CADERNOS DE DEREITO ACTUAL
www.cadernosdedereitoactual.es

© ***Cadernos de Dereito Actual*** Nº 31. Núm. Ordinario (2026), pp. 176-195
·ISSN 2340-860X - ·ISSNe 2386-5229

Forensic approaches to verifying the evidence reliability in the process of collecting and evaluating information during pre-trial investigations

Andrii Antoshchuk[1]
National Academy of Internal Affairs
Olha Dobrova[2,*]
Interregional Academy of Personnel Management
Olena Volobuieva[3]
Donetsk State University of Internal Affairs
Vladas Tumalavičius[4]
Turiba University
Oksana Bryskovska[5]
National Academy of Internal Affairs

[1] PhD in Legal Sciences, Associate Professor, Head of the Department of Criminalistics and Forensic Medicine, National Academy of Internal Affairs, Kyiv, Ukraine. His main scientific interests are: methods of investigating certain types of criminal offences, tactics for conducting certain investigative (search) activities. E-mail: andriiantoshchuk15@gmail.com.
[2] PhD in Sciences, Interregional Academy of Personnel Management, Kyiv, Ukraine. E-mail: kravchenkooolha@yahoo.com (corresponding author).
[3] Donetsk State University of Internal Affairs, Kropyvnytskyi, Ukraine. She investigates psychological, personnel and gender aspects of professional activity in the security sector and the educational systems of these services. Her main scientific interests are: criminal procedure and criminalistics. E-mail: olena_volobueva@ukr.net.
[4] Dr.iur., Leading Researcher, Turiba University, Riga, Latvia. He has research publications on security, public administration, law, and international integration. E-mail: vladas.t@gmail.com.
[5] PhD in Law, Senior Researcher, Lead Researcher, Research Laboratory on Crime Prevention Problems of the Educational and Scientific Institute of Police Activities, National Academy of Internal Affairs, Kyiv, Ukraine. She examines criminal procedure, investigative-operational activity, illicit arms trafficking, and cyber-crime issues in Ukraine. E-mail: oksanabryskovska@ukr.net.

Abstract: The purpose of this research was to determine appropriate forensic methods for evaluating the reliability of evidence and to formulate a procedural algorithm for investigators and prosecutors that guarantees a systematic and consistent verification of the evidentiary framework. To this end, a doctrinal legal analysis of the provisions of national and international law (CPC of Ukraine, Budapest Convention, ISO/IEC 27001), a comparative examination of EU and US practices (EPPO Guidelines, Federal Rules of Evidence, Bundesgerichtshof, Sąd Najwyższy), and a content analysis of 20 Supreme Court decisions from Ukraine were conducted. The findings showed that the principal criteria for reliability were proportionality, transparency, and the efficacy of remedial measures. Methodologically, these criteria were operationalized through a rule-based coding scheme applied to the selected legal instruments and judicial decisions, with cross-jurisdictional triangulation of recurring procedural defects and verification steps. It was found that in Ukrainian jurisprudence, the predominant cause for deeming evidence inadmissible was the violation of the procedural protocol for its collection, whereas in Germany and Poland, deficiencies in the "chain of custody" were more prevalent. The comparison with international standards revealed a structural divergence between formal reliability requirements and their procedural operationalization within the national process. The scientific novelty lies in the establishment of a stepwise, auditable algorithm for validating evidence, which integrates doctrinal legal, comparative, and empirical approaches into a coherent framework of procedural evaluation. This study also emphasizes the need to strengthen procedural practices within Ukraine, aligning them with European standards and technical safeguards, thereby improving the consistency of evidence verification. The practical significance of the study lies in the possibility of applying its findings to develop guidelines and methodological recommendations, as well as to strengthen the professional competencies of investigators and prosecutors in the field of evidence verification within Ukraine.

Keywords: Evidence Admissibility, Reliability, Criminal Process, Digital Evidence, Saturation Principle, International Standards, Verification Algorithm

Resumen: El propósito de esta investigación fue determinar enfoques forenses para la evaluación de la fiabilidad de las pruebas y diseñar un algoritmo procedimental dirigido a investigadores y fiscales que asegure una verificación sistemática y coherente del conjunto probatorio. Con este fin, se llevó a cabo un análisis doctrinal jurídico de las disposiciones del derecho nacional e internacional (CPC de Ucrania, Convenio de Budapest, ISO/IEC 27001), un examen comparativo de las prácticas de la UE y los EE. UU. (Directrices de la Fiscalía Europea, Reglas Federales de Prueba, Bundesgerichtshof, Sąd Najwyższy) y un análisis de contenido de 20 sentencias del Tribunal Supremo de Ucrania. Las conclusiones mostraron que los criterios principales de fiabilidad eran la proporcionalidad, la transparencia y la eficacia de las medidas correctivas. Metodológicamente, estos criterios se operacionalizaron mediante un esquema de codificación basado en reglas aplicado a los instrumentos normativos seleccionados y a las decisiones judiciales, con triangulación interjurisdiccional de defectos procedimentales recurrentes y pasos de verificación. Se constató que, en la jurisprudencia ucraniana, la causa predominante para considerar inadmisibles las pruebas era la violación del protocolo procesal para su obtención, mientras que en Alemania y Polonia prevalecían las deficiencias en la «cadena de custodia». La comparación con las normas internacionales reveló una divergencia estructural entre los requisitos formales de fiabilidad y su operacionalización procedimental dentro del proceso nacional. La novedad científica reside en el establecimiento de un algoritmo metódico por etapas y auditable para validar las pruebas, que integra enfoques doctrinales, comparativos y empíricos en un marco coherente de evaluación

procedimental. Las implicaciones prácticas de este estudio vienen determinadas por el potencial de utilización de los resultados para formular directrices y recomendaciones metodológicas, así como para mejorar las competencias de los investigadores y fiscales en el ámbito de la verificación de pruebas.

Palabras clave: Admisibilidad de las pruebas, Fiabilidad, Proceso penal, Pruebas digitales, Principio de saturación, Normas internacionales, Algoritmo de verificación

1. Introduction

In the global landscape of criminal justice, the imperative of authenticating evidence assumes new dimensions under the influence of digitalization. Evidence increasingly manifests in the form of electronic artifacts (data extracted from cloud services, network logs, or multimedia objects), necessitating not only legal scrutiny but also thorough technical verification. As articulated by Nath et al.[6], even the most minimal breach in the chain of custody can undermine digital material's evidentiary power. This is due to the fact that the continuity of source fixation and transmission is an essential prerequisite for establishing authenticity. A study conducted by Cermak et al.[7] demonstrates that the application of relational graphs and network analysis algorithms facilitates the detection of patterns within digital flows that can either corroborate or refute the authenticity of evidence. A similar concept is explored by Kretz et al.[8], who maintain that the technology of layered attestation, that is multi-tiered verification of data integrity, mitigates the falsification risk and enhances forensic assessment's reproducibility. Within the broader context of advancements in artificial intelligence, Palekar and Kumar[9] show that self-attention models can be semantically adapted to label images and audio evidence, thereby increasing the accuracy of their interpretation during pretrial investigations.

Despite the growing availability of technical tools for verifying digital artifacts, procedural practice often remains fragmented: legal requirements for admissibility are articulated at a high level of generality, while the technical steps needed to demonstrate integrity, provenance, and reproducibility are inconsistently documented and unevenly applied. As a result, reliability assessments may depend on ad hoc judgments rather than on a transparent and repeatable verification sequence, which increases the risk of evidentiary exclusion and undermines the predictability of pre-trial decision-making.

This research seeks to determine appropriate forensic methodologies for assessing the reliability of evidence and to elaborate a procedural algorithm for investigators and prosecutors that enables a consistent and structured verification of the evidentiary base. The study involves an examination of national and international law-enforcement practices related to evidentiary reliability in order to

---

[6] NATH, S.; SUMMERS, K.; BAEK, J.; AHN, G.-J. "Digital evidence chain of custody: Navigating new realities of digital forensics", In Proceedings of the 2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA) (p. 11–20). Institute of Electrical and Electronics Engineers, 2024. https://doi.org/10.1109/TPS-ISA62245.2024.00012

[7] CERMAK, M.; FRITZOVÁ, T.; RUSŇÁK, V.; SRAMKOVA, D. "Using relational graphs for exploratory analysis of network traffic data", Forensic Science International: Digital Investigation, v. 45, n. (Supplement), 2023, 301563. https://doi.org/10.1016/j.fsidi.2023.301563

[8] KRETZ, I. D.; PARRAN, C. C.; RAMSDELL, J. D.; ROWE, P. D. "Evidence tampering and chain of custody in layered attestations", arXiv:2402.00203, 2024. https://doi.org/10.48550/arXiv.2402.00203

[9] PALEKAR, V.; KUMAR, S. L. "An effective image annotation using self-attention based stacked bidirectional capsule network", Computer Standards Interfaces, v. 93, 2025,103973. https://doi.org/10.1016/j.csi.2025.103973

define key verification criteria, an assessment of the most effective forensic techniques capable of ensuring the relevance and admissibility of evidentiary information under conditions of digital transformation, and the development of practical recommendations for investigators and prosecutors in the form of a procedural algorithm that integrates doctrinal legal, comparative, and empirical approaches. Such an integrated framework is intended to support a comprehensive evaluation of evidential reliability at the pre-trial investigation stage.

