CHALLENGES AND PERSPECTIVES OF THE DIGITAL TRACE IN THE ERA OF ARTIFICIAL INTELLIGENCE AND DEEPFAKE TECHNOLOGIES

Jana Zachar Kuchtová[1], **PhD**
Jozef Meteňko, PhD
Department of Criminalistics and Forensic Sciences, Academy of the Police Force in Bratislava, Slovakia

ABSTRACT

Purpose: The paper examines how artificial intelligence, particularly deepfake technologies, influences the meaning and usability of the digital trace in criminalistics. The aim is to identify the main challenges in securing and evaluating digital evidence and to outline perspectives for its further application in criminal proceedings.

Design/Methods/Approach: The study applies an analytical approach that combines a review of current technological trends with an examination of criminalistic methods used for detecting and interpreting digital traces. It is based on available scholarly sources and international reports that reflect ongoing debates on the credibility of digital evidence.

Findings: Artificial intelligence complicates the identification and reliability of traditional digital traces, while at the same time generating new types of traceable artifacts that can be used in criminalistics. Deepfakes illustrate the risks of manipulating multimedia evidence, but also emphasise the need for developing new methods of detection and evaluation.

Originality/Value: The paper offers a multidisciplinary perspective on the digital trace in the age of artificial intelligence. By linking technological, criminalistics, and legal aspects, it underlines the necessity of methodological and legislative adaptation in order to preserve the credibility of digital evidence in criminal proceedings.

Keywords: digital trace; criminalistics; deepfake; digital evidence; provenance; C2PA; AI Act.

About the authors:

Capt. JUDr. **Jana Zachar Kuchtová**, PhD, is an Assistant at the Department of Criminalistics and Forensic Sciences at the Academy of the Police Force in Bratislava. Her research interests focus on informatics, digital traces, and the application of new technologies in criminalistics. She has authored and co-authored several scholarly publications and actively participates in projects related to the modernisation of selected criminalistics methods.

Prof. JUDr. **Jozef Meteňko**, PhD, has been a Head of the Department of Criminalistics and Forensic Sciences at the Academy of the Police Force in Bratislava more as 20 years. He has addressed his research projects in the fields: Theory of police science, Methods of work at the crime scene, criminalistics documentation, criminalistics photography, Development of criminalistics – tactical methods, Security at major events, Prevention police activities in youth crime, and others. These were mainly

1 jana.kuchtova@minv.sk

international projects. He co-authored seven academic text-books, including two foreign, he wrote 9 monographs, several university textbooks and over 600 scientific and special studies at home and abroad, mainly in the course of research activities. He has had 20 students for postgraduate PhD study, more than 100 diploma theses and a large number of other qualifications and final works. E-mail: jozef.metenko@minv.sk

INTRODUCTION

The circumstances in which traces appear, persist, and are examined in criminalistics are radically altered by the digitisation of every aspect of social life. Digital traces are an extension of pre-existing methods of information recording and transmission within technical systems, and are not a novel phenomenon. Digital traces have an electromagnetic or electronic material substrate that grounds them in the physical world, despite the fact that their form is technologically mediated rather than physically tangible. Their ontological character is evolving; they may now come from autonomous or generative systems in addition to human activity. Therefore, informational, technological, and interpretive qualities determine their criminalistic value.

According to this concept, a digital trace is a particular kind of criminalistics trace - the field trace, which is a specific information carrier that results from automated or human activity and that emerges, evolves, and partly vanishes within the digital environment. Its capacity to mediate the relationship between an object with act production, and its consequences - trace, that is, to make it possible to be an information carrier for reconstructing an event, identifying subjects, and confirming the veracity of data obtained - gives it criminalistics value. (Metenko & Metenkova, 2024; Metenko, 2004)

The authenticity and recognition of digital traces are called into question by generative AI and deepfake systems, which can create artificial content that is nearly identical to the real thing. These necessitates redefine techniques for protecting and evaluating digital evidence, as well as establish new standards for evidentiary value and manipulation detection. The digital trace is frequently a potentially artificial interpretation rather than a reflection of reality.

