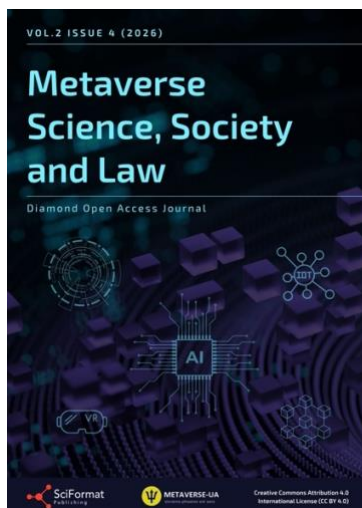




Metaverse Science, Society and Law

Vol. 2, Issue 4 (2026)



Publisher:
SciFormat Publishing Inc.

ISNI: 0000 0005 1449 8214
2734 17 Avenue Southwest, Calgary,
Alberta, Canada, T3E0A7

+15878858911
✉ editorial-office@sciformat.ca

ARTICLE TITLE	THE USE OF ARTIFICIAL INTELLIGENCE IN FORENSIC SCIENCE: CHALLENGES AND PROSPECTS
----------------------	---

DOI	https://doi.org/10.69635/mssl.2026.2.4.68
------------	---

RECEIVED	08 July 2026
-----------------	--------------

ACCEPTED	08 October 2026
-----------------	-----------------

PUBLISHED	16 October 2026
------------------	-----------------

LICENSE	
----------------	---

The article is licensed under a **Creative Commons Attribution 4.0 International License**.

© The author(s) 2026.

This article is published as open access under the Creative Commons Attribution 4.0 International License (CC BY 4.0), allowing the author to retain copyright. The CC BY 4.0 License permits the content to be copied, adapted, displayed, distributed, republished, or reused for any purpose, including adaptation and commercial use, as long as proper attribution is provided.

THE USE OF ARTIFICIAL INTELLIGENCE IN FORENSIC SCIENCE: CHALLENGES AND PROSPECTS

Anatolii Lazebnyi

Candidate of Legal Sciences, Associate Professor, Department of Criminal Law and Procedure, Educational and Research Institute of Law, State Tax University, Ukraine

ORCID ID: 0000-0001-9812-6151

Bogdan Krymchanin

Fourth-year Student, State Tax University, Ukraine

ORCID ID: 0009-0003-4339-6658

ABSTRACT

This article examines the opportunities and challenges associated with the use of artificial intelligence (AI) in forensic science at the stages of collecting, examining, and evaluating evidentiary information. It considers the use of machine-learning algorithms, computer vision, and language models to process digital datasets, analyse photographs and video recordings, conduct biometric comparisons, examine documents, and detect synthetically generated content. AI can accelerate information retrieval and help identify relationships between data; however, technological efficiency does not guarantee the reliability of the result. The article analyses the risks of algorithmic bias, limited explainability, errors in training data, loss of digital context, breaches in the chain of custody, and excessive reliance on automated conclusions. In light of Ukrainian legislation and European approaches, it proposes a multi-level model for verifying neural-network outputs. The model includes documenting the tool, preserving original data, independent validation, describing methodological limitations, and ensuring that the parties to proceedings have a genuine opportunity to challenge the result. The article argues that AI should remain an auxiliary tool, while final forensic conclusions and procedural decisions must be made by competent human professionals in accordance with the law.

KEYWORDS

Artificial Intelligence, Forensic Science, Digital Evidence, Forensic Examination, Admissibility of Evidence, Algorithmic Bias, Reliability

CITATION

Anatolii Lazebnyi, Bogdan Krymchanin. (2026) The Use of Artificial Intelligence in Forensic Science: Challenges and Prospects. *Metaverse Science, Society and Law*. Vol. 2, Issue 4. doi: 10.69635/mssl.2026.2.4.68

COPYRIGHT

© The author(s) 2026. This article is published as open access under the **Creative Commons Attribution 4.0 International License (CC BY 4.0)**, allowing the author to retain copyright. The CC BY 4.0 License permits the content to be copied, adapted, displayed, distributed, republished, or reused for any purpose, including adaptation and commercial use, as long as proper attribution is provided.

Introduction

The digitalisation of society is changing both the ways in which criminal offences are committed and the methods used to investigate them. Information relevant to criminal proceedings increasingly exists in the form of electronic messages, metadata, camera recordings, digital images, audio files, mobile-device data, and network activity. The volume of such data may exceed the capacity for manual processing; consequently, artificial intelligence (hereinafter AI) algorithms are becoming important tools for searching, classification, and preliminary analysis.