Accordingly, the paper addresses the following problem: how to operationalize broadly formulated admissibility and reliability requirements into an auditable sequence of verification actions that can accommodate both traditional evidence and digital/technological artifacts. The proposed algorithm does not purport to introduce new legal standards; rather, it systematizes verification steps into "gatekeeping" checkpoints (proportionality, transparency, and remedial efficacy) and specifies the documentation outputs expected at each checkpoint, thereby strengthening consistency and reducing interpretive variability in practice.

The practical value of the study lies in the preparation of clear and applicable recommendations for law-enforcement bodies aimed at improving the quality of evidence, promoting greater consistency in judicial practice, and strengthening public trust in the results of pre-trial investigations.

2. Literature review

In the scholarly literature, the issue of evidential reliability is examined across several interrelated domains, among which technological, methodological, and forensic aspects predominate. At the same time, the reviewed scholarship frequently addresses reliability either at the level of general admissibility principles or within isolated technical subfields, which creates a recurring gap between legally required reliability findings and the operational steps needed to demonstrate integrity, provenance, and reproducibility—especially for digital and mixed (digital–biological) evidence. The impact of artificial intelligence on the detection, interpretation, and evaluation of digital evidence is the subject of vigorous discourse. For instance, Aldahmani et al.[10] proposed a model for AI-driven detection of criminal traces at crime scenes, emphasizing the automated object documentation and the minimized human intervention. A similar perspective is adopted by Arthanari et al.[11], who regard machine learning as a mechanism to enhance the precision of data interpretation. That being said, their model is primarily focused on the laboratory phase of analysis, which constrains its practical validation within a procedural framework of pre-trial verification and documentation. Bhoyar et al.[12] extend this rationale by elucidating the capabilities of AI-driven pollen analysis; however, their methodology does not tackle the critical issue of results reproducibility in legal proceedings through standardized verification outputs and audit trails. Conversely, Bamigbade et al.[13] focus not on algorithmic precision,

---

[10] ALDAHMANI, F. K. A. M., ALMEHRZI, G. S. M. A., ALSEREIDI, E. M. S. M., ALDAHMANI, A. A. K. A., ALAHBABI, E. M. M. "Recent research study on AI-based crime scene evidence detection", In 2024 7th International Conference on Advanced Communication Technologies and Networking (CommNet) (pp. 1–6). IEEE, 2024. https://doi.org/10.1109/CommNet63022.2024.10793266

[11] ARTHANARI, A.; RAJ, S. S.; VIGNESH, R. "A narrative review in application of artificial intelligence in forensic science: Enhancing accuracy in crime scene analysis and evidence interpretation", Journal of International Oral Health, v. 17, n. 1, 2025,p. 15–22. https://doi.org/10.4103/jioh.jioh_162_24

[12] BHOYAR, L.; SRIVASTAVA, B. "Revolutionizing forensic investigations through AI-driven pollen analysis: A narrative review", Review of Palaeobotany and Palynology, v. 344, 2025, 105440. https://doi.org/10.1016/j.revpalbo.2025.105440

[13] BAMIGBADE, O.; SHEPPARD, J.; SCANLON, M. "Computer vision for multimedia geolocation in human trafficking investigation: A systematic literature review",

instead concentrate on applying computer vision to detect multimedia evidence in human trafficking cases, underscoring the imperative of maintaining a chain of custody. The second avenue of research pertains to the establishment of digital forensics standards and the evaluation of the institutional maturity of evidence collection systems. Thus, Zīle et al.[14] examine the interplay between digital forensics and criminal policy, illustrating the Latvian-Ukrainian approach to the development of unified standards for the collection and assessment of electronic evidence. Their findings resonate with those of Kudeikina[15], who considers expert testimony as a form of evidence in Latvian civil proceedings, highlighting the significance of professional qualifications and procedural integrity of expert analyses in ensuring the reliability of judicial outcomes. A separate category of literature is dedicated to the metrological and procedural reliability of digital tools. Brunty[16] emphasizes the necessity of validating digital expertise methodologies as a prerequisite for evidence admissibility, while Cao et al.[17] introduce the notion of "data trace", considered as an indicator of the reproducibility and transparency in evidentiary information processing. Notwithstanding these advances, standards-oriented studies often remain framework-level: they identify what should be ensured (integrity, authenticity, traceability), yet provide limited guidance on how investigators and prosecutors should sequence verification actions, document intermediate results, and apply "stop/go" thresholds at the pre-trial stage.

The third category of literature pertains to biological and specialized evidence, where reliability often depends not on technical procedures but on the interpretation nuances. Arslan[18] illustrates that microchimerism complicates the identification of individuals, as a solitary biological sample may encompass multiple DNA profiles. This challenges the traditional presumption of genetic uniqueness that is still upheld by forensic laboratories. In Bansode et al.[19], a comparable issue is illustrated through forensic entomology: the authors assert that even the collection of samples does not guarantee their reliability if environmental conditions disrupt the life cycle of insects. Lytvyn et al.[20] delve into the challenges associated with the execution of judicial decisions, positing that the efficacy of decision enforcement is intrinsically linked to public trust in justice and the dependability of the evidence on which these decisions are predicated. Fragkou et al.[21] advocate for a multimodal

---

arXiv:2402.15448, 2024. https://doi.org/10.48550/arXiv.2402.15448

[14] ZĪLE, A.; VILKS, A.; POLIANSKYI, A. "Digital forensics and criminal policy: Latvian–Ukrainian perspective", Socrates, v. 24, n. 3, 2022, p. 140–149. https://doi.org/10.25143/socr.24.2022.3.140-149

[15] KUDEIKINA, I. "Port as evidence in the civil proceedings of Latvia", Archives of Criminology and Forensic Sciences, v. 1, 2020, p. 73-79. https://doi.org/10.32353/acfs.1.2020.05

[16] BRUNTY, J. "Validation of forensic tools and methods: A primer for the digital forensics examiner", WIREs Forensic Science, v. 4, n. 1, 2022, e1474. https://doi.org/10.1002/wfs2.1474

[17] CAO, Z.; GAO, B.; LIU, Z.; XIONG, X.; WANG, B.; PEI, C. "Data trace as the scientific foundation for trusted metrological data: A review for future metrology direction", PeerJ Computer Science, v. 11, 2025, e3106. https://doi.org/10.7717/peerj-cs.3106

[18] ARSLAN, Z. "Microchimerism: The mystery of multiple DNA and its implications in forensic sciences", Forensic Science International, v. 367, 2025, 112345. https://doi.org/10.1016/j.forsciint.2024.112345

[19] BANSODE, S.; MORAJKAR, A.; RAGADE, V.; MORE, V.; KHARAT, K. "Challenges and considerations in forensic entomology: A comprehensive review", Journal of Forensic and Legal Medicine, v. 110, 2025, 102831. https://doi.org/10.1016/j.jflm.2025.102831

[20] LYTVYN, N.; ANDRUSHCHENKO, H.; ZOZULYA, Y. V.; NIKANOROVA, O. V.; RUSAL, L. M. "Enforcement of Court Decisions as a Social Guarantee of Protection of Citizens Rights and Freedoms", Prawo i Więź, v. 39, 2022, p. 80–102. https://doi.org/10.36128/priw.vi39.351

[21] FRAGKOU, K.; KETSEKIOULAFIS, I.; TOUSIA, A.; PIAGKOU, M.; BACOPOULOU, F.; FERENTINOS, P.; PEYRON, P.-A., BACCINO, E.; MARTRILLE, L.; PAPADODIMA, S. "From fragile lives to forensic truth: Multimodal forensic approaches to pediatric homicide and

approach that combines independent methodologies (morphological, toxicological, genetic), yet this strategy is vulnerable to varying degrees of technical precision across laboratories. The problem of cognitive bias in evidence is analyzed by Bird et al.[22] as a systemic concern: the expert, knowing the context of the case, unconsciously influences the anticipated outcome. Crown et al.[23] propose to mitigate this effect through blind estimation methods; however, their model oversimplifies the interaction between human factors and procedural inaccuracies. Both approaches acknowledge the problem, yet they fail to consider that cognitive errors are exacerbated particularly in mixed (digital-biological) scenarios. In a study by Makarenkov and Kosa[24], the utilization of digital technologies in forensic practice is examined as a mechanism for identifying corruption risks and threats to national security, though the authors emphasize that the absence of unified criteria for the reliability of digital evidence hinders the establishment of a coherent assessment system. The analysis reveals that contemporary digital methodologies can enhance the precision and expediency of forensic investigations. However, interdepartmental integration and standardized authentication protocols remain inadequately developed, thereby reducing the evidentiary weight of the information obtained.

