property is the following. Modifying any record r_k changes the value h_k and, consequently, all subsequent values. An alteration can be concealed only by rebuilding the entire chain. This would require forging the signatures of all subsequent operators and the timestamps issued by the third party.

Data minimisation: the Merkle tree

A computer search usually produces far more data than is relevant to the case. The judicial body must seize only what is connected with the offence (Art. 159(13) CCP [40]), and the CJEU requires access to the data on a phone to be proportionate [19]. This creates a tension. To prove integrity, the complete image should be retained. To respect private life, only part of it should reach the case file.

We propose to resolve this tension with a Merkle tree [45]. The hash values of the extracted files are combined in pairs until a single root value is obtained, which is recorded in the ledger at the time of acquisition. Later, for a relevant file, only that file and a small number of intermediate hash values need to be placed in the case file. For n files, about $\log_2 n$ values are needed, for example about 17 values for 100,000 files. The court can thus verify that the file comes from the acquired image without the rest of the content being entered into the case file or disclosed to the parties.

Threat model

Evaluating a security mechanism requires specifying the attacks against which it offers protection. The proposed model addresses four categories of threats.

The first is modification of the data after acquisition. It is detected by comparing the hash value of the data with the value H0 recorded at acquisition or, for a file filed separately, with the root of the Merkle tree. The residual risk is nil, provided that H0 was recorded correctly.

The second is the deletion or reordering of ledger records. The chaining of hash values and the numbering of records make any such intervention visible. One exception remains, however: truncating the end of the ledger leaves an internally consistent chain and can be detected only by external anchoring of the final value.

The third is the retroactive insertion of an operation, countered by the timestamp issued by a third party. The residual risk lies in the compromise of the timestamping service.

The fourth is the repudiation of an operation by the operator who performed it, ruled out by the qualified electronic signature. The attack remains possible only if the operator's private key has been compromised.

Two situations, by contrast, remain outside the model and mark its limits. Alteration of the data before acquisition cannot be detected, because the value H0 is computed over data that are already altered. Protection here lies with the procedural safeguards of the search: the warrant, the presence of the assisting witness and of the lawyer, and audio-video recording. Likewise, a defective forensic tool may misinterpret the data even if their integrity is preserved. The mechanism records the tool and the version used, but the correctness of the result depends on the independent validation of the tool. The mechanism therefore guarantees that the evidence has not changed since acquisition. It guarantees neither that the acquisition was lawful nor that the tool interpreted the data correctly. These aspects remain within the remit of judicial review and of expert examination.

Signed ledger or blockchain?

Recent literature frequently proposes distributed blockchain ledgers for the chain of custody [43]. We consider that, for Romanian criminal proceedings, a centralised ledger with qualified signatures and timestamps is the more proportionate solution (Table 3).

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue X October 2026

Table 3. Signed ledger compared with blockchain-based solutions

Criterion	Signed ledger + qualified timestamp	Public blockchain	Permissioned blockchain
Tamper resistance	high (C1, C3)	very high	high
Confidentiality (C5)	yes, only hash values are published, to a third party	problematic: data are replicated publicly	yes, if the participants are authorities only
Compatibility with data erasure (Directive 2016/680)	yes	no	limited
Legal recognition	legal framework exists (eIDAS)	no specific framework	no specific framework
Cost and complexity	low	variable	high
Explainability before the court	high	low	medium

The specific advantage of blockchain, the absence of a central trusted authority, is of limited value in a context in which the state is in any event the holder of the criminal action and the court reviews the evidence. The current value of the chain must, however, be anchored periodically with a third party independent of the criminal investigation body, for example by communicating it to the judge of rights and liberties. The tamper-detection experiments (Table 4) show that, without such anchoring, truncation of the ledger and its rewriting through collusion cannot be detected.

Compatibility with the procedural law in force

The model does not require amending the CCP in order to be implemented on an experimental basis. It builds on the option, already provided by law, of signing the data and certifying their integrity (Art. 143(2.1), Art. 170(2.1)–(2.4) CCP) [40]. Art. 170(2.5) refers, for these operations, to methodological rules, which provide the natural framework for detailed technical regulation. The lege ferenda proposal deriving from the model is twofold. First, signing the data and recording the hash value should become mandatory rather than optional. Second, the defence should have an express right of access to the forensic image, to the reference value and to the ledger.

Experimental validation

The model was implemented as a Python prototype and evaluated experimentally along four dimensions: (a) the ability to detect intentionally induced alterations; (b) the overhead compared with an ordinary acquisition; (c) the time needed for verification by the court or the defence; (d) the size of Merkle proofs. The source code, raw data and reproduction instructions are publicly available under a CC BY 4.0 licence in the Zenodo repository [50].