The relevance of this topic stems from the dual impact of technological development. On the one hand, machine learning makes it possible to process large volumes of information more quickly and identify patterns that may be difficult to detect through manual analysis. On the other hand, generative systems can create realistic but false images, videos, voice messages, and texts. Systematic reviews of AI applications in forensic science demonstrate a broad range of potential uses while emphasising the need for human oversight and verification of results.

The issue is not merely whether AI can be useful, but under what conditions its use is scientifically justified, procedurally proper, and compatible with the guarantees of a fair trial. The Criminal Procedure Code of Ukraine defines evidence in terms of factual data obtained in accordance with the procedure established by law and specifies the permissible procedural sources of evidence [1]. Accordingly, an algorithmic output cannot automatically be regarded as evidence merely because it is digital in origin.

The aim of this article is to examine the potential applications of AI in forensic science and identify the legal, methodological, and organisational conditions required to ensure the reliability and admissibility of its outputs. The article's scientific novelty lies in substantiating a multi-level model for verifying algorithmic outputs that combines technical validation, procedural traceability, professional assessment, and the possibility of effective challenge.

The use of artificial intelligence in forensic science requires further comprehensive scholarly analysis in Ukraine, particularly with regard to the detection, collection, examination, and evaluation of evidentiary information; the reliability of digital traces; the identification of signs of manipulation of electronic data; and the proper verification of automated analytical results. At the same time, certain aspects of forensic technology, digital forensics, the use of information technology in criminal investigations, and the application of specialised knowledge have been examined in the works of scholars including O. M. Bodunova, A. V. Borovyk, O. H. Kolb, I. M. Kopotun, O. V. Kostenko, V. P. Liubavina, O. M. Lytvynov, N. A. Luhina, A. M. Lazebnyi, and others. Further research is nevertheless needed into the forensic capabilities of AI, the limits of its use in handling digital evidence, methods for verifying the authenticity of digital objects, and the development of scientifically grounded recommendations to ensure the reliability, reproducibility, and procedural verifiability of results produced by these technologies.

Part 1. Opportunities for Using Artificial Intelligence in the Collection, Examination, and Processing of Evidentiary Information

AI should be understood as a set of methods for recognition, classification, prediction, searching, and pattern detection. These include machine-learning algorithms, neural networks, computer vision, natural language processing, and automated multimedia-analysis tools. Their functionality depends on the task, the quality of the input materials, the characteristics of the training dataset, and the conditions of use. It is therefore unjustified to place the same level of trust in different systems.

The first area involves the preliminary processing of digital information. When examining electronic devices or copies of storage media, investigators and specialists may encounter thousands of documents, images, messages, and event logs. Algorithms can group files by type, time, subject matter, or similarity, identify duplicates, and help prioritise materials for further examination. This does not replace the procedural seizure or examination of evidence, but it can make the handling of data already obtained lawfully more efficient.

Nevertheless, the result of automated classification is only an investigative lead. For example, assigning a message to a particular thematic category does not establish its significance without considering context, irony, professional jargon, or linguistic characteristics. Algorithmic conclusions must therefore be checked against the original sources and must not be incorporated into procedural documents as established facts without further analysis.

The second area concerns the examination of photographs and video recordings. Computer vision can assist in detecting objects, tracking movement within a recording, comparing image segments, and identifying possible signs of editing. This may be useful when analysing surveillance footage, open-source materials, or video obtained from digital devices. However, image enhancement is not equivalent to the recovery of reliable information: some systems reconstruct details that are not present in the original file.

The original should therefore be preserved, derivative copies should be recorded separately, and all operations should be documented. Where sharpening, noise reduction, or fragment reconstruction has been applied, the expert must distinguish the original data from elements generated through computational processing. Otherwise, a visually convincing result may be mistakenly perceived as an accurate representation of the original scene.

The third area is biometric comparison of faces and voices. Algorithms can rank similar images or voice samples, identify distinctive features, and assist in searching for potential matches. Research on the evaluation of AI in forensic science recommends considering technical, scientific, and professional-societal indicators of reliability rather than merely noting that an algorithm was used [2]. It is important to establish whether the system has been validated for the specific task and for materials of the relevant quality.

Recording quality, lighting, camera angle, video compression, background noise, the speaker's emotional state, and other factors may affect the result. A high accuracy rate on a test dataset does not guarantee the same level of accuracy for a particular recording. The result of biometric comparison should therefore be treated as auxiliary information, accompanied by a clear description of its limitations, rather than as conclusive identification.