In summary, scientific papers cover a diverse spectrum, ranging from artificial intelligence and digital readiness to biological and cognitive determinants. However, the reviewed strands remain insufficiently integrated at the procedural level: studies that strengthen technical accuracy (AI and tool validation), institutional capacity (standards and maturity), and interpretive safeguards (bias mitigation and multimodality) rarely converge into a unified pre-trial verification sequence that specifies (i) what must be checked, (ii) in what order, and (iii) what documentary outputs are required to demonstrate reliability. At the same time, there exists a notable deficiency in research that would integrate these methodologies into a cohesive forensic model for assessing evidence reliability in pretrial investigations, which constitutes the primary objective of this article. Accordingly, the present study synthesizes these domains into a single operational framework by translating high-level reliability requirements into an auditable algorithm of verification checkpoints (proportionality, transparency, and remedial efficacy) that can incorporate specialized modules for digital artifacts (e.g., integrity verification and chain-of-custody controls) alongside established approaches for biological and expert evidence.

3. Methodology

The study was conducted between January and September 2025 and executed in three interconnected stages, combined into a single methodological framework. Its aim was to delineate forensic methodologies for verifying the evidence reliability during the pretrial investigation stage. Also, the task was to establish a coherent algorithm of actions for investigators and prosecutors that ensures the integrity and verifiable reliability of the evidentiary base through a structured sequence of auditable verification steps and documented checkpoints. The methodology was

---

suspect death", Diagnostics, v. 15, n. 11, 2025, p. 1383. https://doi.org/10.3390/diagnostics15111383

[22] BIRD, C.; JONES, K.; BALLANTYNE, K. "Cognitive bias and contextual information management: Considerations for forensic handwriting examinations", Wiley Interdisciplinary Reviews: Forensic Science, v. 6, n. 4, 2024, e1530. https://doi.org/10.1002/wfs2.1530

[23] CROWN, N.; MARQUIS, R.; KUPFERSCHMID, E.; DZIEDZIC, T.; BELIC, D.; KERZAN, D. "Error mitigation in forensic handwriting examination: The examiner's perspective", Forensic Sciences Research, v. 9, n. 4, 2024, owae065. https://doi.org/10.1093/fsr/owae065

[24] MAKARENKOV, O.; KOSA, V. "Forensic Technique for Identifying Corruption Challenges to National Security through Digital Technologies", Baltic Journal of Economic Studies, v. 10, n. 4, 2024, p. 288–300. https://doi.org/10.30525/2256-0742/2024-10-4-288-300

predicated upon the integration of three analytical approaches (normative, comparative, empirical), culminating in a unified system of proof verification, provisionally termed the "triangle of verification." Within this framework, each approach fulfills an independent function: the legal level establishes the criteria, the comparative level assesses their applicability, and the empirical level evaluates their reproducibility in judicial practice. It is at the intersection of these levels that the logical sequence of procedural actions is constructed, which this study proposes as a generalized schema for reliability verification.

At the initial stage, a normative analysis of the norms governing the procedures for the formation, collection, and evaluation of evidence was undertaken.The national component encompassed the Criminal Procedure Code of Ukraine[25], the Criminal Code of Ukraine[26], the Law of Ukraine "On Electronic Identification and Electronic Trust Services"[27], the Law of Ukraine "On Basic Principles of Cybersecurity of Ukraine"[28], as well as by-laws legislation: the Order of the Prosecutor General's Office "On Approval of the Regulation on the Unified Register of Pretrial Investigations"[29] and the Order of the Prosecutor General No. 409 "On Ensuring the Processing of Operational Information"[30]. The international segment included the Budapest Convention[31], Council of Europe Recommendations on Electronic Evidence[32], the UN Digital Evidence Manual[33], ISO/IEC 27001:2022[34], and Ensuring Human Rights Compliance in Cybercrime Investigations OSCE[35]. The

[25] Law of Ukraine "Criminal Procedural Code of Ukraine"(No. 4651-VI, adopted April 13, 2012; current version as of August 1, 2025, based on Law No. 4560-IX). Verkhovna Rada of Ukraine. Available at: https://zakon.rada.gov.ua/go/4651-17 (accessed on 13 August 2025).
[26] Criminal Code of Ukraine (No. 2341-III, enacted April 5, 2001; current version as of July 17, 2025). Verkhovna Rada of Ukraine. Available at: https://zakon.rada.gov.ua/go/2341-14 (accessed on 13 August 2025).
[27] Law of Ukraine "On Electronic Identification and Electronic Trust Services" (No. 2155-VIII, adopted October 5, 2017; current version as of December 18, 2024). Verkhovna Rada of Ukraine. Available at: https://zakon.rada.gov.ua/go/2155-19 (accessed on 13 August 2025).
[28] Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine" (No. 2163-VIII, adopted October 5, 2017; current version as of June 28, 2024). Verkhovna Rada of Ukraine. Available at: https://zakon.rada.gov.ua/laws/show/2163-19 (accessed on 13 August 2025).
[29] Office of the Prosecutor General of Ukraine. Order No. 298 on the approval of the Regulations on the Unified Register of Pre-trial Investigations: procedure for its formation and maintenance, 2020, June 30 (current version as of September 16, 2025). Available at: https://zakon.rada.gov.ua/laws/show/v0298905-20 (accessed on 13 August 2025).
[30] Office of the Prosecutor General of Ukraine. Order No. 409 on the procedure for preparing, submitting, and processing special reports on criminal offenses and socially resonant events, 2020, September 3. Available at: https://wd.clarity-project.info/resource/73111d11-6184-4162-8740-6f69b8f294d7 (accessed on 13 August 2025).
[31] Council of Europe. The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols, 2001. Available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention (accessed on 13 August 2025).
[32] Council of Europe. Electronic Evidence Guide v.3.0: Guidelines on the treatment of electronic evidence in criminal proceedings. Strasbourg: Council of Europe, 2022. Available at: https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/s3fs-public/2025-06/guidelines-trtmnt-elctrnc.pdf (accessed on 13 August 2025).
[33] United Nations. Guide for First Responders on the Collection of Digital Devices in the Battlefield. New York: United Nations, 2024. Available at: https://www.un.org/counterterrorism/sites/default/files/guide-first_responders-digital_devices_in_battlefield.pdf?utm_source=chatgpt.com (accessed on 13 August 2025).
[34] ISO/IEC 27001:2022. Information technology—Security techniques—Guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva: International Organization for Standardization, 2022. Available at: https://www.iso.org/standard/44381.html (accessed on 13 August 2025).
[35] OSCE. Ensuring Human Rights Compliance in Cybercrime Investigations, 2023. Available at: https://www.osce.org/files/f/documents/e/3/554901.pdf (accessed on 13 August 2025).

analysis was conducted at three levels (legislative, sub-legal, institutional) to identify gaps and delineate criteria for the authenticity verification. At this stage, the range of forensic techniques deemed suitable for subsequent effectiveness testing in the comparative analysis was also clarified. Additionally, the fundamental technical verification parameters, including the chain of custody, hash verification, instrument protocol, procedural mandate, and evidentiary relevance were identified as pivotal variables for further comparative and empirical analysis. The second stage was dedicated to a comparative analysis of the law enforcement practices within the European Union and the United States. The focal point of this comparison was three jurisdictions that exemplify models of evidentiary law. The United States serves as an illustration of a common law system characterized by a well-developed doctrine regarding the interplay between reliability and admissibility, as articulated in the Federal Rules of Evidence[36]. Germany epitomizes a continental model, wherein the Bundesgerichtshof[37] consistently upholds the principle of Beweisverwertungsverbot (the prohibition of utilizing evidence obtained in violation of procedural norms). Poland represents a post-socialist system that has been adapted to align with European standards, where the Sąd Najwyższy[38] establishes flexible criteria for the admissibility of digital evidence. The comparative analysis was conducted in accordance with the principles of positive (systems with established practices) and negative control (systems devoid of specific regulations). At this juncture, a structural framework for the reliability verification was formulated, delineating the logical progression of procedural actions, from the initial documentation of evidence to its assessment concerning admissibility and proportionality.

In the third stage, empirical validation of the identified patterns was conducted through a comprehensive content analysis of 20 final rulings from the Supreme Court of Ukraine[39] spanning the years 2018 to 2024, specifically addressing the evidence reliability and admissibility. The sample was formed based on key terms, namely "admissibility of evidence", "falsification of evidence", "violation of the collection procedure", and was determined following the saturation principle. The unit of analysis encompassed the paragraphs within the motivational sections that pertained to admissibility criteria. MAXQDA (for coding), NVivo (for stability verification), and AntConc (for pattern analysis) were employed to ensure reproducibility. The findings from the empirical phase facilitated assessing the practical applicability of the devised verification scheme and refined the sequence of its components.

The operationalization of key concepts was carried out in accordance with international standards: "proportionality" – the balance between interference in individual rights and public necessity (ECHR proportionality test); "transparency" – substantiated reasoning underpinning the judgment; "effectiveness of the remedy" – the presence of real consequences for the parties involved (exclusion of evidence

---

[36] Federal Rules of Evidence. Federal rules of evidence as amended to December 1, 2023 (Committee Print No. 6), 2023. Available at: https://www.uscourts.gov/sites/default/files/evidence_federal_rules_pamphlet_dec_1_2023.pdf (accessed on 13 August 2025).

[37] Bundesgerichtshof. EncroChat-Data may be used for the Investigation of serious criminal Offences. 2022. Karlsruhe: Federal Court of Justice of Germany, 2022. https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/EN/2022/2022038.html (accessed on 13 August 2025).