Experimental setup

Virtual machine with 2 Intel Xeon cores and 8 GB RAM, Linux, Python 3.13.16, cryptography library 50.0.1. The hash function is SHA-256. Operator signatures use Ed25519 as a substitute for the qualified electronic signature. The timestamping service is simulated by a separate Ed25519 key that enforces monotonic times.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue X October 2026

The test data are synthetic, generated with a fixed seed (20261021), so that all results are reproducible. The test ledger contains 20 records describing a typical computer search: acquisition, recording of the Merkle root, working copy, analysis, delivery of the report, filing with the court.

Tamper detection

Thirteen tampering scenarios were simulated, each in 1,000 trials with random parameters (position of the modified byte, targeted record, modified field, etc.). The results are presented in Table 4.

Table 4. Tamper detection rate (1,000 trials per scenario)

Code	Scenario	Detected
T1	one bit modified in the forensic image	1,000 / 1,000
T2	one bit modified in a file filed with a Merkle proof	1,000 / 1,000
T2b	foreign file presented as coming from the image	1,000 / 1,000
T3	modification of a field in a record	1,000 / 1,000
T4	deletion of an intermediate record	1,000 / 1,000
T5	swapping the order of two records	1,000 / 1,000
T6	retroactive insertion by an operator holding only their own key	1,000 / 1,000
T8	signature produced with an unauthorised key	1,000 / 1,000
T9	backdating of a timestamp	1,000 / 1,000
T4b	ledger truncation (deletion of the last records), internal verification	**0 / 1,000**
T4c	ledger truncation, with the final value anchored with a third party	1,000 / 1,000
T7a	rewriting of the ledger by colluding operators who hold all the keys, with new timestamps, internal verification	**0 / 1,000**
T7b	the same rewriting, with the final value anchored with a third party	1,000 / 1,000

The result for the first nine scenarios was expected by construction. It nevertheless confirms that the implementation respects the properties described for the record structure. Scenarios T4b and T7a are more relevant. They reveal two attacks that internal verification of the ledger cannot detect. A truncated ledger remains internally consistent, because each retained record is correctly linked to the previous ones. Likewise, a ledger rewritten in its entirety by persons who control all the signing keys and can obtain new timestamps is, cryptographically speaking, a valid ledger. Both attacks become 100% detectable if the final value of the chain is periodically communicated to a third party independent of the criminal investigation body (T4c, T7b).

This conclusion has direct consequences for the legal design of the mechanism. External anchoring is not an optional trust-enhancing measure but a necessary condition for the integrity of the chain of custody. In Romanian criminal procedure, the natural moments for anchoring are: communicating the value to the judge of rights and liberties after the computer search, filing it with the preliminary chamber together with the indictment, and communicating it to the defence.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue X October 2026

Overhead

The overhead was measured in two variants. In the first, the data are already in memory and only computation is measured. In the second, a complete acquisition is measured, including reading from and writing to disk.

The baseline is ordinary practice: a bit-for-bit copy and computation of the SHA-256 of the image in a single pass. In the same pass, the model adds a hash value for each file, then builds the Merkle tree and writes six signed records. The results are presented in Table 5.

Table 5. Overhead of the model (median of 11 runs)

Image	Files	Computation only: baseline → model	Computation overhead	With disk: baseline → model	Overhead with disk
256 MB	≈ 1,000	0.19 s → 0.39 s	+0.20 s (×2.05)	0.61 s → 0.75 s	+0.14 s (+23%)
1 GB	≈ 4,000	0.73 s → 1.48 s	+0.75 s (×2.03)	2.26 s → 3.80 s	+1.53 s (+68%)
4 GB	≈ 16,000	—	—	12.6 s → 15.4 s	+2.87 s (+23%)

The computation overhead is stable and predictable: about **0.75–0.80 s** per GB of data on the test machine. This cost corresponds to a second SHA-256 pass over the file contents, needed for the leaves of the Merkle tree. Building the tree and signing the six records took between 1.5 and 14 ms, a negligible fraction.

The relative overhead measured with disk varied between 23% and 68%, even though the interquartile ranges were narrow. The variation reflects the behaviour of the virtual machine's storage subsystem (caching, synchronous writes), not the mechanism itself. For this reason, the indicator we consider representative is the absolute computation cost per GB. In a real acquisition from a physical medium through a write blocker, the relative share depends on the speed of the medium. The two hash passes can also be parallelised on different cores. Both aspects must be measured on real forensic equipment before operational conclusions are drawn.

Verification time

Verification time grows linearly with the number of records, at about 0.19 ms per record (Table 6). The cost is dominated by verifying the two signatures in each record, that of the operator and that of the timestamp. An ordinary case file, with a few dozen operations on a piece of evidence, is verified in less than 20 ms. Verifying the ledger is therefore not a practical burden for the court or the defence. The expensive part remains recomputing the hash value of the image, which takes as long as reading it in full.

Table 6. Full ledger verification time (median of 5 runs)

Records	Verification time	Per record	Ledger size
10	1.9 ms	0.19 ms	7.7 KB
100	18.8 ms	0.19 ms	77 KB
1,000	187 ms	0.19 ms	775 KB
10,000	1.95 s	0.20 ms	7.6 MB

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue X October 2026

Merkle proofs

The proof size grows logarithmically with the number of files (Table 7).