The fourth area concerns the examination of documents, handwriting, and signatures. Neural networks can assist in classifying documents, identifying text regions, comparing images, and detecting possible alterations. Ukrainian researchers have noted the promise of AI for handwriting and technical-forensic examinations, while emphasising that it should be used as one stage of comparative analysis rather than as a substitute for an expert [3].

Handwriting and signatures exhibit individual yet variable characteristics. Automated comparison may identify relevant areas, but a specialist must assess the conditions under which the writing was produced, the quality of the copy, the possibility of imitation, and natural handwriting variation. Conclusions should be based on a method suitable for the specific object, not solely on a numerical similarity score.

The fifth area involves detecting synthetically generated or altered media. Deepfake-detection tools analyse image artefacts, temporal inconsistencies, audio-signal characteristics, and other indicators. NIST research emphasises the need to test the robustness of such tools against new generation methods, compression, and further processing [4]. A negative detection result does not prove that a file is authentic, while a positive result does not, by itself, establish who created it or the circumstances of its creation.

The sixth area involves analysing large datasets and identifying relationships between events. AI can detect recurring identifiers, temporal overlaps, shared contacts, or similar methods of operation. Such analysis can help generate investigative hypotheses, but correlation does not establish causation. A shared digital marker does not necessarily indicate a common user or coordinated conduct; identified patterns must therefore be corroborated by other evidence.

Large language models constitute a separate category of tools. They can help structure materials, formulate search queries, and summarise large volumes of text. However, they may generate non-existent references, inaccurately summarise documents, or conflate facts with assumptions. They are best used for auxiliary navigation, with legally significant assertions checked against primary sources. Transferring materials to external services requires a separate assessment of the legal basis and security implications.

In criminal proceedings, it is necessary to distinguish the original object, the result of technical processing, and a conclusion formally documented in accordance with procedural requirements. The Criminal Procedure Code of Ukraine identifies testimony, physical evidence, documents, and expert opinions as procedural sources of evidence [1]. A file containing an algorithmic output therefore does not, in itself, constitute a new procedural source of evidence not recognised by law. The Law of Ukraine "On Forensic Examination" defines forensic examination as research based on specialised knowledge for the purpose of providing an opinion [5]. Software may form part of such research, but it does not remove the requirements concerning the expert's competence and responsibility.

The use of AI must also be considered in relation to privacy protection. Biometric comparison and large-scale analysis of communications may significantly affect human rights. Personal data protection legislation

requires the amount of data processed to correspond to the specified purpose and prohibits excessive collection [6]. The technical ability to analyse data does not, in itself, provide a lawful basis for doing so.

The European Union Artificial Intelligence Act establishes a risk-based approach and specific rules for certain areas of law enforcement and biometrics [7]. The Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law calls on states to uphold transparency, accountability, privacy protection, reliability, and appropriate safeguards [8]. These instruments provide important guidance for the further development of Ukraine's methodological and regulatory approaches.

Part 2. Challenges in Ensuring the Reliability and Admissibility of AI Outputs in Forensic Science

The principal difficulty in using AI is that an algorithmic output may appear accurate and objective even though it depends on the limitations of the model, the data, and the conditions of use. Automation does not eliminate human error and may sometimes conceal it behind a complex technical process. In forensic practice, this may affect the selection of an investigative hypothesis, the assessment of testimony, or the preparation of an expert opinion.

First, there is the problem of limited explainability. Some deep-learning systems produce outputs through complex internal parameters that are difficult to translate into understandable features. If a specialist cannot explain which data influenced the result, which alternatives were considered, and under what conditions the system may fail, there is a risk of uncritical reliance on the technology. Research on AI evaluation in forensic science stresses that explainability must be accompanied by technical validation, scientific justification, and professional review [2]. Second, the quality and representativeness of training data are crucial. If the data do not reflect real-world conditions of use, the algorithm may perform less effectively for certain groups of people, languages, accents, devices, or recording types. An overall accuracy score may conceal differing false-positive and false-negative rates. It is therefore necessary to assess not only overall accuracy but also known limitations, testing conditions, and error rates.

Another challenge is the difference between laboratory conditions and real-world practice. A model tested on high-quality photographs may be unreliable when applied to blurred frames; a voice-recognition system may perform poorly on noisy recordings; and a deepfake detector may be less reliable after transcoding. A review of AI and computer-vision applications in forensic science highlights the promise of these technologies but also notes the limitations of some datasets and the lack of sufficient testing under real-world conditions [9]. The suitability of a system for the specific object and task must therefore be established.

A further concern is the modification of algorithms or software environments. An online service may update its model without any obvious change to the interface, meaning that repeating an analysis at a later date may produce a different result. To ensure reproducibility, the tool's name, model version, date of use, settings, input data, preprocessing operations, and complete output should be recorded. A provider's trade-secret claims should not automatically remove the need for adequate reliability testing.