[38] Sąd Najwyższy. Wyrok z dnia 13 maja 2021 r., sygn. V CSKP 41/21. Warszawa: Sąd Najwyższy, 2021. Available at: https://www.inforlex.pl/dok/tresc%2CFOB00000000000005398370%2CWyrok-SN-z-dnia-13-maja-2021-r-sygn-V-CSKP-41-21.html (accessed on 13 August 2025).

[39] Unified State Register of Court Decisions. State Judicial Administration of Ukraine, 2025. Available at: https://reyestr.court.gov.ua (accessed on 13 August 2025).

retrial, annulment of sentence, evidence retrial). Validation entailed cross-coding of results, juxtaposition with international UNODC and EPPO Guidelines, as well as an analysis of adverse examples. The result of this three-stage investigation yielded the formulation of a coherent scheme for verifying the evidence reliability, which combines legal norms, international standards, as well as empirical patterns of judicial practice, serving as a methodological foundation for the professional training of investigators and prosecutors.

4. Results

The results of the normative analysis revealed that the current Criminal Procedural Code of Ukraine[40] and the Criminal Code of Ukraine[41] lack specialized protocols for ascertaining the digital evidence's authenticity. The provisions of these legal frameworks are confined to broad stipulations regarding admissibility and relevance, yet they fail to delineate criteria for technical authenticity or procedures pertaining to the "chain of custody". The Law of Ukraine "On Electronic Identification and Electronic Trust Services"[42] establishes foundational legal principles for the utilization of electronic signatures and authentication mechanisms; however, it does not incorporate these elements within the field of criminal proceedings. A parallel deficiency is evident in the Law of Ukraine "On Basic Principles of Cybersecurity of Ukraine"[43], which establishes strategic directives for state policy but neglects to devise procedural instruments for scrutinizing digital evidence in the context of criminal investigations. It is of note that even the subordinate legal framework remains disjointed. The Order of the Prosecutor General's Office "On Approval of the Regulation on the Unified Register of Pretrial Investigations"[44] and the Order of the Prosecutor General No. 409 "On Ensuring the Processing of Operational Information"[45] govern registration procedures but do not stipulate requirements for digital data preservation, the its verification, or the affirmation of its immutability throughout the procedural cycle. This fragmentation engenders a lack of standardized protocols, compelling investigators and prosecutors to adopt disparate and inconsistent methodologies.

A comparative analysis with international legal instruments unveiled marked discrepancies in the level of regulatory precision. For instance, the Federal Rules of Evidence[46] in the United States establish explicit criteria for the authenticity of digital evidence and mandate procedural verification of its authenticity upon admission to the judicial process. In Germany, the jurisprudence of the Bundesgerichtshof[47] invokes the principle of Beweisverwertungsverbot, which safeguards against the inclusion of evidence procured in contravention of established protocols, yet it does not delineate the procedures for verifying electronic data. The Polish legal system, as articulated in the ruling of Sąd Najwyższy[48], exhibits a degree of flexibility in the deployment of digital evidence; however, it has yet to establish a cohesive model for overseeing its reliability.

International standards, namely, the Budapest Convention[49], the Electronic Evidence Guide[50], and the Ensuring Human Rights Compliance in Cybercrime

[40] Law of Ukraine "Criminal Procedural Code of Ukraine". 2025. Ibid.
[41] Criminal Code of Ukraine. 2025. Ibid.
[42] Law of Ukraine "On Electronic Identification and Electronic Trust Services". 2025. Ibid.
[43] Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine". 2025. Ibid.
[44] Office of the Prosecutor General of Ukraine. 2025. Ibid.
[45] Office of the Prosecutor General of Ukraine. 2020. Ibid.
[46] Federal Rules of Evidence. 2023. Ibid.
[47] Bundesgerichtshof. 2022. Ibid.
[48] Sąd Najwyższy. 2021. Ibid.
[49] Council of Europe. 2001. Ibid.
[50] Council of Europe. 2022. Ibid.

Investigations[51] primarily concentrate on the technical dimensions of data retention and the safeguarding of human rights, yet they lack direct procedural incorporation within Ukrainian practice. In light of the study's objectives, the preponderance of national regulations illustrated in the accompanying table is justified by the necessity for a comprehensive examination of Ukrainian legislation as the principal focus of the analysis. International and foreign sources are presented for comparative scrutiny of key provisions, thereby facilitating an assessment in terms of aligning the Ukrainian system with universally accepted standards for verifying the evidence reliability. As mentioned in the methodology, the first "normative" stage focuses on Ukrainian legislation and includes international instruments such as the Budapest Convention and Council of Europe recommendations, while these are discussed in the context of the second "comparative" stage in the results. International standards, namely, the Budapest Convention, the Electronic Evidence Guide, and the Ensuring Human Rights Compliance in Cybercrime Investigations, primarily concentrate on the technical dimensions of data retention and the safeguarding of human rights, yet they do not establish a unified procedural sequence for evidentiary verification that can be directly applied at the pre-trial stage within Ukrainian criminal proceedings. To elucidate the identified disparities, a synthesized matrix of national and foreign regulatory deficiencies and risks pertaining to the evidentiary base is presented in Table 1.

Table 1. Analytical gaps in the national regulatory framework for verifying the evidence validity.

Norma	**Gap**	**Consequence**
Criminal Procedure Code of Ukraine (2025)	Lack of a clear procedure for verifying the authenticity and integrity of digital evidence	Risk of divergent judicial practice in assessing admissibility and reliability
Criminal Code of Ukraine (2025)	Insufficient specificity on evidence falsification and procedural consequences	Risk of a formalized assessment of credibility without documented verification steps
Law of Ukraine "On Electronic Identification and Electronic Trust Services" (2025)	The procedure for integrating electronic trust services into criminal proceedings has not been settled	Inconsistent use of electronic signatures and seals in evidentiary documentation
Law of Ukraine "On Basic Principles of Cybersecurity of Ukraine" (2025)	Lack of mechanisms to verify compliance with human rights during cyber investigations	Risk of procedural challenges related to rights compliance in pre-trial digital evidence collection
Order of the Prosecutor General's Office "On the Unified Register of Pre-Trial Investigations" (2025)	Uniform requirements for digital data preservation and verification in the Unified Register of Pre-Trial Investigations are not defined	Fragmentation of documentation practices and reduced traceability of evidentiary records
Order of the Prosecutor General No. 409 (2020)	The procedure for evaluating operational information as evidence is not regulated	Risk of inconsistent admissibility assessments and reduced evidentiary weight of operational materials
Federal Rules of Evidence (2023, USA)	Residual reliance on judicial discretion in assessing credibility	Variability in evidentiary assessments across courts despite formal authenticity requirements
Bundesgerichtshof (2022, Germany)	Strict application of the Beweisverwertungsverbot principle without specifying verification steps for digital evidence	Exclusionary safeguards are applied, while digital verification remains procedurally under-specified
Sąd Najwyższy (2021, Poland)	Lack of unified chain of custody standards for digital evidence	Case-by-case flexibility with limited standardization of admissibility criteria for digital evidence

[51] OSCE. 2023. Ibid.

Norma	Gap	Consequence
The Budapest Convention (2001) - Normative Stage	Does not contain operational pre-trial verification procedures for implementation in national systems	Framework-level obligations with indirect impact on day-to-day evidentiary verification
Council of Europe: Electronic Evidence Guide (2022) - Normative Stage	It is not binding on Member States and there is no monitoring of implementation	Non-binding guidance with heterogeneous implementation across jurisdictions
OSCE (2023): Ensuring Human Rights Compliance in Cybercrime Investigations - Normative Stage	Focused on human rights, but without clear procedural integration into the criminal process	Rights safeguards are articulated, while procedural embedding in evidence verification remains partial
ISO/IEC 27001:2022	Defines technical standards without fixing procedural guarantees	Misalignment between information-security controls and procedural proof requirements

Source: consolidated by the author on the basis of the Law of Ukraine "Criminal Procedural Code of Ukraine"[52], Criminal Code of Ukraine[53], Law of Ukraine "On Electronic Identification and Electronic Trust Services"[54], Law of Ukraine "On Basic Principles of Cybersecurity of Ukraine"[55], Order of the Office of the Prosecutor General "On the Unified Register of Pre-Trial Investigations"[56], Order of the Prosecutor General No. 409 "On Ensuring the Processing of Operational Information"[57], Federal Rules of Evidence[58], Bundesgerichtshof[59], Sąd Najwyższy[60], Budapest Convention[61], Council of Europe[62], OSCE[63], ISO/IEC 27001[64].