A ten-thousand-fold increase in the number of files, from 100 to 1,000,000, enlarges the proof only from 224 to 640 bytes. In practice, a relevant file can be placed in the case file together with a proof of a few hundred bytes attesting that it comes from the acquired image, without disclosing the rest of the device's content. The result directly supports requirement C6 and responds to the tension between integrity and proportionality identified in the CJEU case law [19].

Table 7. Size and cost of membership proofs (1,000 random proofs for each size)

Files in image	Hash values in proof (max.)	Proof size	Tree construction	Verification of one proof
100	7	224 bytes	< 1 ms	3.6 µs
1,000	10	320 bytes	1 ms	4.9 µs
10,000	14	448 bytes	8 ms	6.4 µs
100,000	17	544 bytes	86 ms	8.2 µs
1,000,000	20	640 bytes	1.4 s	9.6 µs

Limitations of the evaluation

The test data are synthetic (random bytes), not images of real devices. Ed25519 was used instead of the qualified electronic signature. Real qualified signatures, generated on secure devices, are slower and may increase signing and verification time. Timestamping was simulated locally. A real service adds network latency to each record. The implementation is in Python. An operational implementation would most likely have lower costs. The measurements were performed on a single, virtualised hardware configuration.

These limitations concern the absolute time values, not the qualitative conclusions: tamper detection, the need for external anchoring and the logarithmic growth of proofs do not depend on the hardware configuration.

ARTIFICIAL INTELLIGENCE IN CRIMINAL PROCEEDINGS

Three roles of artificial intelligence in relation to digital evidence

The debate on artificial intelligence (AI) in criminal justice often deals with a single scenario: the algorithm that "judges" or predicts a person's behaviour. In the field of digital evidence, however, AI intervenes in three distinct roles, each with a different legal regime.

- AI as a tool for processing evidence**.** Automated triage systems select potentially relevant items from a very large volume of extracted data. Other systems recognise objects or persons in images, transcribe and translate audio recordings, extract text from scanned documents or reconstruct communication networks. Their output is not new evidence but a selection or transformation of existing evidence.

- AI as an assessment tool. Some systems assess the reliability of evidence, the credibility of a source or the risk posed by a person. Here AI no longer transforms the data but makes a value judgement about them.

- AI as a source of forgery. Generative tools make it possible to fabricate audio recordings, videos or images that are hard to distinguish from authentic ones. In this role, AI is not a tool of the judicial body but a threat to the authenticity of evidence.

The distinction matters because Regulation (EU) 2024/1689 [28] treats the first two roles differently. The third is mainly a matter for the rules on taking and assessing evidence.

The European legal framework

Since 2 February 2025, the Artificial Intelligence Act has prohibited AI systems used to assess or predict the risk of a natural person committing a criminal offence, where the assessment is based solely on profiling the person or on their personality traits (Art. 5(1)(d)) [28].

The prohibition does not apply to systems that merely support a human assessment already based on objective and verifiable facts directly linked to a criminal activity. Scholars have stressed the narrow scope of the prohibition: the conditions are cumulative, and systems falling outside it may nevertheless qualify as high-risk systems [25]. The use of real-time remote biometric identification in publicly accessible spaces for law enforcement purposes is also prohibited, subject to strictly listed exceptions (Art. 5(1)(h)) [28].

Annex III classifies as high-risk, among others, systems used by law enforcement authorities to evaluate the reliability of evidence in the course of the investigation or prosecution of criminal offences (point 6(c)) and systems assisting a judicial authority in researching and interpreting facts and the law (point 8) [28]. The European Commission's guidance specifies that tools which merely process, restore or extract data so that they can then be examined by a human expert do not evaluate the reliability of evidence [27]. It follows that most forensic tools in the first role described above do not, as such, fall into the high-risk category. This conclusion is important, because these are precisely the tools most widely used in practice. The obligations for Annex III systems apply only from 2 December 2027, following the postponement introduced by the Digital Omnibus [31], [54].

A person affected by a decision taken on the basis of the output of a high-risk system listed in Annex III, which produces legal effects or similarly significantly affects them, has the right to obtain clear and meaningful explanations of the role of the system in the decision-making procedure and of the main elements of the decision (Art. 86) [28]. The right is, however, subsidiary: it applies only where it is not already provided for by another Union act, and it may be restricted by Union law or by national law in accordance with Union law. Directive 2016/680 requires Member States to prohibit decisions based solely on automated processing, including profiling, which produce adverse legal effects for the data subject. An exception is permitted only by law and with safeguards, at least the right to obtain human intervention (Art. 11) [22].