THEORETICAL FRAMEWORK OF THE DIGITAL TRACE IN CRIMINALISTICS

The criminalistic trace is an objectively existing carrier of information about an event that is related to the phenomenon under research and investigation in terms of causality, time, and space. The digital trace is not information itself but a carrier of information that can be interpreted for criminalistics purposes, serving as a medium through which the event becomes knowable. According to the Slovak school of criminalistics, any digitally stored or transmitted information with evidentiary value is considered a digital trace. With the ability to record and transmit information that enables the reconstruction of a past event, it acts as an information link between an action and its result. The information content, carrier, criminalistic value, and connection to the event define each trace. (Metenko & Metenkova, 2024; Metenko, 2004)

Despite being conceptually identical to the traditional trace, the digital trace is qualitatively different because it only exists through its technological medium, such as data systems, networks, or devices, and vanishes as soon as the carrier's integrity is jeopardised (Casey, 2011). Digital traces, in contrast to other material traces, are relatively ephemeral and unstable; their continued existence is contingent

upon the reliability of data structures, storage systems, and the precision of the collection and preservation processes. It is a unique kind of evidential phenomenon that criminalistics must interpret within a new ontological framework due to its volatility and reliance on technological stability.

The digital trace is a mediated construct that is perceived through its technological representation from an epistemological perspective. There are two levels of interpretation: the technical level, which involves creating and processing data, and the cognitive level, which involves assigning meaning. Verification standards that guarantee the validity, authenticity, and integrity of digital evidence are necessary for this dual mediation (Eurojust, 2022). From a criminalistic perspective, this mediation represents a dual cognitive process: the trace connects the technological layer of data with the epistemic layer of understanding by both transmitting information and co-creating the investigator's knowledge about the investigated activity. The proposed Digital Authenticity Framework (D-AUTH), which operationalises the verification of digital trace as future evidence through procedural, contextual, and technical controls, is based on these principles.

Digital traces can be the result of automated or human activity. While secondary traces result from system processes, primary traces are the result of intentional or unintentional human activity (Casey, 2011; Brenner, 2010). The establishment of their integrity, continuity, and origin determines their evidential value.

Analytically, the digital trace blends causal determinism and information abstraction, necessitating the fusion of traditional forensic principles with computer-science techniques and methods. Hash verification, complete chain-of-custody documentation, and the preservation of the original data structure continue to be crucial procedural requirements (INTERPOL, 2021).

By creating data that has all the formal characteristics of authentic traces, but no causal connection to actual events, artificial intelligence makes this framework more difficult to understand (Mirsky & Lee, 2021; Verdoliva, 2020). These "pseudo-traces" cast doubt on criminalistics epistemological underpinnings and change the main inquiry from "What does the trace reveal?" to "Is the trace real?" (Qureshi et al., 2024). As a result, the digital trace maintains the traditional trace identification, reconstruction, and verification capabilities while requiring a revised methodological and epistemological interpretation appropriate for the algorithmic environment of contemporary reality. These theoretical premises later form the basis of the proposed Digital Authenticity Framework (D-AUTH), which operationalises the verification of authenticity, provenance, and integrity of digital evidence in AI-mediated environments.

TERMINOLOGICAL CLARIFICATION: TYPOLOGY OF DIGITAL TRACES

On the basis of the definition of terms for digital trace typology, digital traces can be grouped according to their provenance, potential for evidence, and causal relationship to reality. From a criminalistic perspective, these classifications specify not only the data source but also its dependability and probative purpose. Communication logs, login credentials, and file metadata are examples of primary digital traces that are directly caused by human activity in the digital environment and have a direct causal relationship to human behaviour (Casey, 2011; Brenner, 2010).

Systems and infrastructures, such as log files, cache memory, or network routing data, automatically create secondary digital traces without direct human involvement (Casey, 2011).

Artificial intelligence or generative models are the source of synthetic traces, which have the formal characteristics of evidence (timestamp, format, metadata) but no confirmed causal connection to any actual event (Mirsky & Lee, 2021; Verdoliva, 2020; Qureshi et al., 2024). The growing interdependence between algorithmic and human activity in digital environments is reflected in hybrid traces, which combine elements of AI and authenticity (for example, real audio combined with artificial imagery).