Table 1 summarizes the principal statutes governing evidence collection and verification, highlighting the existing deficiencies and their consequences. The analysis showed that the predominant issues stem from the absence of operationally defined criteria for the admissibility of electronic evidence within the Criminal Procedure Code (CPC), the insufficient development of chain of custody protocols, as well as the fragmented regulatory landscape pertaining to cybersecurity. These shortcomings were associated with disparate judicial practices and a reduction in the predictability of evidentiary assessments, thereby increasing the risk of decreased evidentiary value. Concurrently, international standards (ISO/IEC, Council of Europe, OSCE) were identified as providing framework-level requirements for integrity and traceability, while leaving procedural implementation choices to national systems. Importantly, the Budapest Convention, the Council of Europe's Electronic Evidence Guide, and the OSCE's Ensuring Human Rights Compliance in Cybercrime Investigations are now specifically categorized under the "Normative Stage". This distinction emphasizes their role in providing overarching guidelines without direct procedural integration, contrasting with the operationalized approaches found in national jurisdictions.

The comparative analysis revealed recurring authentication components across the European Union and the United States, as well as their reflected application in Germany and Poland. In EU practice, the evidence evaluation is conducted through a three-step framework – procedural integrity, technical authenticity, and relevance

[52] Law of Ukraine "Criminal Procedural Code of Ukraine". 2025. Ibid.
[53] Criminal Code of Ukraine. 2025. Ibid.
[54] Law of Ukraine "On Electronic Identification and Electronic Trust Services". 2025. Ibid.
[55] Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine". 2025. Ibid.
[56] Office of the Prosecutor General of Ukraine. 2025. Ibid.
[57] Office of the Prosecutor General of Ukraine. 2020. Ibid.
[58] Federal Rules of Evidence. 2023. Ibid.
[59] Bundesgerichtshof. 2022. Ibid.
[60] Sąd Najwyższy. 2021. Ibid.
[61] Council of Europe. 2001. Ibid.
[62] Council of Europe. 2022. Ibid.
[63] OSCE. 2023. Ibid.
[64] ISO/IEC 27001. 2022. Ibid.

to the matter at hand[65]. In the United States, control is based on a synthesis of Federal Rules of Evidence (FRE) 901 and the Daubert test, whereby admissibility is contingent upon the methodology's reliability, its verifiability, and its acceptance within the scientific community. German legal practice[66] emphasizes a "transparent technical pathway", characterized by detailed logging of all access stages and the use of checksums; identified deficiencies in the preservation chain were linked to exclusion or to limitations in evidentiary weight. In Poland[67], a comparable framework is employed: the origin, authenticity, and comprehensiveness of the forensic report are scrutinized, and in cases of infringement, the court may either reduce the evidentiary weight or require additional confirmation. The overarching conclusion drawn from the comparative findings was that admissibility determinations were consistently conditioned on a comprehensive and replicable chain of custody alongside standardized technical procedures.

Figure 1 delineates a comparative matrix of checkpoints (chain of custody, hash verification, instrument protocol, procedural mandate, relevance) and typical judicial outcomes (confirmation/restriction/exclusion) across the EU, USA, Germany, and Poland.

Figure 1 shows the principal standards of proof verification within international jurisprudence (EU, USA, Germany, Poland). Quantification was conducted on a scale of 0 to 1, where 1 signifies the presence of an explicit, operationally documented requirement supported by consistent practice, and 0 denotes its absence. For each jurisdiction, the values in Figure 1 were assigned by coding whether the relevant checkpoint is (a) expressly regulated and (b) procedurally operationalized in practice; the total coverage index represents the arithmetic mean of the checkpoint scores. The total coverage index is as follows: EU – 0.95, Poland – 0.93, USA – 0.85, Germany – 0.68. The diagram reveals that higher coverage values were recorded in EU and Polish law, combining requirements for the chain of custody (1.0 and 1.0), hash verification (0.9 and 0.9), technical traceability (0.9 and 0.9), method reporting (1.0 and 1.0), and independent oversight (1.0 and 1.0). In the United States, the main focus is placed on the Daubert test (1.0), which assesses the reliability of methodologies. However, other parameters (e.g., chain of custody – 0.7 and technical traceability – 0.8) are primarily established through judicial practice. Germany demonstrated procedural safeguards (chain of custody – 0.9, reporting – 0.8, supervision – 0.9), while lower scores were recorded in technical specifics (traceability – 0.4 and hash verification – 0.5). The summarized findings indicate that all four jurisdictions shared a foundational core of checkpoints, namely chain of custody, reporting, and independent oversight. In addition, the cross-jurisdictional comparison showed higher differentiation in the technical checkpoints (traceability and hash verification), which were operationalized more consistently in the EU and Poland than in the USA and Germany.

A content analysis of twenty rulings from the Supreme Court of Ukraine (2020–2024) showed recurrent admissibility rationales. In most cases, the court invoked arguments pertaining to adherence to the chain of custody and the principle of proportionality between individual rights and public necessity, demanding transparent rationales for decisions and the effectiveness of

[65] European Public Prosecutor's Office (EPPO). Operational Guidelines on Investigation, Evocation Policy and Referral of Cases (College Decision 029/2021, as amended), 2022. https://www.eppo.europa.eu/sites/default/files/2022-02/EPPO_Operational_Guidelines_College_Decision_029.2021_as%20amended_by_College%20decision_007.2022.pdf

[66] Bundesgerichtshof. 2022. Ibid.

[67] Sąd Najwyższy. 2021. Ibid.

available remedies. Following the examination of the twentieth case, no new categories emerged, indicating category saturation within the selected corpus.

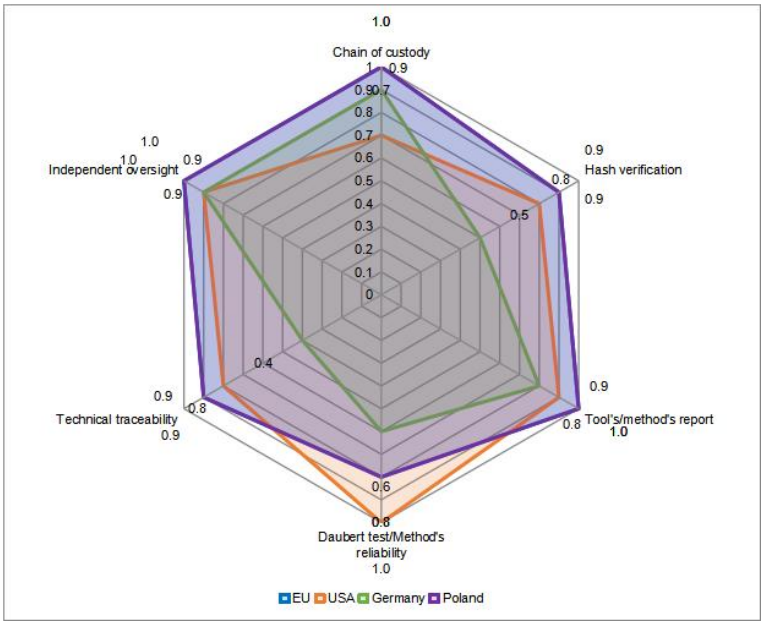

Figure 1. Availability of key standards for evidence verification in international practice. Source: consolidated by the author based on ISO/IEC 27001[68]; European Public Prosecutor's Office[69]; Federal Rules of Evidence[70]; Bundesgerichtshof[71]; Sąd Najwyższy[72]. Note. Scale: 0–1 (0 = no standard, 1 = full availability/implementation)

The structural framework of the algorithm for ascertaining the reliability of evidence reflects the rationale of a triadic control mechanism, which combines the legal, logical, and practical dimensions of evidentiary assessment. It is predicated on three interconnected criteria, namely proportionality, transparency, and efficiency, that collectively constitute a cohesive system for determining the admissibility of evidence during pre-trial investigations. The novelty of this approach lies not in the introduction of new criteria, but rather in the manner in which they are synthesized into a sequential verification algorithm that links regulatory mandates, technical validations (such as chain of custody, hash verification, and instrument protocol), and the corresponding documentation outputs produced by authorized entities. The proposed schema elucidates the interplay between the three tiers of control (normative, comparative, and empirical) and illustrates how each level influences the practical determination of evidence reliability.

As shown in Figure 2, the process of validating the evidence authenticity is executed through a three-step sequence combining legal, technical, and logical-evaluative control elements. At the first stage, a proportionality check is conducted, entailing the alignment evaluation between the intervention in personal rights and the overarching public necessity. This level is predicated on the European Convention on Human Rights (ECHR) proportionality test, thereby facilitating the exclusion of evidence procured beyond the procedural mandate or in contravention of the principle of minimal limitation of rights.

[68] ISO/IEC 27001. 2022. Ibid.
[69] European Public Prosecutor's Office (EPPO). 2022. Ibid.
[70] Federal Rules of Evidence. 2023. Ibid.
[71] Bundesgerichtshof. 2022. Ibid.
[72] Sąd Najwyższy. 2021. Ibid.

Subsequently, in the second stage, transparency is verified, which encompasses the rationale behind procedural determinations, the thoroughness of action documentation, and the presence of coherent logic in the construction of the evidentiary base. This methodology ensures the reproducibility of the actions undertaken by investigators or prosecutors, supported by technical indicators, such as the chain of custody, hash verification, instrument protocol, and procedural documentation, and mitigates the risk of arbitrary interpretations of facts.