Council of Europe instruments

The European Ethical Charter on the use of AI in judicial systems, adopted by the CEPEJ on 3–4 December 2018, sets out five principles: respect for fundamental rights, non-discrimination, quality and security, transparency, impartiality and fairness, and the principle under user control [11]. The Charter recommends the greatest reservations regarding the use of AI in criminal matters. The Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225) was opened for signature in Vilnius in September 2024, and the European Union was among the first signatories [16]. The Union ratified the Convention on 15 May 2026, at the 135th session of the Committee of Ministers held in Chișinău [17]. So far, the only ratification deposited with the Secretary General of the Council of Europe is that of the European Union. Although the treaty has gathered more than 20 signatures (including from non-European states such as the United States, the United Kingdom, Japan and Canada), the threshold required for its entry into force has not yet been reached. At the time of writing, Romania has not yet signed the treaty in its own name. Source: Council of Europe, Treaty Office – Chart of signatures and ratifications of Treaty 225, status as of 22.10.2026.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue X October 2026

Risks to procedural safeguards

The analysis of the legal framework reveals a paradox. The AI tools with the greatest practical influence on evidence, those used for triage and extraction, are precisely the ones that, as a rule, do not fall into the high-risk category. European bar associations have, moreover, argued for classifying the automated triage of digital evidence as high-risk [10]. We consider that the procedural risks of these tools are real, for at least four reasons.

- A triage system does not decide what is true, but what a human will examine. Items that the system does not flag may never be seen by the investigator. The Code of Criminal Procedure, however, requires criminal investigation bodies to gather and take evidence "both in favour of and against the suspect or defendant" (Art. 5(2) CCP) [40]. A system calibrated to find evidence of guilt may unintentionally filter out exculpatory evidence. The risk is not visible in the case file, because the case file contains only what was selected.

- Machine learning models do not, as a rule, provide a justification of their output that can be debated adversarially. In Yalçınkaya, the ECtHR held that the inability of the defence to verify electronic evidence directly requires the courts to carry out a more rigorous review [29]. The reasoning applies all the more to an output produced by a model that not even the judicial body can explain.

- Human–machine interaction research describes the tendency of users to accept the output of an automated system even when other evidence contradicts it (automation bias). The requirement of human intervention in Art. 11 of Directive 2016/680 [22] risks becoming a formality if the human merely confirms what the system has proposed.

- Many models, especially generative ones, do not produce the same output on repeated runs. Their versions change frequently, and providers do not always keep old versions. An output that cannot be reproduced cannot be verified by the defence expert, which contradicts the reproducibility requirement set out in the discussion of the digital forensics cycle.

The specific problem of AI-generated content

Content generated or modified with AI affects evidence in two ways. The first is obvious: a fake recording may be presented as authentic. The second is subtler and has been called the liar's dividend (liar's dividend) in the Anglo-American literature: the mere technical possibility of forgery makes it possible to challenge authentic evidence. US courts have begun to respond to both risks. They combine traditional authentication methods (witnesses, chain of custody, metadata) with technical expertise and require a factual basis for authenticity challenges, without relying exclusively on detection tools, which lag behind generative models [1]. The proposed model offers a partial answer. It cannot establish whether a recording was forged before acquisition (a limitation acknowledged in the description of the threat model). It can, however, prove that a piece of evidence has not been modified since acquisition. The challenge to authenticity thus shifts to narrower and more easily verifiable ground: the time and conditions of acquisition. For content produced by modern devices, standards for attesting provenance at source, in which the capture device signs the content, may complement this mechanism. In [32], the authors carry out a formal security analysis of the C2PA protocols and conclude that, for the time being, the system should not be relied upon for high-stakes uses, including as evidence in court. Attestation at source is therefore a future complement rather than a present guarantee.

Proposals

On the basis of this analysis, we put forward four proposals, the first of which follows directly from the proposed model.

Every use of an AI system on the evidence should be recorded as a separate operation in the ledger, by extending the custody ledger to operations performed with AI (Figure 5).

