Jurnal Hukum Prasada
Volume 13, Number 1, 2026, pp 37-45
ISSN (print) 2337-795X; ISSN (online) 2548-4524
https://doi.org/10.22225/jhp.13.1.2026.37-45

OPEN ACCESS
*Original Research Article*

Article received: January 8, 2026 Reviewed: March 27, 2026 Accepted: March 30, 2026

# The Probative Power of Deepfake-Based Electronic Evidence in Fraud Crimes

Wahyu Slamet Permadi[1] | Aries Isnandar[1] | Yogi Prasetyo[1]

1. Universitas Muhammadiyah Ponorogo, Jawa Timur, Indonesia

Correspondence regarding this article should be addressed to:
Wahyu Slamet Permadi, Universitas Muhammadiyah Ponorogo, Jawa Timur, Indonesia
Email address: wpermadi64@gmail.com

**Abstract**. Advances in artificial intelligence technology, especially deepfakes, pose serious problems for the system of evidence in criminal law, particularly in the handling of digital-based fraud. Audio and visual manipulation that increasingly resembles authentic conditions has the potential to undermine the authenticity and integrity of electronic evidence, increase the possibility of misrepresentation, and hinder efforts to achieve material truth and legal certainty. This study aims to analyze the legal position and evidentiary value of deepfake-based electronic evidence in criminal fraud cases according to the Indonesian positive law framework, as well as to formulate a model for assessing the reliability of electronic evidence that is responsive to the dynamics of artificial intelligence development. This research uses a normative legal research method through a legislative, conceptual, and comparative approach. Primary and secondary legal materials are analyzed qualitatively through a review of national norms regarding electronic evidence and a comparison of digital evidence practices in a number of other jurisdictions. The findings of the study show that normative recognition of electronic evidence in Indonesian criminal procedure law is already available, while technical regulations related to authentication and evaluation of the reliability of artificial intelligence-based electronic evidence, particularly deepfakes, have not been specifically formulated. The absence of specific technical regulations weakens the material strength of evidence and places the assessment of judges and digital forensic experts as the main determining factors. The urgency of strengthening criminal procedure law is emphasized through the application of the Electronic Evidence Reliability Framework (EERF), which integrates digital forensic verification, metadata validation, and the continuity of the chain of custody of electronic evidence to ensure justice, legal certainty, and the protection of the rights of the parties in the criminal justice process.

**Keywords**: criminal procedure law; deepfake; digital fraud; electronic evidence

## Introduction

The development of artificial intelligence (AI) technology has given rise to various digital innovations that have had a significant impact on social life and the legal system, one of which is deepfake technology. Deepfake is a deep learning-based audio and visual engineering technique capable of producing highly realistic digital representations that are difficult to distinguish from factual events (Verdoliva, 2020). In the context of criminal law, particularly fraud, this technology poses serious problems because it is often used as a means of constructing deceptions to convince victims (Hidayat and Putri, 2023). This situation makes deepfake not only a technological issue but also a fundamental challenge to the criminal evidence system that relies on the search for material truth (Hamzah, 2021).

In Indonesian criminal procedure law, evidence plays a central role as the basis for forming a judge's conviction. Recognition of electronic evidence has been granted through Law Number 11 of 2008 concerning Electronic Information and Transactions and its amendments, which expands the types of

evidence as regulated in Article 184 of the Criminal Procedure Code (Mertokusumo, 2023). Several studies confirm that electronic evidence is a necessity in the modern justice system, but its validity is highly dependent on the principles of data authenticity and integrity (Siregar et al., 2024). In recent developments, the existence of deepfake technology has shifted the paradigm of electronic evidence authentication due to its ability to manipulate reality precisely and is difficult to detect with conventional methods (Prasetyo and Alamsyah, 2024).

However, previous studies have generally focused on the normative recognition of electronic evidence and cybercrime in general, without adequately addressing the specific characteristics of AI-based electronic evidence. A major limitation of these studies lies in the absence of technical authentication standards for synthetic evidence generated by AI algorithms (Suryana, 2022). Consequently, there is no comprehensive analytical framework for how deepfake evidence should be assessed in criminal proceedings, particularly when it is used to prove deception in fraud (Putra and Nugroho, 2021).