Even an accurate algorithm cannot ensure reliability if the original file has been altered, incompletely copied, or incorrectly identified. The source, time of acquisition, person who made the copy, tools used, file hash values, and subsequent transformations should be recorded. The AI output must be linked to the specific version of the input object, rather than merely to its filename.

The risk of confirmation bias must also be considered. If an investigator or expert already favours a particular hypothesis, the algorithm's output may be interpreted selectively: matches may be treated as confirmation, while inconsistencies are dismissed as insignificant. Bias may arise from the wording of a query, the selection of materials, or the choice of a threshold value. To reduce this risk, tasks should be framed neutrally, alternative hypotheses documented, and independent verification conducted wherever possible.

The reliability of outputs generated by generative models is another important issue. Such models may produce persuasive but fabricated explanations, misquote documents, conflate sources, or respond confidently despite insufficient information. A language model's output should therefore not be treated as an independent source of established facts. Every legally significant assertion must be checked against the original source, while automated assessments of media files should be supplemented by examination of their provenance, metadata, and content.

The admissibility of evidence requires particular attention. Articles 84–86 of the Criminal Procedure Code of Ukraine link evidentiary significance to the lawful acquisition of factual data, relevance, and admissibility; Article 94 also requires the reliability of evidence and its interrelationship with other evidence

to be assessed [1]. There is therefore no basis for treating all AI outputs as automatically admissible or automatically inadmissible. The assessment depends on the type of material, how the input data were obtained, compliance with procedure, the reliability of the method, and the possibility of verification.

It is also important to distinguish admissibility from reliability. Material may have been obtained in procedural compliance with the law yet remain unreliable because of a weak method or poor-quality data. Conversely, a technically persuasive result does not remedy human-rights violations in obtaining the underlying information. A software report cannot, therefore, replace a comprehensive legal assessment.

The defence must also be guaranteed a genuine opportunity to challenge AI-generated results. Where a conclusion depends substantially on an algorithm, the parties should be able to examine the methodology, question the expert, review the input data, and identify the system's limitations. Research on the right to procedural accuracy in digital evidence highlights the importance of access to the data-processing chain, explanations of results, and the parties' participation in the key stages of their formation [10]. Technical complexity must not reduce evidentiary review to a mere formality.

The use of AI technologies must also be accompanied by appropriate protection of personal data and confidential information. Transferring materials to an external service may create risks of disclosing information about victims or witnesses, or information relating to a pre-trial investigation. Before using such a service, it is necessary to establish the legal basis for processing and assess the location of data storage, access permissions, deletion periods, and the possibility of reusing the data. The volume of material transferred must be necessary for the lawful purpose [6].

Finally, the limits of responsibility of those involved in using AI must be defined. An algorithmic error cannot simply be attributed to the software itself. It is necessary to determine who selected the tool, whether it was suitable for the task, who verified the output, and whether it was used beyond its intended purpose. An expert is responsible for their own opinion, while an official is responsible for procedural decisions made within the scope of their authority. Automation must not create a "zone of irresponsibility."

In 2025, a responsible framework for the use of AI in forensic science was proposed, focusing on the practical implementation of principles through evaluation, guidance, and project registration [11]. For Ukraine, a similar approach would be promising: before introducing a tool, its purpose, risks, success criteria, testing procedure, known limitations, and responsible persons should be identified.

We propose a multi-level model for verifying AI outputs. The first level is technical: confirming data integrity and recording the system version and parameters. The second is scientific and methodological: verifying the validity of the method, known error rates, and limits of applicability. The third is professional: critical assessment by a competent expert and comparison with independent data. The fourth is procedural: ensuring that the parties can examine the result, ask questions, and submit an alternative examination [12].

In practice, this model could be implemented through a standardised AI-use protocol specifying the purpose of use, the legal basis for processing the data, a description of the input material, the system's name and version, processing parameters, the output, known limitations, the method of independent verification, and details of the responsible specialist. The protocol would not replace the procedural form prescribed by law, but would ensure traceability of the technological stage [12].

Documentation requirements should be proportionate to risk. File sorting has a different level of impact from automated biometric comparison, the result of which may affect a person's identification. The more significantly an algorithmic conclusion affects human rights, the more stringent the requirements should be for independent validation, explanation, and challenge. European approaches support risk-based regulation and human oversight [8].

It would be appropriate to establish a system for the independent testing of forensic AI tools. This system should include standardised test datasets, publication of evaluation methodologies, retesting after substantial updates, and a register of tools recommended for specific tasks. Registration must not, however, create a presumption of infallibility: even a validated system must be assessed for its suitability to the particular case.