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue X October 2026

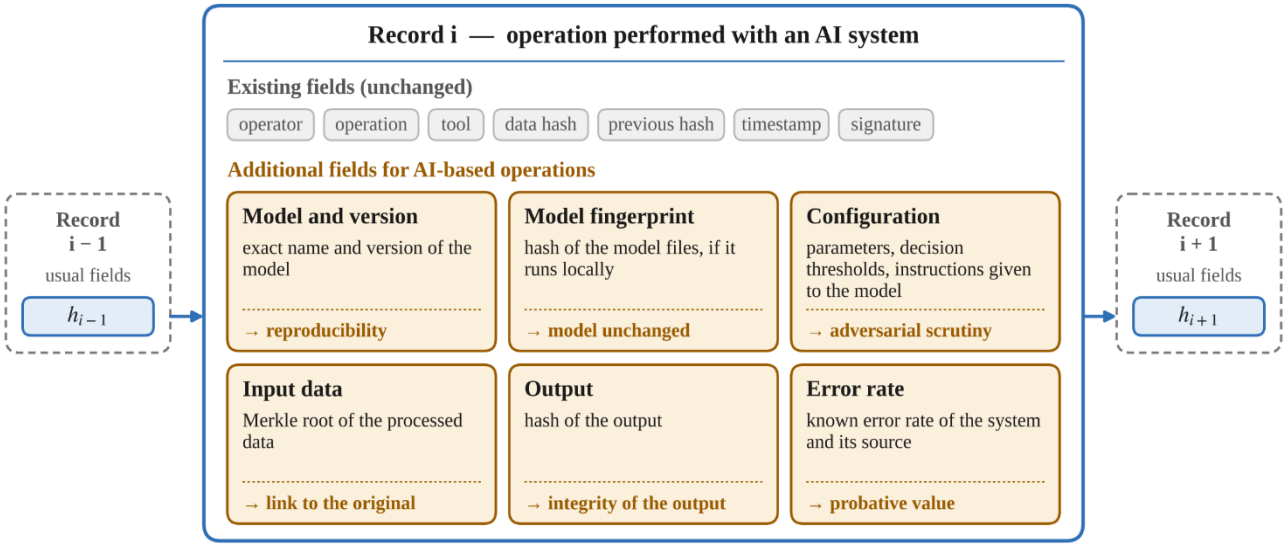


Figure 5. Custody ledger record extended for operations performed with an AI system

The extension does not require a change of architecture. The experimentally evaluated prototype can accommodate these fields without modifying the chaining mechanism, and the verification cost remains in the order of 0.2 ms per record.

- The defence should receive not only the items selected by the system but also the list of rejected items, together with the threshold used. Only in this way can compliance with Article 5(2) CCP be verified. Merkle proofs make this possible without disclosing the content of irrelevant items.

- Directive 2016/680 already prohibits basing a procedural measure solely on the output of an AI system in the case of automated decisions with legal effects [22]. We propose that this prohibition be expressly enshrined in the CCP, together with an obligation for the judicial body to state to what extent it relied on the output of the system.

- AI tools used in criminal investigations should be tested on reference datasets, and their error rate should be published, so that the tools can be validated independently. Otherwise, the court has no benchmark for assessing the probative value of the output. For high-risk systems, the obligations of the AI Act will impose documentation and human oversight requirements from 2 December 2027 [28], [31]. For other tools, the obligation should be established through national methodological rules.

DISCUSSION AND RECOMMENDATIONS

The results of the analysis lead to a finding of principle. Romanian criminal procedural law correctly formulates the requirement of integrity of digital evidence but leaves it without mandatory means of verification. The necessary technical instruments exist and are already mentioned in the CCP, but they are optional.

The experiments further show that even signing each operation is not sufficient: without periodic anchoring of the ledger with an independent third party, its truncation or rewriting by persons who control all the keys remains undetectable. The following recommendations are addressed to practitioners, the legislature and training institutions.

Pending any legislative intervention, judicial bodies can already apply a minimum discipline for digital evidence within the limits of the law in force. Table 8 proposes a checklist that can be used by the prosecutor, the preliminary chamber judge and the defence.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue X October 2026

Table 8. Minimum checklist for digital evidence

Check	Question	Where to check	Consequence of a negative answer
☐	Is the hash value of the image recorded at the time of acquisition?	search report, acquisition report	integrity cannot be verified later
☐	Does the hash value of the examined copy match the one recorded at acquisition?	expert report or technical-scientific finding report	the evidence may have been altered
☐	Are the tool, its version and the extraction method indicated?	expert report or technical-scientific finding report	the result cannot be reproduced by another expert
☐	Is each operation documented, with its author and time?	log of operations (custody ledger)	the chain of custody is incomplete
☐	Has the final value of the chain been communicated to an independent third party?	judge's ruling, case file	truncation or rewriting of the ledger cannot be ruled out
☐	Have the criteria for selecting the relevant data been explained, including those applied by automated tools?	expert report, prosecutor's order	compliance with the limits of the warrant and with Article 5(2) CCP cannot be verified
☐	Does the defence have access to the data needed for independent verification?	defence requests, court rulings	equality of arms is affected

We propose three interventions. First, turning the option of signing the data (Article 143(2.1) and Article 170(2.1)–(2.4) CCP) into an obligation, together with mandatory recording of the hash value at acquisition and at every transfer. Second, expressly enshrining the right of the defence to obtain, under conditions ensuring confidentiality, the data needed to verify the integrity of the evidence. Third, adopting the methodological rules referred to in Article 170(2.5) CCP, which could regulate the format of the custody ledger, the moments of external anchoring and the recording of operations performed with artificial intelligence tools. The implementation of Regulation (EU) 2023/1543 [42] offers a natural opportunity for these clarifications, since evidence obtained from providers in other Member States raises the same problems of integrity and traceability.

Digital evidence requires a common language between lawyers and computer scientists. Initial and continuing training programmes for judges and prosecutors should include the basic technical notions (forensic image, hash function, chain of custody, the limits of automated tools), and computer science degree programmes should include elements of procedural law relevant to digital forensics. The collaboration between faculties of law and of computer science, from which this article also stems, can serve as a model.