This lack of regulation and evidentiary standards has direct implications for criminal justice practice. In the absence of binding authentication guidelines, the assessment of the validity of deepfake evidence relies heavily on expert testimony and the subjective beliefs of judges (Arief, 2022). This situation has the potential to create legal uncertainty and the risk of judicial error, particularly when doctored audio-visual evidence is treated as if it represents factual events (Yuliana, 2023). Therefore, a normative approach is needed that can systematically integrate the technical aspects of digital forensics into the criminal evidence system.

The novelty of this research lies in the formulation of a conceptual framework for assessing the reliability of deepfake-based electronic evidence, which has not been widely developed in Indonesian criminal law studies. This research develops an Electronic Evidence Reliability Framework (EERF) that integrates the principles of algorithmic trust and digital provenance chain as the basis for objectively evaluating the reliability of electronic evidence (West and Farrell, 2023). This approach offers a new perspective that assesses evidence not only from its external form but also from the transparency of its formation process and digital traceability (Ramos and Hutton, 2022).

The purpose of this study is to analyze the legal standing and probative value of deepfake-based electronic evidence in fraud crimes under Indonesian positive law, while also formulating a model for assessing the reliability of electronic evidence that is adaptive to developments in artificial intelligence. This article is structured with an introduction, research methods, results and discussion, and a conclusion containing conclusions and recommendations for updating criminal procedural law to maintain its relevance to the challenges of contemporary digital technology (Putra and Nugroho, 2021).

## Method

This study is a conceptual article that uses a normative legal research approach to systematically examine the position and evidentiary value of electronic evidence sourced from deepfake technology in criminal fraud cases. The normative legal approach was chosen because this study focuses on the analysis of positive law, the principles of evidence, and the development of normative arguments relevant to developments in artificial intelligence technology and criminal evidence law (Romero-Moreno, 2025).

The research method was conducted through a limited literature survey of recent scientific articles discussing electronic evidence, digital content manipulation, and the implications of deepfakes on criminal evidence systems. This literature survey aimed to record the conceptual approaches, normative solutions, and limitations of the legal framework that had been presented in previous studies as the basis for formulating the normative ideas developed in this study (Firdaus and Puspita, 2025).

Operationally, this study uses three normative approaches. The statute approach is used to analyze criminal procedural law provisions and regulations related to electronic evidence in Indonesia and to

identify normative gaps in dealing with algorithmically manipulated digital content. The conceptual approach is applied to build a theoretical understanding of the authenticity, integrity, and credibility of digital evidence in the context of deepfake technology. Furthermore, the comparative approach is used to examine international legal discourse and best practices that have developed in the literature related to the challenges of proving digital evidence and the threat of deepfakes to the criminal justice system (Firdaus and Puspita, 2025).

These three approaches are used as an analytical basis for formulating a conceptual model of evidence that is adaptive to developments in artificial intelligence technology, taking into account the constraints of authentication, verification, and reliability of deepfake evidence, as well as the limitations of the existing legal framework in distinguishing between authentic and synthetic content (Darmawan et al., 2025).

## Discussion

### The Position of Deepfake-Based Electronic Evidence in the Indonesian Criminal Evidence System

Electronic evidence is gaining importance in the criminal justice process. In Indonesian criminal procedure law, Article 184 of the Criminal Procedure Code (KUHAP) requires that evidence be valid for consideration by a judge. Recognition of modern electronic evidence is stipulated in Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE), which recognizes electronic information and/or documents as evidence as long as they meet the requirements of authenticity, integrity, and accountability. However, this regulation is general in nature and does not specifically distinguish between types of electronic evidence that have manipulative characteristics, such as deepfakes in audio and visual form, thus raising legal questions regarding its position in the context of accurate and fair criminal evidence (Haida and Nuriyatman, 2024).

From a legal positivist perspective, the recognition of electronic evidence in the ITE Law reflects the legislative adaptation to the rapidly evolving digital reality. This aligns with research findings showing that the Indonesian legal system has evolved to accept digital evidence in line with modern evidentiary needs, but still has a normative gap regarding the nature of evidence synthetically produced by artificial intelligence algorithms (Hartono and Yuliartini, 2020).

Deepfakes, as a synthetic technology, use artificial intelligence to generate visual or audio content that appears real but never actually occurred. This characteristic raises an epistemological issue in the context of criminal evidence, namely doubting the causal relationship between the evidence and the facts themselves. In evidentiary theory, evidence must demonstrate relevance and reliability regarding the events in question; when evidence is created through an artificial reconstruction process, it loses the objective character necessary to materially prove the facts (Mohamed et al., 2023).