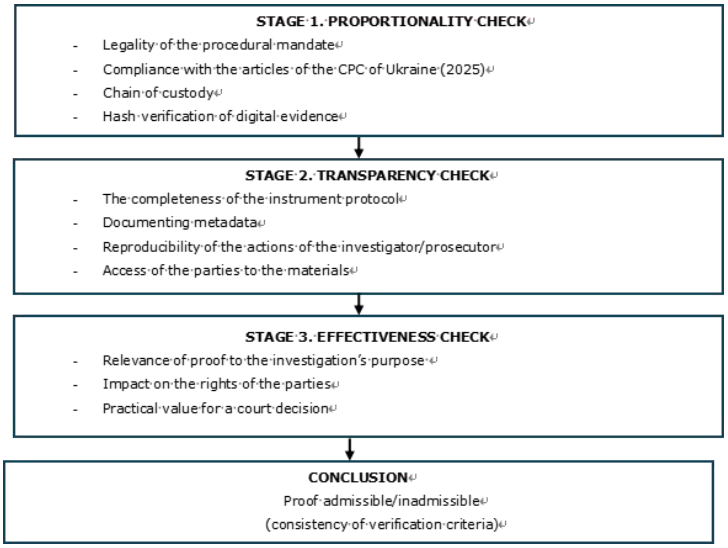

Figure 2. Structural diagram of the algorithm for verifying the evidence validity.

The third stage encompasses an effectiveness check, which ascertains whether the evidence is capable of producing a tangible legal outcome and is materially linked to the realization of justice while maintaining balance between the parties involved. The relevance of the evidence to the matter at hand, its influence on the investigative outcome, and adherence to the principle of justice are scrutinized. Evidence is deemed admissible only if all three criteria are consistently satisfied. A breach of any single criterion was treated as inadmissibility and necessitates re-evaluation.

Thus, the framework presented in Figure 2 reflects a structured sequence of verification checkpoints for reliability assessment, linking the stipulations of national legislation (first "normative" stage) with international standards (second "comparative" stage) (EPPO Guidelines, UNODC, ISO/IEC 27001). It was formulated as an algorithm for investigators and prosecutors, intended to standardize documentation and decision points across the proportionality, transparency, and effectiveness stages.

5. Discussion

The results obtained are consistent with international approaches that underscore the significance of procedural safeguards to verify the evidence validity. In U.S. legal frameworks, the principles of proportionality and transparency, as enshrined in the Federal Rules of Evidence, establish a judicious *balance* between the evidentiary weight and the safeguarding of parties' rights. At the same time, as posited by Palkova[73], the implementation of forensic data science as a universal

[73] PALKOVA, K.; AGAPOVA, O.; ZĪLE, A.; POLIANSKYI, A.; VADYM, K.; HASPARIAN, S.; MYKHAILO, M. "Sustainability of open educational resources in Forensic Sciences:

paradigm is feasible only with a robust technical foundation and standardized protocols, which remain conspicuously absent within the Ukrainian context. The necessity for formal validation of methodologies is corroborated by Brunty[74]; nevertheless, national practice remains contingent upon judicial discretion and lacks the established validation mechanisms, thereby diminishing the stability of judicial decisions. European studies by Qian et al.[75] as well as Loovens and Tinmaz[76] elucidate the advantages of integrating digital protocols with explainable artificial intelligence (XAI) and deepfake-forensics systems. However, the adoption of such instruments in Ukraine is quite limited by a dearth of certified laboratories and resources requisite for ensuring technical traceability. Practical models of digital forensics described by Kazaure et al.[77], alongside the framework for developing anti-corruption mechanisms and enhancing security in the financial sector proposed by Kussainov et al.[78], may prove beneficial for establishing a national system for validating evidence authenticity. However, they necessitate adaptation to the prevailing levels of institutional preparedness, regulatory limitations and the financial capabilities of public entities.

In contrast to the practices observed in Germany and Poland, where uncertainties regarding the chain of custody almost invariably result in the exclusion of evidence, Ukrainian cassation practice predominantly concentrates on procedural infractions during evidence collection. This trend aligns with the findings of Yermachenko et al.[79], which advocate for the implementation of intelligent digital infrastructure management mechanisms and public oversight of data reliability within the digital society, as well as with the investigation conducted by Mcuba et al.[80], which underscores the escalating vulnerability of judicial systems to deepfake manipulation. The international scholarly corpus reveals considerably more structured methodologies concerning specialized types of evidence. In the field of medical and legal expertise, Kaur et al.[81] and Nimbkar and Bhatt[82] describe clear

---

international experience", European Journal of Sustainable Development, v. 11, n. 3, 2022, p. 71. https://doi.org/10.14207/ejsd.2022.v11n3p71

[74] BRUNTY, J. 2022. Ibid.

[75] QIAN, H.; XIA, L.; GE, R.; FAN, Y.; WANG, Q.; JING, Z. "From black boxes to glass boxes: Explainable AI for trustworthy deepfake forensics", Cryptography, v. 9, n. 4, 2025, p. 61. https://doi.org/10.3390/cryptography9040061

[76] LOOVENS, J.; TINMAZ, H. "A systematic literature review of deepfakes in forensic science", Forensic Imaging, v. 43, 2025, 200647. https://doi.org/10.1016/j.fri.2025.200647

[77] KAZAURE, A. A.; JANTAN, A.; YUSOFF, M. N. "Digital forensics investigation approaches in mitigating cybercrimes: A review", Journal of Information Science Theory and Practice, v. 11, n. 4, 2023, p. 14–27. https://doi.org/10.1633/JISTaP.2023.11.4.2

[78] KUSSAINOV, K.; GONCHARUK, N.; PROKOPENKO, L.; PERSHKO, L.; VYSHNIVSKA, B.; AKIMOV, O. "Anti-corruption management mechanisms and the construction of a security landscape in the financial sector of the EU economic system against the background of challenges to european integration: Implications for artificial intelligence technologies", Economic Affairs (New Delhi), v. 68, n. 1, 2023, p. 509-521. https://doi.org/10.46852/0424-2513.1.2023.20

[79] YERMACHENKO, V.; BONDARENKO, D.; AKIMOVA, L.; KARPA, M.; AKIMOV, O.; KALASHNYK, N. "Theory and practice of public management of smart infrastructure in the conditions of the digital society' development: Socio-economic aspects", Economic Affairs (New Delhi), v. 68, n. 1, 2023, p. 617-633. https://doi.org/10.46852/0424-2513.1.2023.29

[80] MCUBA, M.; SINGH, A.; IKUESAN, R. A.; VENTER, H. "The effect of deep learning methods on deepfake audio detection for digital investigation", Procedia Computer Science, v. 219, 2023, p. 211–219. https://doi.org/10.1016/j.procs.2023.01.283

[81] KAUR, S.; KAUR, S.; RAWAT, B. "Medico-legal evidence collection in child sexual assault cases: A forensic significance", Egyptian Journal of Forensic Sciences, v. 11, n. 1, 2021, p. 41. https://doi.org/10.1186/s41935-021-00258-y

[82] NIMBKAR, P. H.; BHATT, V. D. "A review on touch DNA collection, extraction, amplification, analysis and determination of phenotype", Forensic Science International, v. 336, 2022, 111352. https://doi.org/10.1016/j.forsciint.2022.111352

protocols for the collecting, storing, and analyzing biological materials that ensure the results' reproducibility and reliability. The analysis by Khan et al.[83] in the field of forensic odontology substantiates the efficacy of employing AI techniques to enhance identification precision, while Liu et al.[84] propose an open AI framework for automating analytical procedures in forensic investigations. The application of digital technologies is gradually permeating cyberforensics: Paracha et al.[85] illustrate how AI algorithms improve the detection of network threats. In this regard, Pham and Vu[86] hold that the implementation of cyberforensic audit systems enhances transparency and reproducibility in reporting. Within the context of Ukrainian practice, these methodologies can serve as a blueprint for gradually establishing indigenous authentication procedures, although their implementation requires technical adaptation and sufficient personnel support.

Thus, the analysis reveals both alignments with global trends, in particular standardization of procedures, assessments of proportionality and transparency, validation of instruments, as well as discrepancies attributable to gaps in the Criminal Procedure Code and the absence of developed protocols for specific types of evidence. That being said, the devised algorithm can function as an adaptive instrument that progressively harmonizes national practice with international standards while preserving its procedural specificity. In contrast to approaches that either remain principle-based (admissibility and relevance standards) or tool-specific (isolated validation of particular forensic techniques), the proposed algorithm is distinctive in operationalizing reliability into a stepwise, auditable sequence of checkpoints that integrates legal thresholds, technical integrity controls, and documentation outputs within a single pre-trial workflow. Its practical implication lies in reducing the dependence of admissibility decisions on ad hoc discretion by introducing replicable "gatekeeping" decision points—proportionality, transparency, and effectiveness—through which investigators and prosecutors can consistently justify evidence acquisition, demonstrate chain-of-custody integrity (including hash-based controls where applicable), and record remedial actions when defects are identified. As a result, the algorithm is positioned not as a substitute for jurisdiction-specific rules, but as a unifying procedural template capable of strengthening predictability and evidentiary stability under conditions of digital transformation.