Lastly, purposefully created or falsified artifacts that mimic real evidence are known as pseudo-traces. Their ontological falsity and perceptual realism pose an epistemological risk by blurring the boundary between reality and simulation. The idea of hybrid or pseudo-traces, though not explicitly acknowledged in conventional criminalistic theory, captures the changing epistemic difficulties of AI-mediated environments.

This typology emphasises the need for multimodal verification and critical evaluation of authenticity in AI-mediated contexts, while also capturing the dynamic nature of digital evidence, where traces may come from both human and machine behaviour.

This typology clarifies the methodological and epistemological differences among digital artifacts used in criminalistics/forensic analysis. The ability to accurately classify a trace is necessary for evaluating its causal relationship to an event, chain of custody, and probative value in court. This approach, which emphasises the preservation of carrier integrity and contextual documentation of the digital environment, is in line with current international forensic standards, including ENFSI's guidelines for image and video authenticity verification and INTERPOL's Guidelines for Digital Forensics First Responders (2021).

ARTIFICIAL INTELLIGENCE AS A FACTOR OF TRANSFORMATION IN CRIMINALISTIC TRACE ANALYSIS

Since it alters the creation, processing, and interpretation of traces, the impact of artificial intelligence on the evolution of criminalistic trace analysis marks a paradigm shift in criminalistics. AI presents new forms that are partially or completely algorithmic in origin, following the typology of digital traces. As a result, the field must reevaluate its methodological and epistemological presumptions. AI is now a topic, a tool, and a distorting factor of criminalistic cognition rather than just a tool to support analysis.

1. AI systems produce traces themselves, including logs, configuration information, algorithmic parameters, and outputs that document autonomous system behaviour, which can be examined for criminalistics purposes. Since the meaning of these machine-origin traces depends on knowing how the model or system functioned, specialised techniques of algorithmic attribution and contextual reconstruction are needed (Casey, 2011).

2. By processing large datasets, identifying patterns, and connecting disparate data, artificial intelligence (AI) improves investigators' analytical skills. When decisions are made using "black box" models, it facilitates probabilistic reasoning but also raises questions about accountability, reproducibility, and transparency (Eurojust, 2022). In order to meet evidential requirements, algorithmic outputs must continue to be interpretable, verifiable, and reproducible.

3. The fundamental tenet of causality is called into question by AI, which distorts reality by creating artificial content that is identical to authentic records. Although "pseudo-traces" produced by deepfake technologies lack an ontological foundation in reality, they formally resemble genuine evidence (Mirsky

& Lee, 2021; Verdoliva, 2020). Through the so-called liar's dividend, these artefacts have the potential to skew perception, divert investigations, or erode reliable evidence (Chesney & Citron, 2019).

Therefore, algorithmic literacy and methodological discipline must be combined in criminalistics: detection, provenance verification, and contextual documentation must be used in addition to traditional analysis. Thus, the question of artificial intelligence becomes not only a technical one but also a philosophical and epistemological one, forcing criminalistics to consider not only "What does the trace reveal?" but also "Is the trace real?"

The function of criminalistics science must go beyond interpretation in this new setting, where traces may be artificially created or modified; it must also involve the detection and technical validation of authenticity. The primary detection techniques and their methodological drawbacks in AI-mediated evidence analysis are thus described in the following section.

TECHNICAL METHODS OF DETECTION AND THEIR LIMITATIONS

The primary reaction to the spread of manipulated media has been the quick development of AI-based forensic methods. They generally aim to discriminate between real and manipulated image, audio, or video data, often by identifying artefacts that may be incompatible with genuine content, although their approaches and transparency vary.

Benchmarking and Model Evaluation

For training and assessing detectors, public datasets like FaceForensics++ and the DeepFake Detection Challenge (DFDC) continue to be essential resources. The findings highlight the necessity of ongoing benchmarking by demonstrating that performance declines under compression, unknown synthesis methods, and out-of-distribution circumstances (Rössler et al., 2019).

Detection Approaches

Contemporary detectors based on convolutional neural networks (CNNs) and transformers often learn to recognise subtle spatial-temporal irregularities such as texture inconsistencies, blending edges, or micro-movements that can indicate manipulation (Verdoliva, 2020). In order to uncover manipulations that are invisible to the naked eye, complementary forensic techniques examine anomalies in the signal and metadata, such as double compression, irregularities in the sensor, or inconsistent EXIF data (Casey, 2011).