This debate has also received attention in international comparative studies. Several international articles have asserted that traditional authentication standards are not designed to handle evidence derived from content engineered with generative algorithms, leading some academics to advocate expanding the rules of evidence to include adequate technical verification mechanisms (UC Law Journal, 2022) in (*Deepfake dalam Persidangan: Seruan untuk Memperluas Peran Pengawas Hakim dalam Melindungi Proses Hukum dari Pemalsuan Teknologi | Jurnal Hukum UC*, n.d.)

From empirical research in Indonesia, there is a gap in norms that makes it difficult for law enforcement officials to classify deepfake actions according to the appropriate criminal corridor, because legal doctrine has not yet established specific evidentiary parameters for generative evidence (W. Putra, 2025).

This issue is further complicated when deepfake evidence is used in fraud cases involving financial fraud or extortion schemes, as deepfake manipulators often use other data such as digital metadata, communication records, and organically constructed digital footprints to bolster their false narratives.

This approach requires multiple layers of evidence testing through content validation, metadata authentication, and comparison with other supporting evidence such as witness testimony or transaction records (Haida and Nuriyatman, 2024).

## The Probative Strength of Deepfake Evidence in Fraud Cases

Fraud is a criminal act that requires mens rea (malicious intent) and requires an element of deception that causes the victim to suffer material harm. In the digital age, fraud methods have become increasingly complex with the emergence of deepfakes, which manipulate a person's image to appear as if they are doing or saying something real when they are not (Putri et al., 2024).

In the context of Indonesia's criminal evidence system, which adheres to the principle of free evidence (vrije bewijskracht), judges are given the freedom to assess all evidence presented without a strict hierarchy, but must still be based on rational and proportional beliefs regarding the facts of the case. However, deepfake evidence introduced into court without adequate technical authentication risks clouding the judge's judgment because its visual nature is very convincing, but it cannot guarantee that the content truly reflects the reality of the criminal event (Syukri, 2024).

Deepfake evidence should be considered circumstantial evidence because it provides only a seemingly realistic representation of visual or audio content, but does not directly prove the perpetrator's actions. The assessment of this type of evidence requires the integration of digital forensic verification, as without valid technical mechanisms, digital manipulation can mislead judges and undermine the search for material truth (Sandoval et al., 2024).

Empirical studies of the use of electronic evidence in criminal proceedings show that its effectiveness depends heavily on how the evidence is obtained and presented in court, as well as on compliance with applicable legal procedures. When digital evidence is presented without comprehensive verification, especially evidence processed through AI, its evidentiary strength is weakened and can be questioned by a judge (Divaresky and Yusuf, 2025).

This issue is further complicated when deepfake evidence is used in fraud cases involving financial fraud or extortion schemes, as deepfake manipulators often use other data such as digital metadata, communication records, and organically constructed digital footprints to bolster their false narratives. This approach requires multiple layers of evidence testing through content validation, metadata authentication, and comparison with other supporting evidence such as witness testimony or transaction records (Haida and Nuriyatman, 2024).

## Challenges to Authentication Standards and Judge Assessment

The development of deepfake technology poses significant challenges to Indonesia's criminal evidence system, particularly in the context of authenticating electronic evidence. Research shows that existing verification mechanisms are unable to ensure the authenticity of evidence generated by artificial intelligence algorithms, significantly increasing the potential for judicial error (W. Putra, 2025) .

Traditional authentication standards, which have traditionally been applied to conventional documents or simple electronic evidence, have proven inadequate for handling generative evidence. This is reinforced by international research that highlights that deepfake algorithms can create videos or audio that are indistinguishable from real footage without the aid of AI-based forensic methods (D. M. West and Farrell, 2023).

In Indonesian court practice, judges still rely on the testimony of digital forensic experts to assess the authenticity of electronic evidence. However, the methods used are case-by-case and not yet standardized, making the assessment of deepfake evidence subjective and potentially leading to disparities in verdicts between cases with similar evidence characteristics (Suryana, 2022).

Furthermore, limited institutional and technical capacity of law enforcement officials adds to the complexity. The lack of digital forensic laboratories capable of AI-based manipulation detection and the absence of national competency standards for digital forensic experts mean that testing deepfake

evidence often relies on individual skills, thus impacting the consistency of court decisions (B. Putra and Nugroho, 2023).