The legal analysis is limited to Romanian law and European Union law, without a systematic comparison with other national systems. The experimental evaluation used synthetic data, a simulated timestamping service and Ed25519 signatures instead of qualified ones. The qualitative conclusions do not depend on these choices, but the absolute time values must be confirmed on real forensic equipment.

CONCLUSIONS

The article started from three research questions. As to the first, concerning the procedural safeguards required by the integrity of digital evidence, the answer is that Romanian and European law cumulatively require the integrity of the data, the possibility for the defence and the court to verify it, and the proportionality of the interference with private life. The case law of the ECtHR and the CJEU gives these requirements concrete content, especially with regard to defence access to raw data.

As to the second question, concerning the technical means by which these safeguards can be met and verified, we proposed a chain-of-custody model based on a ledger chained through hash functions, signed by each operator and periodically anchored with an independent third party, complemented by a Merkle tree for data minimisation. The evaluation of the prototype showed that the model detects any alteration after acquisition, at a low computational cost and with very small proofs. The most important result, however, concerns legal design: external anchoring of the ledger is a necessary, not optional, condition for the integrity of the chain of custody.

As to the third question, concerning artificial intelligence, we showed that the tools with the greatest practical influence, those used for data triage and extraction, largely remain outside the high-risk category of Regulation (EU) 2024/1689. Their risks to procedural safeguards are nevertheless real, particularly because of the asymmetry of triage and the lack of reproducibility. Recording these operations in the same custody ledger and giving the defence access to the full output of the triage can reduce these risks without architectural changes.

Future research directions include testing the model on real equipment and data, extending it to cloud-based evidence and to end-to-end encrypted communications, and a comparative analysis of how other Member States apply Regulation (EU) 2023/1543. The overall conclusion of the article is that the integrity of digital evidence can be demonstrated, not merely presumed, if procedural law turns the technical instruments already mentioned in the law into mandatory safeguards.

REFERENCES

1. Akhlaghi M. (2025). Laboratoire de cyberjustice. Deepfakes in courtrooms: How judges are adapting to a new reality. Université de Montréal. https://cyberjustice.openum.ca/s/24524
2. Antoci, A., & Cozma, T.-M. (2025). Autenticitatea și integritatea probelor electronice în procesul penal: provocări teoretico-practice [Authenticity and integrity of electronic evidence in criminal proceedings: Theoretical and practical challenges]. Revista Națională de Drept, 2(254), 38–46. https://doi.org/10.52388/1811-0770.2025.2(254).04
3. Apostol, A. (2023). Case study on the effects of Constitutional Court Decision No. 51/2016 on pending proceedings. Analele Universității „Dunărea de Jos" din Galați, Fascicula XXVI: Științe juridice, 6(2), 35–47. https://www.ceeol.com/1278712
4. Ayers, R., Brothers, S., & Jansen, W. (2014). Guidelines on mobile device forensics (NIST Special Publication 800-101 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-101r1
5. Barbu, D., & Ghebaru, P. D. (2026). Percheziția informatică: când telefonul tău devine martor împotriva ta [The computer search: When your phone becomes a witness against you]. Universul Juridic. https://www.ujmag.ro/drept/perchezitia-informatica
6. Brezinski, D., & Killalea, T. (2002). Guidelines for evidence collection and archiving (RFC 3227). Internet Engineering Task Force. https://doi.org/10.17487/RFC3227
7. Buneci B. (2019). Percheziţia informatică – procedeu probatoriu pentru descoperirea, identificarea şi strângerea probelor stocate într-un sistem informatic [The computer search: An evidentiary procedure for discovering, identifying and gathering evidence stored in a computer system]. Instrumentul Bibliometric Național. Științe juridice. https://ibn.idsi.md/