Provenance and Cryptographic Control

Projects such as the Content Authenticity Initiative and the C2PA standard embed signed manifests that document the origin and editing history of a file. Although they improve provenance verification, these credentials do not confirm that the scene being portrayed is accurate (Coalition for Content Provenance and Authenticity, 2024).

Limitations and Ongoing Evaluation

As generative models advance, so do detection tools. Techniques like post-processing, re-encoding, or "fingerprint removal" lessen generalisation, which means that no detector is completely trustworthy.

Provenance validation, multimodal content detection, and procedural safeguards like chain-of-custody and cryptographic hashing must thus be combined in three layers for effective verification.

With a focus on reproducibility and benchmark transparency, independent initiatives such as NIST's Open Media Forensics Challenge (Open MFC) continuously evaluate detection systems across modalities (NIST, 2024–2025).

LEGISLATIVE AND NORMATIVE FRAMEWORK OF THE EUROPEAN UNION

The European Union has created a unified regulatory framework governing accountability, transparency, and evidential admissibility in AI-assisted procedures in response to the swift integration of AI into legal and investigative systems.

The foundation of this framework is the Artificial Intelligence Act (Regulation (EU) 2024/1689), which goes into effect on August 1, 2024. While provisions for general-purpose AI systems (GPAI) go into effect on August 2, 2025, the majority of obligations will be applicable within 24 months. The Act establishes a risk-based methodology that calls for openness, record-keeping, and human supervision, especially for AI tools utilised in law enforcement and justice. It creates an obligation for criminalistics to guarantee algorithmic traceability, supervision, and model behaviour recording.

The first legally binding international treaty on AI, the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law (2024), complements the EU Act by enshrining the principles of accountability, explainability, and judicial review for systems that impact fundamental rights (Council of Europe, 2024).

The Eurojust-eu-LISA Joint Report (2022) describes useful AI applications in criminal justice at the operational level, including NLP-based document analysis, digital evidence triage, and audio-visual anonymisation. Contextual integrity - maintaining software versions, configurations, and analytical audit logs - is emphasised as the basis for evidential reliability, which the AI Act subsequently reflects.

Lastly, the ENFSI and INTERPOL standards, which outline procedural requirements for securely gathering, archiving, and validating digital evidence, including keeping audit records of analytical settings, have incorporated AI-related recommendations (INTERPOL, 2021; ENFSI, 2021).

These tools work together to create a multi-layered regulatory framework that links technological innovation and evidential legality. To ensure that the evidential pursuit of truth is consistent with AI-driven realities, they demand that AI-assisted criminalistic techniques continue to be transparent, traceable, and reproducible.

CONCLUDING REMARKS ON THE ROLE OF ARTIFICIAL INTELLIGENCE IN CRIMINALISTICS

Artificial intelligence is reshaping the ontological, epistemological, and methodological foundations of criminalistics. It no longer functions merely as a tool but as an autonomous element influencing the creation, processing, and interpretation of information.

The concept of criminalistics trace must therefore be redefined. AI introduces "machine-generated realities" in which traces may arise without any causal link to real events. Criminalistic truthfulness - the ability of a trace to convey reliable knowledge about reality - requires new interpretative and verifica-

tion frameworks combining causality, identification, and reconstruction with technical mechanisms such as metadata analysis, algorithmic auditability, and synthetic-pattern detection.

AI enhances analytical efficiency by enabling large-scale data examination and the discovery of hidden patterns, yet simultaneously threatens evidential integrity by generating synthetic or falsified content. Criminalistics must thus adopt a balanced approach - *augmented judgment* -where algorithmic precision complements, but never replaces, human expertise and responsibility.

Normatively, digital-evidence standards based on digital traces must ensure accountability for autonomous outputs and the protection of data integrity. Ethical guidance is equally vital to prevent algorithmic bias and preserve due process and justice (Eurojust, 2022).

Criminalistics is entering a new developmental phase as an interdisciplinary science that must account for the cognitive processes of artificial systems. The trace, once a direct imprint of reality, increasingly becomes an algorithmic construct. Its future credibility depends on maintaining balance between methodology and technology, automation and accountability, and knowledge and its source - ensuring that even in an AI-mediated world, the pursuit of truth remains the central mission of criminalistics.