From a legal doctrine perspective, judges' freedom of proof (vrije bewijskracht) should be limited by the principle of judicial prudence, particularly when dealing with evidence that is highly technologically manipulated. Judges must consider the integrity, authenticity, and relevance of digital evidence as prerequisites for deciding cases of deepfake fraud (Arief, 2022).

## Electronic Evidence Reliability Framework (EERF) Conceptual Framework

In response to the challenges of authentication and evidentiary strength, this study proposes the Electronic Evidence Reliability Framework (EERF) as a conceptual model for assessing the reliability of deepfake-based electronic evidence. This framework consists of two main pillars: Algorithmic Trust Doctrine and Digital Provenance Chain.

The Algorithmic Trust Doctrine emphasizes the openness, accountability, and auditability of algorithms that generate evidence. This principle requires that the evidence generation process be independently replicable, verifiable, and auditable, thereby minimizing the risk of uncontrolled presentation of manipulated evidence (C. Ramos and Hutton, 2022).

The Digital Provenance Chain ensures traceability of evidence from its creation to its presentation in court. Every step, from data collection, recording, storage, and AI-based processing, is recorded chronologically and irreversibly. This allows judges to assess evidence based on a clear digital path, not just its visual content (D. M. West & Farrell, 2023).

The implementation of EERF strengthens the validity and strength of evidence through several technical mechanisms:

AI-Based Digital Forensic Verification: Identifies indications of manipulation, GAN generative patterns, and metadata inconsistencies.

Metadata Validation: Ensures the authenticity of digital traces, including timestamps, geotags, and file integrity.

Digital Chain of Custody (Blockchain): Ensures the security and immutability of data from creation to presentation in court (Verdoliva, 2020).

With EERF, deepfake evidence is no longer assessed solely visually or intuitively, but rather through technical indicators that can be retested and scientifically validated. This aligns with the principle of the best evidence rule, which emphasizes that raw data and the authentication process have the highest evidentiary value (Arvitto, 2025).

This framework also provides normative guidelines for judges in assessing electronic evidence, so that decisions rely not only on freedom of evidence but also on the principle of prudence based on scientific evidence. With the implementation of the EERF, it is hoped that there will be increased legal certainty, a reduced risk of wrongful convictions, and fair protection of the rights of defendants and victims (Suteki, 2021).

## Implications for Criminal Procedure Law Reform and EERF Integration

The development of deepfake technology has changed the evidentiary landscape in digital fraud cases. The judicial system's reliance on digital evidence has increased significantly, necessitating adaptive reforms to criminal procedural law. Research findings indicate that the absence of nationally binding authentication standards increases the risk of disparity in verdicts, judicial errors, and potential violations of the principle of procedural fairness. Therefore, criminal procedural law reform is needed to establish a clear and standardized mechanism for verifying digital evidence (W. Putra, 2025).

The Electronic Evidence Reliability Framework (EERF) is one conceptual solution that bridges this regulatory gap. This framework integrates the algorithmic trust doctrine, which demands the transparency of algorithms and the auditability of the evidence creation process, and a digital

provenance chain that ensures the traceability of evidence from creation to trial. The implementation of the EERF enables judges to objectively assess deepfake evidence, reducing reliance on intuitive judgment and increasing legal certainty (D. M. West & Farrell, 2023).

The implementation of EERF in the Indonesian criminal justice system can be carried out through three main stages: first, verification of the metadata and digital footprint of each submitted piece of evidence; second, an audit of the deepfake evidence-forming algorithm by a digital forensic expert; and third, integration of the verification results into the judge's considerations in establishing a criminal conviction. With this approach, deepfake evidence is no longer assessed solely on its visual appearance, but also through technical indicators that can be retested and accounted for (C. Ramos & Hutton, 2022).

Furthermore, legal reform must also include strengthening the institutional capacity of law enforcement officials, including digital forensic laboratories and the competence of AI forensic experts. Current institutional limitations hamper the evidence authentication process and increase the risk of misjudgment. With adequate forensic laboratories, the process of verifying deepfake evidence can be conducted scientifically and uniformly across jurisdictions, thereby increasing the consistency of decisions (Suteki, 2021).