8. Carrier, B. (2005). File system forensic analysis. Addison-Wesley Professional. https:// scholar.google.com/
9. Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers and the Internet (3rd ed.). Academic Press. https://scholar.google.com/
10. CCBE. (2025). CCBE response to the targeted stakeholder consultation on the implementation of the AI Act's rules for high-risk AI systems. Council of Bars and Law Societies of Europe. https://www.ccbe.eu/
11. CEPEJ. (2018). European ethical charter on the use of artificial intelligence in judicial systems and their environment. Council of Europe. https://rm.coe.int/ethical-charter
12. Ciorea, P. (2017). Considerații asupra percheziției informatice [Considerations on the computer search]. Penalmente Relevant, (1). https://www.ceeol.com/555336
13. Constitutional Court of Romania. (2009). Decision no. 1258 of 8 October 2009 on the plea of unconstitutionality of the provisions of Law no. 298/2008. https://legislatie.just.ro
14. Constitutional Court of Romania. (2016). Decision no. 51/2016 on the plea of unconstitutionality of the provisions of Article 142(1) of the Code of Criminal Procedure. https://www.ccr.ro/
15. Constitutional Court of Romania. (2017). Decision no. 244 of 6 April 2017 on the plea of unconstitutionality of the provisions of Article 145 of the Code of Criminal Procedure. MO, Part I, no. 529 of 6 July 2017. https://www.ccr.ro
16. Council of Europe. (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225). https://www.coe.int/
17. Council of Europe. (2026, May 15). European Union ratifies the Council of Europe Framework Convention on Artificial Intelligence. https://www.coe.int/en/web/artificial-intelligence
18. Court of Justice of the European Union. (2024a). Judgment of 30 April 2024, M.N. (EncroChat), C-670/22. ECLI:EU:C:2024:372.
19. Court of Justice of the European Union. (2024b). Judgment of 4 October 2024, C.G. v Bezirkshauptmannschaft Landeck, C-548/21, ECLI:EU:C:2024:830.
20. Crișan, E. G. (2017). Rolul percheziției informatice în probarea infracțiunilor contra drepturilor de proprietate intelectuală [The role of the computer search in proving offences against intellectual property rights]. Acta Universitatis Sapientiae, Legal Studies, 6(2), 249–258. https://acta.sapientia.ro/
21. Crosby, S. A., & Wallach, D. S. (2009). Efficient data structures for tamper-evident logging. In Proceedings of the 18th USENIX Security Symposium. USENIX Association. https://www.usenix.org/
22. 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 the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. Official Journal of the European Union, L 119, 4.5.2016, 89–131. https://eur-lex.europa.eu/eli/dir/2016/680/oj
23. Directive (eu) 2023/1544 of the european parliament and of the council laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings. Oficial Journal of European Union. Eur-Lex, L 191. CELEX 3A32023L1544
24. Directive 2014/41/eu of the european parliament and of the council regarding the European Investigation Order in criminal matters. Oficial Journal of European Union. Eur-Lex, L 130. CELEX32014L0041
25. Dushi, D., & Marcu, B.-I. (2026). Red lines under the EU AI Act: Unpacking the prohibition of individual risk assessment for the prediction of criminal offences. Future of Privacy Forum. https://fpf.org/
26. ENFSI. (2026). Best practice manual for the forensic examination of documents (ENFSI-BPM-FIT-01). European Network of Forensic Science Institutes. https://enfsi.eu/
27. European Commission. (n.d.). AI Act Service Desk: Law enforcement. Use cases classified as high-risk (Annex III, point 6). https://ai-act-service-desk.ec.europa.eu/de/node/466
28. European Commission. (2024). AI Act Explorer. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689, 12.7.2024. CELEX 202401689
29. European Court of Human Rights. (2023). Yüksel Yalçınkaya v. Türkiye [GC], application no. 15669/20, judgment of 26 September 2023. https://hudoc.echr.coe.int/

30. European Union (2024). Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. Official Journal of the European Union, L 257. CELEX 32024R1183
31. European Union (2026). Digital omnibus regulation on AI. Regulation (EU) 2026/1744 as regards the simplification of the implementation of harmonised rules on artificial intelligence. Official Journal of the European Union. Eur-Lex. Access to European Union Law. CELEX 32026R1744
32. Golaszewski, E., Krawetz, N., Sherman, A. T., Zieglar, E., Matukumalli, S. K., Yus, R., Kegley, C. L., Barthel, M., Bowman, W., Barot, B., & Kullman, K. (2026). Verifying provenance of digital media: Why the C2PA specifications fall short. https://doi.org/10.48550/arXiv.2604.24890
33. Grădinaru, S. (2024). Controversies regarding the legality of interceptions carried out through the National Center for Interception of Communications within the Romanian Information Service. Annals of 'Dunarea de Jos' University of Galati: Legal Sciences (ALS), Fascicle XXVI, 2024, v. 7, n. 1, p. 55. ISSN 2601-9779. https://www.gup.ugal.ro/ugaljournals/
34. High Court of Cassation and Justice, Criminal Division. (2014). Interlocutory ruling no. 3147 of 12 December 2014. https://www.scj.ro
35. High Court of Cassation and Justice, Criminal Division. (2024). Decision no. 642 of 25 September 2024. https://www.scj.ro
36. High Court of Cassation and Justice, Panel for the Resolution of Points of Law in Criminal Matters. (2018). Decision no. 2 of 8 February 2018. https://www.scj.ro
37. High Court of Cassation and Justice, Panel for the Resolution of Points of Law in Criminal Matters. (2023). Decision no. 56 of 18 September 2023 (case no. 1.235/1/2023). Monitorul Oficial al României, Part I, no. 910 of 10 October 2023. https://www.scj.ro
38. ISO/IEC Standard, International. (2014). Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. International Organization for Standardization. igital Evidence and Electronic Signature Law Review. 10.14296/deeslr.v10i0.2015
39. Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response (NIST Special Publication 800-86). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-86
40. Law no. 135/2010 on the Code of Criminal Procedure, published in Monitorul Oficial al României, Part I, no. 486 of 15 July 2010, as subsequently amended and supplemented. https://legislatie.just.ro
41. Law no. 64/2004 ratifying the Council of Europe Convention on Cybercrime, adopted in Budapest on 23 November 2001, published in Monitorul Oficial al României, Part I, no. 343 of 20 April 2004. https://legislatie.just.ro/51288
42. Legislative Observatory. European Parliament (2023). Electronic evidence regulation: European production and preservation orders for electronic evidence in criminal matters. Official Journal of the European Union, L 191, 28.7.2023, 118–180. https://oeil.europarl.europa.eu/
43. Lone, A. H., & Mir, R. N. (2019). Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. Digital Investigation Journal, V 28, Pages 44–55. https://doi.org/10.1016/j.diin.2019.01.002
44. Merkevičius, R. (2024). Judgment of the Court of Justice of the European Union of 30 April 2024 in the "EncroChat case" (case No. C-670/22): Does this judgment really legitimise forum shopping in criminal proceedings, and how will it impact Lithuanian criminal proceedings? Teisė, 132, 20–36. https://doi.org/10.15388/Teise.2024.132.2
45. Merkle, R. C. (1988). A digital signature based on a conventional encryption function. In C. Pomerance (Ed.), Advances in Cryptology - CRYPTO '87 (Lecture Notes in Computer Science, Vol. 293, pp. 369–378). Springer. https://doi.org/10.1007/3-540-48184-2_32
46. Moise, A. C. (2024). Some Applications of the Artificial Intelligence in the Field of Forensic Investigation. Analele Stiintifice Ale Universitatii Alexandru Ioan Cuza Din Iasi Stiinte Juridice, 70, 39. https://access.heinonline.com/
47. Murariu, A.-S. (2023). Contestarea, în procedura camerei preliminare, a încheierii judecătorului de drepturi și libertăți prin care s-a admis măsura de supraveghere tehnică [Challenging, in the preliminary chamber procedure, the ruling of the judge of rights and liberties authorising technical surveillance]. Revista Universul Juridic, (9), 21–31. https://www.ceeol.com/1235553