METHODOLOGICAL AND PRACTICAL IMPLICATIONS FOR CRIMINALISTICS

The most obvious example of how criminalistics has evolved in the era of artificial intelligence is the methodological reconfiguration of how digital trace is viewed, validated, and evaluated. The notion that a trace is a tangible record of an incident that arises from direct contact between an offender and their environment served as the basis for traditional criminalistics methodology. This model was effective as long as there was a clear causal relationship between the event and its trace. This relationship, however, falters in the age of algorithmic reality since artificial intelligence can now mediate, modify, or even create a trace.

This shift calls for a substantial methodological modification. The idea of digital authenticity must now be viewed by the field as the practical counterpart of material authenticity. While digital authenticity can be verified by physical or chemical examination, it must be established through a sequence of interconnected technical, analytical, and logical procedures. Therefore, a criminalistic analysis must take into account the circumstances surrounding the creation of the trace, processing, and transmission in addition to its content (Casey, 2011).

This modification has the methodological effect of giving traditional criminalistic categories an algorithmic and informational component. Instead of merely studying a trace as the result of an event, it is now possible to study it as the result of a processing system with its own internal logic and dynamics. Thus, it is necessary to create an analytical framework that can distinguish between authentic, fraudulent, and modified traces. This adds a new element to criminalistics by bringing the identification principle into the field of algorithmic attribution: the analysis of the behaviour and origin of the data object.

Theoretically, the ongoing development of criminalistics can be considered a part of the growth of security-oriented cognition. According to Ivančík (2022), the methodological foundations of security must consider the interdependence of knowledge, governance, and technology since every act of cognition also functions as an act of direction. The analysis of digital traces, which necessitates a systematic assessment of technological operations from the perspectives of security and cognition, can benefit equally from this concept.

Practically speaking, technical accuracy and interpretive reasoning must be combined in criminalistic analysis. Investigators must examine digital traces as evidence provenance, structure, data environment, and processing context in addition to its security. Therefore, European organisations (Eurojust, 2022) recommend establishing a comprehensive integrity ecosystem for digital traces use as evidence, which includes audit records of the algorithms used in data processing, software versions, system configurations, and metadata.

The core principles of criminalistic thinking - cause, credibility, and verification - must be maintained while being reinterpreted in the digital sphere. Whereas classical criminalistics focused on the physical relationships between a trace and an event, modern criminalistics must look into informational and algorithmic relationships, which are often indirect, probabilistic, and dynamic, even though they exist in a material environment. Since the outcome of such analysis is rarely a binary conclusion but rather a graded level of probability, higher levels of expertise and interpretive judgment are needed.

In this new context, the role of the criminalist changes from that of an observer to that of an interpreter of technological processes. The modern investigator needs to understand not only the evidence but also the systems of evidence generation, transformation, and analysis. As a result, criminalistic inquiry becomes an interdisciplinary process that integrates concepts from computer science, ethics, logic, and law. Without this information, the full complexity of digital traces evidential value cannot be assessed.

Special attention must also be paid to the issue of accountability for decisions made with AI assistance. When algorithmic outputs affect the conclusion of a criminal investigation or proceeding, it must be clear who is in charge of their use and interpretation. AI must be used as a tool to help, not as a decision-maker in and of itself, according to legal and methodological frameworks. This perspective is encapsulated in the concept of augmented judgment, which is decision-making that combines algorithmic precision with human critical oversight.

Ultimately, rather than being a threat, the methodological and practical implications of artificial intelligence should be viewed as an evolutionary catalyst. They compel criminalistics to systematically reexamine its theoretical foundations, expand its toolkit of methods, and seek out new insights into truth in an environment where reality itself can be manufactured. As a result, criminalistics is changing from being a science of traces to one that understands and interprets traces in the context of algorithmic reality. However, ensuring that truth can be recognised even in the face of perfect technological imitation remaining its core objective.