6. Limitations

The scope of analysis was limited to 20 decisions of the Supreme Court, a limitation that is nonetheless justified by the saturation principle, while excluding the practices of lower courts and international legal assistance. Furthermore, the statistical dimension of international practice remains fragmented, and the proposed algorithm is exclusively applicable at the pre-trial investigation stage, omitting judicial proceedings.

---

[83] KHAN, M. S.; AFRIDI, U.; AHMED, M. J.; ZEB, B.; ULLAH, I.; HASSAN, M. Z. "Comprehensive evaluation of artificial intelligence applications in forensic odontology: A systematic review and meta-analysis. ICCK Transactions on Intelligent Systematics, v. 1, n. 3, 2024, p. 176–189. https://doi.org/10.62762/TIS.2024.818917

[84] LIU, Y.-W., ZOU, D.-H., DONG, H.-W., LIU, Y.-Y., FU, E.-H., TIAN, Z.-L., LIU, N.-G. "An open-source interactive AI framework for assisting automatic literature review in forensic medicine: Focus on brain injury mechanisms", PLOS ONE, v. 20, n. 8, 2025, e0329349. https://doi.org/10.1371/journal.pone.0329349

[85] PARACHA, M. A.; JAMIL, S. U.; SHAHZAD, K.; KHAN, M. A.; RASHEED, A. "Leveraging AI for network threat detection–A conceptual overview", Electronics, v. 13, n. 23, 2024, p. 4611. https://doi.org/10.3390/electronics13234611

[86] PHAM, Q. H.; VU, K. P. "Insight into how cyber forensic accounting enhances the integrated reporting quality in small and medium enterprises", Cogent Business Management, v. 11, n. 1, 2024, 2364053. https://doi.org/10.1080/23311975.2024.2364053

7. Recommendations

It is expedient to broaden the corpus of court decisions by incorporating materials from lower courts and to deepen the international analysis by integrating quantitative data. The practical implementation of the developed algorithm for verifying the evidence reliability should be supported by training sessions for investigators and prosecutors and by methodological guidelines prepared by the Ministry of Internal Affairs and the Office of the Prosecutor General, aligned with international standards, particularly the ECHR proportionality test and ISO/IEC guidelines. Further research should test the algorithm across different evidence categories, including mixed digital–biological scenarios, and examine its applicability beyond the pre-trial stage, including judicial and appellate review.

8. Conclusions

The study elucidated that evidence reliability in criminal proceedings is determined by three interrelated criteria, namely: proportionality, transparency, and remedial effectiveness, each of which is applied as a verification checkpoint during pre-trial investigations. The analysis revealed that in Ukraine, the predominant reason for deeming evidence inadmissible is the violation of the collection protocol. However, in Germany and Poland, deficiencies in the chain of custody and non-compliance with technical requirements for hash verification prevail. A comparative study of the practices in the United States, Germany, and Poland confirmed that jurisdictions with more operationalized verification controls and documentation requirements (e.g., Federal Rules of Evidence, Bundesgerichtshof, Sąd Najwyższy) demonstrate more consistent approaches to admissibility reasoning, compared to contexts where such controls remain under-specified. This highlighted the necessity to strengthen and align procedural practices for evidence verification within Ukrainian law enforcement agencies, particularly by adopting European procedural safeguards and technical integrity controls.

The application of a three-stage verification framework has facilitated the development of a consistent algorithm for evidence evaluation, which combines legal, technical, and logical-evaluative elements of control. Its implementation is intended to enhance the reproducibility of investigative actions in Ukraine, reduce interpretive variability, and improve the quality of prosecution arguments. A practical assessment of the algorithm using the materials from 20 decisions of the Supreme Court of Ukraine (2018–2024) demonstrated that the criteria of proportionality, transparency, and efficiency are complementary, forming an integrated system for reliability assessment. The findings obtained can be leveraged to refine procedural instructions and methodological recommendations within the Ministry of Internal Affairs, the Office of the Prosecutor General, and training centers focused on the professional development of investigators and prosecutors in Ukraine. The proposed algorithm offers a methodological foundation for standardizing evidence verification practices and contributes to procedural alignment of national verification steps with international standards, in particular EPPO Guidelines, UNODC Manual on Digital Evidence, ISO/IEC 27001, and the ECHR proportionality test.

9. References

ALDAHMANI, F. K. A. M., ALMEHRZI, G. S. M. A., ALSEREIDI, E. M. S. M., ALDAHMANI, A. A. K. A., ALAHBABI, E. M. M. "Recent research study on AI-based crime scene evidence detection", In 2024 7th International Conference on Advanced Communication Technologies and Networking (CommNet) (pp. 1–6). IEEE, 2024. https://doi.org/10.1109/CommNet63022.2024.10793266

ARSLAN, Z. "Microchimerism: The mystery of multiple DNA and its implications in forensic sciences", Forensic Science International, v. 367, 2025, 112345. https://doi.org/10.1016/j.forsciint.2024.112345

ARTHANARI, A.; RAJ, S. S.; VIGNESH, R. "A narrative review in application of artificial intelligence in forensic science: Enhancing accuracy in crime scene analysis and evidence interpretation", Journal of International Oral Health, v. 17, n. 1, 2025,p. 15–22. https://doi.org/10.4103/jioh.jioh_162_24

BAMIGBADE, O.; SHEPPARD, J.; SCANLON, M. "Computer vision for multimedia geolocation in human trafficking investigation: A systematic literature review", arXiv:2402.15448, 2024. https://doi.org/10.48550/arXiv.2402.15448

BANSODE, S.; MORAJKAR, A.; RAGADE, V.; MORE, V.; KHARAT, K. "Challenges and considerations in forensic entomology: A comprehensive review", Journal of Forensic and Legal Medicine, v. 110, 2025, 102831. https://doi.org/10.1016/j.jflm.2025.102831

BHOYAR, L.; SRIVASTAVA, B. "Revolutionizing forensic investigations through AI-driven pollen analysis: A narrative review", Review of Palaeobotany and Palynology, v. 344, 2025, 105440. https://doi.org/10.1016/j.revpalbo.2025.105440

BIRD, C.; JONES, K.; BALLANTYNE, K. "Cognitive bias and contextual information management: Considerations for forensic handwriting examinations", Wiley Interdisciplinary Reviews: Forensic Science, v. 6, n. 4, 2024, e1530. https://doi.org/10.1002/wfs2.1530

BRUNTY, J. "Validation of forensic tools and methods: A primer for the digital forensics examiner", WIREs Forensic Science, v. 4, n. 1, 2022, e1474. https://doi.org/10.1002/wfs2.1474

Bundesgerichtshof. EncroChat-Data may be used for the Investigation of serious criminal Offences. 2022. Karlsruhe: Federal Court of Justice of Germany, 2022. https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/EN/2022/2022038.html (accessed on 13 August 2025).

CAO, Z.; GAO, B.; LIU, Z.; XIONG, X.; WANG, B.; PEI, C. "Data trace as the scientific foundation for trusted metrological data: A review for future metrology direction", PeerJ Computer Science, v. 11, 2025, e3106. https://doi.org/10.7717/peerj-cs.3106

CERMAK, M.; FRITZOVÁ, T.; RUSŇÁK, V.; SRAMKOVA, D. "Using relational graphs for exploratory analysis of network traffic data", Forensic Science International: Digital Investigation, v. 45, n. (Supplement), 2023, 301563. https://doi.org/10.1016/j.fsidi.2023.301563

Council of Europe. Electronic Evidence Guide v.3.0: Guidelines on the treatment of electronic evidence in criminal proceedings. Strasbourg: Council of Europe, 2022. Available at: https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/s3fs-public/2025-06/guidelines-trtmnt-elctrnc.pdf (accessed on 13 August 2025).

Council of Europe. The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols, 2001. Available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention (accessed on 13 August 2025).

Criminal Code of Ukraine (No. 2341-III, enacted April 5, 2001; current version as of July 17, 2025). Verkhovna Rada of Ukraine. Available at: https://zakon.rada.gov.ua/go/2341-14 (accessed on 13 August 2025).

CROWN, N.; MARQUIS, R.; KUPFERSCHMID, E.; DZIEDZIC, T.; BELIC, D.; KERZAN, D. "Error mitigation in forensic handwriting examination: The examiner's perspective", Forensic Sciences Research, v. 9, n. 4, 2024, owae065. https://doi.org/10.1093/fsr/owae065

European Public Prosecutor's Office (EPPO). Operational Guidelines on Investigation, Evocation Policy and Referral of Cases (College Decision 029/2021, as amended), 2022. https://www.eppo.europa.eu/sites/default/files/2022-02/EPPO_Operational_Guidelines_College_Decision_029.2021_as%20amended_by_College%20decision_007.2022.pdf

Federal Rules of Evidence. Federal rules of evidence as amended to December 1, 2023 (Committee Print No. 6), 2023. Available at: https://www.uscourts.gov/sites/default/files/evidence_federal_rules_pamphlet_dec_1_2023.pdf (accessed on 13 August 2025).