In the context of comparative international law, several countries, such as the United Kingdom and the United States, have adopted heightened scrutiny regarding AI-based digital evidence. Courts require algorithmic analysis and a digital chain of custody before evidence is admitted. This practice could serve as a model for adapting Indonesian law to make the criminal evidence system more responsive to deepfake technology, in(*Kecerdasan Buatan: Ketidakseimbangan Kekuatan – Blog Jurnal Hukum Universitas Cincinnati*, n.d.).

The use of EERF is also relevant to the principle of the best evidence rule, which places original evidence and digital traces as the primary reference. Therefore, deepfake evidence can only be legally admissible if the entire technical process, metadata, and algorithm used to create it can be verified. This reinforces the principles of material and procedural fairness in criminal trials (Verdoliva, 2020).

Beyond technical aspects, EERF integration also impacts criminal law doctrine regarding legal liability for the use of digital evidence. Judges' judgments must consider the potential for manipulation, the technical capacity of the parties involved, and the risk of misidentification of evidence. By implementing EERF, judges can minimize the risk of admitting misleading evidence and maintain the integrity of the judicial process (B. Putra and Nugroho, 2023).

From an academic perspective, this research emphasizes the importance of synergy between the EERF conceptual framework and national legal regulatory reforms. Proposed reforms include adjustments to the Criminal Procedure Code (KUHAP), strengthening the ITE Law, and developing competency standards for digital forensic experts. Implementation of this system is expected to not only improve the validity of evidence but also reduce the risk of legal errors and strengthen legal certainty in deepfake-based fraud cases (Arvitto, 2025).

Ultimately, the implementation of the EERF makes a significant contribution to the development of digital criminal law in Indonesia. This framework ensures that complex electronic evidence such as deepfakes can be integrated into the evidentiary system, adhering to the principles of objectivity, transparency, and accountability. This implementation is expected to form the foundation for adaptive criminal procedural law reform, responsive to technological developments, and ensuring the protection of the rights of all parties in trials (Arief, 2022).

## Epistemological Dimensions Of Legal Proof In The Deepfake Era

The development of deepfake technology challenges the epistemological foundation of criminal law evidence, which has traditionally relied on the assumption that evidence represents empirical facts that have occurred. In classical evidentiary theory, the probative value of evidence is determined by the causal relationship between the evidence and the legal event being proven. Deepfakes undermine this

relationship by presenting visual or audio representations that have no ontological connection to real events, even though they appear perceptually authentic (Vaccari and Chadwick, 2020).

In this context, deepfake-based electronic evidence can no longer be understood as a reflection of reality, but rather as a probabilistic algorithmic construction. This requires a paradigm shift from fact-based evidence to process-based evidence, namely, an assessment of evidence that focuses not only on content but also on the technical process of its formation (Mirsky and Lee, 2021). Without this approach, the evidentiary system risks adopting the illusion of visual truth as the basis for judicial conviction.

This epistemological problem directly impacts the principle of proof in Indonesian criminal procedure law. The principle of seeking material truth requires that all evidence be able to be tested rationally and objectively. When deepfake technology produces content that is visually nearly identical to reality but cannot be verified using conventional methods, the standard of proof must be expanded with scientific instruments based on advanced forensic technology (Kietzmann et al., 2020).

## Criminal Liability Model in Deepfake Fraud

The criminal liability model for deepfake fraud demonstrates a complexity that goes beyond the single-actor paradigm recognized in classical criminal law. Deepfake fraud generally arises from the interaction of various actors within a digital ecosystem, from artificial intelligence model developers, platform providers, system operators, to those actively distributing or monetizing the manipulative content. This multi-actor nature blurs the direct causal line between actions and consequences, thus requiring an expanded, more functional and systemic construction of criminal liability (Mohamed et al., 2023).

In this context, the doctrines of joint criminal enterprise and co-perpetration become relevant in explaining how criminal responsibility can be imposed on more than one perpetrator who knowingly contributes to the commission of deepfake crimes. Studies of digital criminal law show that the division of roles in technology-based crimes does not eliminate criminal culpability, as long as there is a shared awareness of the crime's purpose and a concrete contribution to the fraudulent process (Sandoval et al., 2024). Thus, criminal responsibility can be attached not only to the creator of deepfake content, but also to those who knowingly facilitate or amplify the impact of the fraud.