METHODOLOGICAL FRAMEWORK FOR DIGITAL AUTHENTICITY

In the era of artificial intelligence, ensuring the authenticity and evidential integrity of digital content necessitates a methodical approach that combines technical verification, contextual documentation, and procedural guarantees. To standardise these processes, the proposed Digital Authenticity Framework (D-AUTH) expands upon ENFSI, INTERPOL, and Eurojust best practices.

Creating a forensic image, using cryptographic hashing (SHA-256, for example), and using write-blocking to preserve the original data are the first steps in the procedural level of authenticity. In addition to contextual records that describe the operating environment, including system versions, configurations, timestamps, and network conditions, each version of the evidence must be recorded within a verified chain of custody (ENFSI, 2021; INTERPOL, 2021). Researchers should also note model version, build identifier, and dataset references that affect results when AI systems are used (Eurojust/eu-LISA, 2022).

The second pillar is provenance verification. The origin and editing history of a file are documented by cryptographically signed metadata frameworks like the C2PA Content Credentials Standard (Coalition for Content Provenance and Authenticity, 2024). Although provenance by itself does not establish veracity, "soft provenance" indicators, such as server logs, CDN records, or first-seen timestamps, may assist authenticity assessments in the absence of such credentials.

Global and local analysis, error-level mapping, photo-response non-uniformity (PRNU), statistical feature extraction, and heat-map visualisation are among the blind and knowledgeable forensic techniques that are integrated into the analytical stage. To increase the probative value, results should, whenever feasible, be cross-checked with independent traces like geolocation, focal length, illumination, or telecom data.

Algorithmic auditability and configuration transparency are crucial for AI-based forensic tools. Model version, reproducibility seed, robustness testing, and probabilistic, rather than binary results, must all be included in the documentation. Forensic reliability includes the explicit recognition of uncertainty. Reproducibility also necessitates that all parameters and processes be adequately documented to enable independent replication by a different specialist.

Thus, the D-AUTH framework combines procedural integrity, forensic detection, and provenance control into a single digital authenticity model. Through the integration of these principles into investigative and judicial processes, criminalistics can preserve the epistemological underpinnings of truth in the age of algorithmic mediation by converting authenticity from a presumption into a verifiable, reproducible, and demonstrable attribute of digital evidence. The D-AUTH framework thus operationalises the core forensic triad of identification, authenticity, and chain-of-custody within AI-mediated environments.

CONCLUSION

One of the most revolutionary developments in criminalistics is the transformation of the digital traces from the end of last century into artificial intelligence in recent years. It has changed the creation, preservation, and interpretation of traces, thereby changing the epistemological underpinnings of the field. The digital trace was once a reliable and verifiable source of information, but it now exists in a dynamic environment where authenticity cannot be assumed.

AI forces important criminalistic ideas to be redefined. It is important to consider the trace as a reflection of an event, as well as a possible algorithmic generation product that could mimic or warp reality. As a result, informational and algorithmic aspects must be incorporated into conventional theories of trace and formatting evidence. "What does the trace reveal?" has given way to "Is the trace real?" as the central epistemological query in criminalistics. Historically, however, such problems have been partially addressed by criminalistics in the past.

Verification frameworks must take algorithmic mediation into consideration in order to address this, assessing digital trace for both its technical integrity and the dependability of the systems that generated it. Multilayered validation that integrates technical, analytical, and interpretative evaluation takes the place of physical verification of classic material traces.

In practice, artificial intelligence (AI) improves analytical ability by processing large datasets and uncovering hidden relationships, but it also poses risks by producing fake or modified traces. Thus, an augmented judgment paradigm - where algorithmic accuracy complements but never takes the place of human expertise and accountability - is necessary to preserve evidential legitimacy.

Labels like "authentic" or "fake" are no longer adequate. Explicit uncertainty estimation must be used to support probabilistic, transparent, and repeatable reasoning in modern criminalistics. Three complementary layers must be integrated for verification to be sustainable:

1. Provenance assurance through the use of audit and cryptographic signatures;
2. Multimodal detection and cross-verification of independent traces in criminalistics content analysis;
3. Maintaining chain-of-custody contextual documentation, and secure hashing is known as procedural integrity.