48. National Institute of Standards and Technology. (2015). Secure hash standard (SHS). Federal Information Processing Standards Publication (180-4). https://doi.org/10.6028/NIST.FIPS.180-4
49. Neagu, I., & Damaschin, M. (2020). Tratat de procedură penală. Partea generală [Treatise on criminal procedure: General part] (3rd ed.). Universul Juridic. https://scholar.google.com/
50. Pintea, F.-A. (2026). Prototip de lanț de custodie verificabil criptografic pentru probe digitale [Prototype of a cryptographically verifiable chain of custody for digital evidence] (Version 1.0.0) [Software]. Zenodo. https://doi.org/10.5281/zenodo.23519444
51. Roibu M., Costăchescu Ș. and Petrușan N. (2026). Electronic evidence in criminal investigations. New obligations for communications service providers. Lawyers Week Journal. https://lawyersweek.net/
52. Romanian Senate, Foreign Policy Committee. (2026). Sinteza lucrărilor Comisiei pentru politică externă [Summary of the proceedings of the Foreign Policy Committee] (L272/2026). https://www.senat.ro/
53. Sandhu, R., Schneier, B., & Kelsey, J. (1999). Secure audit logs to support computer forensics. ACM Transactions on Information and System Security (TISSEC), V 2, no. 2, 1999, pp. 159-176. https://doi.org/10.1145/317087.317089
54. Serban, A. & Marcu, B.-I. (2026). The AI Act implementation timeline: What changes under the AI Omnibus?. Future of Privacy Forum, https://fpf.org/ai
55. Stevens, M., Bursztein, E., Karpman, P., Albertini, A., & Markov, Y. (2017). The first collision for full SHA-1 (Cryptology ePrint Archive, Paper 2017/190; revised version of the paper presented at CRYPTO 2017). https://eprint.iacr.org/2017/190
56. Timișoara Court of Appeal. (2019). Interlocutory ruling no. 121 of 14 October 2019, case no. 654/59/2019. https://portal.just.ro
57. Udroiu, M. (Coord.). (2020). Codul de procedură penală. Comentariu pe articole [The Code of Criminal Procedure: Article-by-article commentary] (3rd ed.). C.H. Beck. https://scholar.google.com/Codul de procedură penala
58. Volonciu, N., et al. (2007). Codul de procedură penală. Comentariu pe articole [The Code of Criminal Procedure: Article-by-article commentary] (4th ed.). Hamangiu. ISBN 978-606-27-2523-5. https://scholar.google.com/
59. Wang, X., & Yu, H. (2005). How to break MD5 and other hash functions. In Annual international conference on the theory and applications of cryptographic techniques. Berlin, Heidelberg: Springer Berlin Heidelberg. Vol. 3494, pp. 19–35. https://doi.org/10.1007/11426639_2
60. Wasim A. & Fahim A. (2024). Human Rights and Technology: Exploring How Technological Advancements Impact Human Rights, Particularly in Surveillance and Data Collection. International-Journal-of-Arts-and-Humanities-Studies. 4(4):19-27. https://doi.org/10.32996/Ijahs.2024.4.4.4