The functional perpetration approach further emphasizes that legal entities who have factual and functional control over technological systems can be held criminally liable, even if they are not directly involved in content manipulation. In the context of deepfake fraud, this functional control can manifest itself in the form of control of computing infrastructure, algorithm management, or strategic decision-making related to the distribution of manipulative content. Modern criminal law literature emphasizes that functional control is more relevant than direct physical involvement in determining perpetrators of crimes in the digital era (C. Ramos & Hutton, 2022).

Furthermore, the development of artificial intelligence technology has given rise to the concept of algorithmic liability in response to the role of algorithms in shaping criminal acts. This concept does not personify algorithms as legal subjects, but rather positions algorithms as instruments that reflect the will, design, and goals of those who control them. Therefore, if a deepfake algorithm is consciously designed or used for fraudulent purposes, the fault can be attributed to the developer or user of the system (D. M. West & Farrell, 2023).

Recent research in law and technology also emphasizes that artificial intelligence algorithms are implicitly normative, as they contain values, assumptions, and goals embedded by their creators. When these values are directed toward identity manipulation or reality manipulation to deceive victims, the algorithm functions as a means rea, a means that reinforces the perpetrator's malicious intent. Therefore, analyzing the algorithm's architecture, training dataset, and system parameters is crucial in proving criminal liability for deepfake fraud (Romero-Moreno, 2025).

Within the Indonesian criminal law framework, the development of this accountability model challenges traditional doctrine, which still emphasizes a direct relationship between actions and

consequences. Without doctrinal adjustments, perpetrators of deepfake fraud could potentially hide behind technical complexities and digital organizational structures. Therefore, strengthening functional and algorithmic accountability approaches is crucial for criminal law to remain effective in addressing AI-based crimes (Prasetyo and Alamsyah, 2024).

Normatively, the application of an adaptive criminal accountability model to deepfake fraud also aligns with the principle of social defense in modern criminal law. By expanding the scope of subjects who can be held accountable, criminal law functions not only repressively but also preventively, by encouraging technology actors to apply prudential and ethical standards in the development and use of AI systems (W. Putra, 2025).

## Conclusion

This study concludes that the research objectives have been achieved, namely to identify the normative weaknesses of the Indonesian criminal evidence system and to analyze the strength of deepfake-based electronic evidence in criminal fraud cases. The results of the study show that the recognition of electronic evidence in the Criminal Procedure Code and the Electronic Information and Transactions Law is still general in nature and does not yet accommodate the characteristics and risks of evidence manipulation based on artificial intelligence. As a result, deepfake evidence has weak material probative value due to the absence of uniform technical authentication standards, so that its assessment in judicial practice is highly dependent on the judge's belief and the testimony of digital forensic experts.

The contribution of this research lies in highlighting the gap between the development of artificial intelligence technology and the readiness of the normative framework for criminal evidence. This research advances the study of criminal procedure law by offering directions for reform through the integration of the Electronic Evidence Reliability Framework (EERF), strengthening the role of the ITE Law as lex specialis for electronic evidence, and standardizing digital forensics and the protection of the rights of the accused. Thus, this research provides a conceptual and normative basis for the development of a more adaptive criminal evidence system that guarantees legal certainty in the era of artificial intelligence.

## References

Arief, B. N. (2022). Bunga Rampai Hukum Pidana Digital dan Pembuktian Elektronik. Pustaka Magister.

Arvitto, R. S. (2025). Implikasi Hukum Deepfake : Telaah terhadap UU ITE dan UU PDP ( Legal Implications of Deepfake : A Review of the ITE Law and the PDP Law ). 4(2), 73–82.

Darmawan, M. T., Junaidi, A., & Khaerudin, A. (2025). Penegakan Hukum Terhadap Penyalahgunaan Deepfake Pada Pornografi Anak Di Era Artifical Intelegence di Indonesia. Jurnal Serambi Hukum, 18(01), 42–54.