These guidelines are based on the Council of Europe Framework Convention on AI and the EU Artificial Intelligence Act, which together set moral and legal guidelines for the responsible application of AI in criminalistics. Even in a time when imitation and reality are becoming more and more similar, digital traces can maintain their evidential credibility by fusing technological accuracy, methodological openness, and normative accountability.

The study emphasises that every digital trace must be examined both technically and as a component of cognition - a carrier of knowledge about the event itself - in accordance with the epistemological framework of criminalistics.

REFERENCES

Brenner, Susan W., "*Cybercrime: Criminal Threats from Cyberspace*" (2010). School of Law Faculty Publications. 115. https://ecommons.udayton.edu/law_fac_pub/115

Casey, E. (2011). *Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet Third Edition.* ISBN: 978-0-12-374268-1

Chesney, R. & Citron, D.K. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, *California Law Review*, 107(6), pp. 1753. Available at: https://scholarship.law.bu.edu/faculty_scholarship/640. ISSN 0008-1221

Coalition for Content Provenance and Authenticity. (2024). *C2PA technical specification* (Version 1.4). Retrieved from https://c2pa.org/specifications/

Council of Europe. (2024). *Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law.* Strasbourg: Council of Europe. Retrieved from https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence

ENFSI. (2021). *Best Practice Manual for the Forensic Examination of Digital Images and Video*. European Network of Forensic Science Institutes. Retrieved from https://enfsi.eu/about-enfsi/structure/working-groups/documents-page/documents/best-practice-manuals/

Eurojust (2022) *Artificial intelligence supporting cross-border cooperation in criminal justice joint report prepared by eu-lisa and eurojust.* doi: 10.2857/364146 Catalogue number: EL-09-22-215-EN-N. ISBN 978-92-95227-17-0

INTERPOL (2021) *Guidelines for Digital Forensics First Responders: Best practices for search and seizure of electronic and digital evidence*. Lyon: INTERPOL.

Ivančík, R. (2022) *Bezpečnosť: teoreticko-metodologické východiská.* Plzeň: Aleš Čeněk. 978-80-7380-873-0.

Meteňko, J., a kol. (2004) *Kriminalistické metódy a možnosti kontroly sofistikovanej kriminality*. Bratislava 2004. Akadémia PZ SR v Bratislave. ISBN 80-8054-336-4, EAN 9788080543365. 356 s., p. 7 et seq.

Meteňko, J., Meteňková, M., (2024) Theory of Criminalistics traces and their system. Kriminalistinė pėdsakų teorija ir jų sistema. [in:] Juodkaitė-Granskienė, G., Mozūraitis, G., Kriminalistika ir teismo ekspertologija: Mokslas, studijos, praktika, *XX. Criminalistics and criminalistic expertology: science, studies, practice*. Mykolo Romerio universitetas, Lietuvos teismo ekspertizės centras, Lietuvos kriminalistų draugija, Lenkijos kriminalistų draugija, Vilnius, 2024, ISSN 2783-7068. 338 p., pp. 41-47.

Mirsky, Y. and Lee, W. (2021) *The Creation and Detection of Deepfakes*. ACM Computing Surveys, 54, 1-41. https://doi.org/10.1145/3425780

National Institute of Standards and Technology. (2024–2025). *Open Media Forensics Challenge (OpenMFC)*. Gaithersburg, MD: U.S. Department of Commerce. Retrieved from https://www.nist.gov/itl/iad/mig/open-media-forensics-challenge

Qureshi, S.M., Li, F., Hussain, A. and Khan, M. (2024). *Deepfake forensics: A survey of digital forensic methods for detecting manipulated media.* https://pmc.ncbi.nlm.nih.gov/articles/PMC11157519/, doi: 10.7717/peerj-cs.2037.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)

Rössler, A., Cozzolino, D., Verdoliva, L., Riess, C., Thies, J., & Nießner, M. (2019). FaceForensics++: Learning to detect manipulated facial images. *Proceedings of the IEEE/CVF International Conference on Computer Vision* (ICCV), 1–11. https://doi.org/10.48550/arXiv.1901.08971

Verdoliva, L. (2020). Media Forensics and Deepfakes: An Overview, in *IEEE Journal of Selected Topics in Signal Processing*, vol. 14, no. 5, pp. 910-932, Aug. 2020, doi: 10.1109/JSTSP.2020.3002101.