FRAGKOU, K.; KETSEKIOULAFIS, I.; TOUSIA, A.; PIAGKOU, M.; BACOPOULOU, F.; FERENTINOS, P.; PEYRON, P.-A., BACCINO, E.; MARTRILLE, L.; PAPADODIMA, S. "From fragile lives to forensic truth: Multimodal forensic approaches to pediatric homicide and suspect death", Diagnostics, v. 15, n. 11, 2025, p. 1383. https://doi.org/10.3390/diagnostics15111383

ISO/IEC 27001:2022. Information technology__Security techniques__Guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva: International Organization for Standardization, 2022. Available at: https://www.iso.org/standard/44381.html (accessed on 13 August 2025).

KAUR, S.; KAUR, S.; RAWAT, B. "Medico-legal evidence collection in child sexual assault cases: A forensic significance", Egyptian Journal of Forensic Sciences, v. 11, n. 1, 2021, p. 41. https://doi.org/10.1186/s41935-021-00258-y

KAZAURE, A. A.; JANTAN, A.; YUSOFF, M. N. "Digital forensics investigation approaches in mitigating cybercrimes: A review", Journal of Information Science Theory and Practice, v. 11, n. 4, 2023, p. 14–27. https://doi.org/10.1633/JISTaP.2023.11.4.2

KHAN, M. S.; AFRIDI, U.; AHMED, M. J.; ZEB, B.; ULLAH, I.; HASSAN, M. Z. "Comprehensive evaluation of artificial intelligence applications in forensic odontology: A systematic review and meta-analysis. ICCK Transactions on Intelligent Systematics, v. 1, n. 3, 2024, p. 176–189. https://doi.org/10.62762/TIS.2024.818917

KRETZ, I. D.; PARRAN, C. C.; RAMSDELL, J. D.; ROWE, P. D. "Evidence tampering and chain of custody in layered attestations", arXiv:2402.00203, 2024. https://doi.org/10.48550/arXiv.2402.00203

KUDEIKINA, I. "Port as evidence in the civil proceedings of Latvia", Archives of Criminology and Forensic Sciences, v. 1, 2020, p. 73-79. https://doi.org/10.32353/acfs.1.2020.05

KUSSAINOV, K.; GONCHARUK, N.; PROKOPENKO, L.; PERSHKO, L.; VYSHNIVSKA, B.; AKIMOV, O. "Anti-corruption management mechanisms and the construction of a security landscape in the financial sector of the EU economic system against the background of challenges to european integration: Implications for artificial intelligence technologies", Economic Affairs (New Delhi), v. 68, n. 1, 2023, p. 509-521. https://doi.org/10.46852/0424-2513.1.2023.20

Law of Ukraine "Criminal Procedural Code of Ukraine"(No. 4651-VI, adopted April 13, 2012; current version as of August 1, 2025, based on Law No. 4560-IX). Verkhovna Rada of Ukraine. Available at: https://zakon.rada.gov.ua/go/4651-17 (accessed on 13 August 2025).

Law of Ukraine "On Electronic Identification and Electronic Trust Services" (No. 2155-VIII, adopted October 5, 2017; current version as of December 18, 2024). Verkhovna Rada of Ukraine. Available at: https://zakon.rada.gov.ua/go/2155-19 (accessed on 13 August 2025).

Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine" (No. 2163-VIII, adopted October 5, 2017; current version as of June 28, 2024). Verkhovna Rada of Ukraine. Available at: https://zakon.rada.gov.ua/laws/show/2163-19 (accessed on 13 August 2025).

LIU, Y.-W., ZOU, D.-H., DONG, H.-W., LIU, Y.-Y., FU, E.-H., TIAN, Z.-L., LIU, N.-G. "An open-source interactive AI framework for assisting automatic literature review in forensic medicine: Focus on brain injury mechanisms", PLOS ONE, v. 20, n. 8, 2025, e0329349. https://doi.org/10.1371/journal.pone.0329349

LOOVENS, J.; TINMAZ, H. "A systematic literature review of deepfakes in forensic science", Forensic Imaging, v. 43, 2025, 200647. https://doi.org/10.1016/j.fri.2025.200647

LYTVYN, N.; ANDRUSHCHENKO, H.; ZOZULYA, Y. V.; NIKANOROVA, O. V.; RUSAL, L. M. "Enforcement of Court Decisions as a Social Guarantee of Protection of Citizens Rights and Freedoms", Prawo i Więź, v. 39, 2022, p. 80–102. https://doi.org/10.36128/priw.vi39.351

MAKARENKOV, O.; KOSA, V. "Forensic Technique for Identifying Corruption Challenges to National Security through Digital Technologies", Baltic Journal of Economic Studies, v. 10, n. 4, 2024, p. 288–300. https://doi.org/10.30525/2256-0742/2024-10-4-288-300

MCUBA, M.; SINGH, A.; IKUESAN, R. A.; VENTER, H. "The effect of deep learning methods on deepfake audio detection for digital investigation", Procedia Computer Science, v. 219, 2023, p. 211–219. https://doi.org/10.1016/j.procs.2023.01.283

NATH, S.; SUMMERS, K.; BAEK, J.; AHN, G.-J. "Digital evidence chain of custody: Navigating new realities of digital forensics", In Proceedings of the 2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA) (p. 11–20). Institute of Electrical and Electronics Engineers, 2024. https://doi.org/10.1109/TPS-ISA62245.2024.00012

NIMBKAR, P. H.; BHATT, V. D. "A review on touch DNA collection, extraction, amplification, analysis and determination of phenotype", Forensic Science International, v. 336, 2022, 111352. https://doi.org/10.1016/j.forsciint.2022.111352

Office of the Prosecutor General of Ukraine. Order No. 298 on the approval of the Regulations on the Unified Register of Pre-trial Investigations: procedure for its formation and maintenance, 2020, June 30 (current version as of September 16, 2025). Available at: https://zakon.rada.gov.ua/laws/show/v0298905-20 (accessed on 13 August 2025).

Office of the Prosecutor General of Ukraine. Order No. 409 on the procedure for preparing, submitting, and processing special reports on criminal offenses and socially resonant events, 2020, September 3. Available at: https://wd.clarity-project.info/resource/73111d11-6184-4162-8740-6f69b8f294d7 (accessed on 13 August 2025).

OSCE. Ensuring Human Rights Compliance in Cybercrime Investigations, 2023. Available at: https://www.osce.org/files/f/documents/e/3/554901.pdf (accessed on 13 August 2025).

PALEKAR, V.; KUMAR, S. L. "An effective image annotation using self-attention based stacked bidirectional capsule network", Computer Standards Interfaces, v. 93, 2025,103973. https://doi.org/10.1016/j.csi.2025.103973

PALKOVA, K.; AGAPOVA, O.; ZĪLE, A.; POLIANSKYI, A.; VADYM, K.; HASPARIAN, S.; MYKHAILO, M. "Sustainability of open educational resources in Forensic Sciences: international experience", European Journal of Sustainable Development, v. 11, n. 3, 2022, p. 71. https://doi.org/10.14207/ejsd.2022.v11n3p71

PARACHA, M. A.; JAMIL, S. U.; SHAHZAD, K.; KHAN, M. A.; RASHEED, A. "Leveraging AI for network threat detection–A conceptual overview", Electronics, v. 13, n. 23, 2024, p. 4611. https://doi.org/10.3390/electronics13234611

PHAM, Q. H.; VU, K. P. "Insight into how cyber forensic accounting enhances the integrated reporting quality in small and medium enterprises", Cogent Business Management, v. 11, n. 1, 2024, 2364053. https://doi.org/10.1080/23311975.2024.2364053

QIAN, H.; XIA, L.; GE, R.; FAN, Y.; WANG, Q.; JING, Z. "From black boxes to glass boxes: Explainable AI for trustworthy deepfake forensics", Cryptography, v. 9, n. 4, 2025, p. 61. https://doi.org/10.3390/cryptography9040061

Sąd Najwyższy. Wyrok z dnia 13 maja 2021 r., sygn. V CSKP 41/21. Warszawa: Sąd Najwyższy, 2021. Available at: https://www.inforlex.pl/dok/tresc%2CFOB00000000000005398370%2CWyrok-SN-z-dnia-13-maja-2021-r-sygn-V-CSKP-41-21.html (accessed on 13 August 2025).

Unified State Register of Court Decisions. State Judicial Administration of Ukraine, 2025. Available at: https://reyestr.court.gov.ua (accessed on 13 August 2025).

United Nations. Guide for First Responders on the Collection of Digital Devices in the Battlefield. New York: United Nations, 2024. Available at: https://www.un.org/counterterrorism/sites/default/files/guide-first_responders-digital_devices_in_battlefield.pdf?utm_source=chatgpt.com (accessed on 13 August 2025).

YERMACHENKO, V.; BONDARENKO, D.; AKIMOVA, L.; KARPA, M.; AKIMOV, O.; KALASHNYK, N. "Theory and practice of public management of smart infrastructure in the conditions of the digital society' development: Socio-economic aspects", Economic Affairs (New Delhi), v. 68, n. 1, 2023, p. 617-633. https://doi.org/10.46852/0424-2513.1.2023.29

ZĪLE, A.; VILKS, A.; POLIANSKYI, A. "Digital forensics and criminal policy: Latvian–Ukrainian perspective", Socrates, v. 24, n. 3, 2022, p. 140–149. https://doi.org/10.25143/socr.24.2022.3.140-149