Training investigators, prosecutors, judges, specialists, and forensic experts is equally important. Digital literacy should include an understanding of false-positive results, the impact of data quality, the distinction between correlation and causation, and methods for verifying digital integrity. The aim is not to turn every legal professional into a developer, but to enable them to ask the right questions and critically assess results.

Conclusions

AI creates new opportunities for forensic science, including the preliminary processing of large digital datasets, analysis of photographs and video recordings, biometric comparison, document examination, detection of synthetic content, and identification of relationships between data. The most defensible approach is to use AI as an auxiliary tool that accelerates professionals' work without replacing independent verification or formal procedural documentation.

The principal risks remain limited explainability, unrepresentative training data, changes in software environments, poor-quality original files, algorithmic bias, and generative errors. Reliability cannot be inferred solely from technological complexity or a system's claimed accuracy.

An AI output does not automatically constitute a separate procedural source of evidence. Its significance is determined by criminal procedure law, the nature of the material, the method of data acquisition, relevance, admissibility, reliability, and its relationship to other evidence. The use of AI in an expert examination does not remove the expert's personal responsibility for their opinion.

The article's scientific novelty lies in substantiating a multi-level model for verifying AI outputs, covering technical integrity, scientific and methodological validity, professional assessment, and procedural verifiability. Practical implementation requires documenting the tool version, preserving original data, recording transformations, conducting independent testing, describing limitations, and ensuring the possibility of an effective challenge.

Further improvement of Ukraine's regulatory framework should involve developing methodological requirements for the use of AI in forensic examinations, introducing a risk-based approach, independently testing tools, and enhancing the digital competence of participants in proceedings. The principal criterion for adopting a technology should be its ability to improve the quality of evidence-based decision-making without weakening human-rights safeguards or the guarantees of a fair trial.

REFERENCES

1. Criminal Procedure Code of Ukraine, Law No. 4651-VI (April 13, 2012, as amended July 21, 2026). <https://zakon.rada.gov.ua/laws/show/4651-17#Text>
2. Durán, J. M., van der Vloed, D., Ruifrok, A., & Ypma, R. J. F. (2024). From understanding to justifying: Computational reliabilism for AI-based forensic evidence evaluation. *Forensic Science International: Synergy*, 9, Article 100554. <https://doi.org/10.1016/j.fs SYN.2024.100554>
3. Nikolaichuk, T., & Solomakha, Y. (2024). On the use of artificial intelligence capabilities in forensic examination. *Criminalistics and Forensic Examination*, 69, 356–364. <https://doi.org/10.33994/kndise.2024.69.34>
4. Guan, H., Horan, J., & Zhang, A. (2025, January 27). Guardians of forensic evidence: Evaluating analytic systems against AI-generated deepfakes [Conference paper]. *Forensics@NIST 2024*. National Institute of Standards and Technology. <https://www.nist.gov/publications/guardians-forensic-evidence-evaluating-analytic-systems-against-ai-generated-deepfakes>
5. On Forensic Examination, Law of Ukraine No. 4038-XII (February 25, 1994, as amended January 1, 2026). <https://zakon.rada.gov.ua/laws/show/4038-12#Text>
6. On Personal Data Protection, Law of Ukraine No. 2297-VI (June 1, 2010, as amended June 14, 2025). <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
7. European Parliament & Council of the European Union. (2024). 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. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>
8. Council of Europe. (2024). Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225). <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence>
9. Morán-Torres, R., Feld, K., Hesser, J., Taalab, Y. M., & Yen, K. (2025). Artificial intelligence and computer vision in forensic sciences: Applications in traumatic injury analysis. *Rechtsmedizin*, 35, 219–225. <https://doi.org/10.1007/s00194-025-00775-3>
10. Stoykova, R. (2024). A new right to procedural accuracy: A governance model for digital evidence in criminal proceedings. *Computer Law & Security Review*, 55, Article 106040. <https://doi.org/10.1016/j.clsr.2024.106040>
11. Stacey, J., Fleming, R., Sheppard, D., Sheppard, J., Dobbie, G., & Karunakaran, D. (2025). A responsible artificial intelligence framework for forensic science. *Forensic Science International*, 375, Article 112548. <https://doi.org/10.1016/j.forsciint.2025.112548>
12. Kostenko, O., Zhuravlov, D., Dniprov, O., & Korotiuk, O. (2023). Metaverse: Model criminal code. *Baltic Journal of Economic Studies*, 9(4), 134–147. <https://doi.org/10.30525/2256-0742/2023-9-4-134-147>