Deepfake dalam Persidangan: Seruan untuk Memperluas Peran Pengawas Hakim dalam Melindungi Proses Hukum dari Pemalsuan Teknologi | Jurnal Hukum UC. (n.d.). Diambil 26 Desember 2025, dari https://www.uclawjournal.org/deepfakes-on-trial-a-call-to-expand-the-trial-judges-gatekeeping-role-to-protect-legal-proceedings-from-technological-fakery/?utm_source=chatgpt.com

Divaresky, R., & Yusuf, H. (2025). Efektivitas Penggunaan Bukti Elektronik dalam Pembuktian Perkara Pidana di Pengadilan Negeri. Jurnal Intelek Dan Cendikiawan Nusantara, 2(5), 9555–9568. https://jicnusantara.com/index.php/jicn/article/view/5406

Firdaus, H. S., & Puspita, L. (2025). Peran Hukum Dalam Mengatasi Penyebaran Konten Deepfake Untuk Penipuan Identitas Digital. UIR Law Review, 9(1), 1–14. https://doi.org/10.25299/UIRLREV.2024.VOL8(2).22095

Haida, R. S. N., & Nuriyatman, E. (2024). Urgensi Pengaturan Perlindungan Hukum Terhadap Korban Deepfake Melalui Artficial Inteligence (Ai) Dari Perspektif Hukum Pidana Indonesia. Jurnal Hukum Respublica, 24(01). https://doi.org/10.31849/RESPUBLICA.V24I01.23327

Hamzah, A. (2021). Hukum Acara Pidana Indonesia. Sinar Grafika.

Hartono, M. S., & Yuliartini, N. P. R. (2020). Penggunaan Bukti Elektronik Dalam Peradilan Pidana. Jurnal Komunikasi Hukum (JKH), 6(1), 281–302. https://doi.org/10.23887/JKH.V6I1.23607

Hidayat, R., & Putri, S. (2023). Deepfake sebagai Modus Baru Penipuan Siber: Tantangan Pembuktian Hukum Pidana. Jurnal

Legislasi Indonesia, 20(3), 221–240.

Kecerdasan Buatan: Ketidakseimbangan Kekuatan – Blog Jurnal Hukum Universitas Cincinnati. (n.d.). Diambil 26 Desember 2025, dari https://uclawreview.org/2023/04/27/artificial-intelligence-power-imbalanced/

Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). Deepfakes: Trick or treat? Business Horizons, 63(2), 135–146. https://doi.org/10.1016/J.BUSHOR.2019.11.006

Mertokusumo, S. (2023). Hukum Acara Pidana Indonesia (Edisi Revisi). Liberty.

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

Mohamed, J., Mekkawi, H., Hassan, J. M., Judge, M., & Hassan, M. (2023). The challenges of Digital Evidence usage in Deepfake Crimes Era. Journal of Law and Emerging Technologies, 3(2), 176–232. https://doi.org/10.54873/JOLETS.V3I2.123

Prasetyo, D., & Alamsyah, R. (2024). Validitas Bukti Elektronik dalam Era Artificial Intelligence. Jurnal Rechtsvinding, 13(1), 55–70.

Putra, A., & Nugroho, B. (2021). Kedudukan Alat Bukti Elektronik dalam Sistem Pembuktian Hukum Acara Pidana Indonesia. Jurnal IUS Kajian Hukum dan Keadilan, 9(2), 417–435.

Putra, B., & Nugroho, A. (2023). Tanggung jawab hukum terhadap penggunaan bukti digital hasil kecerdasan buatan. Jurnal Legislasi Indonesia, 20(4), 505–520. https://garuda.kemdikbud.go.id/documents/detail/3581051

Putra, W. (2025). Kekosongan Norma Autentikasi Bukti Elektronik AI-Based. Jurnal Hukum Normatif, 14(1), 90–110.

Putri, S. M. arani I., Salsabila, N., & Hosnah, A. U. (2024). Kriminalisasi Penggunaan Deepfake dalam Tindak Pidana Penipuan dan Pencemaran Nama Baik: Tantangan dan Solusi Hukum. Jurnal Hukum Legalita, 6(2), 83–90. https://doi.org/10.47637/LEGALITA.V6I2.1453

Ramos, C., & Hutton, T. (2022). Digital Provenance and Evidentiary Standards for Synthetic Media. Computer Law & Security Review, 46, 105684. https://doi.org/10.1016/j.clsr.2022.105684

Ramos, J., & Hutton, E. (2022). Judicial responses to deepfake evidence: A comparative analysis. International Journal of Law and Information Technology, 30(4), 377–412. https://doi.org/10.1093/ijlit/eaac012

Romero-Moreno, F. (2025). Deepfake detection in generative AI: A legal framework proposal to protect human rights. Computer Law & Security Review, 58, 106162. https://doi.org/10.1016/J.CLSR.2025.106162

Sandoval, M. P., de Almeida Vau, M., Solaas, J., & Rodrigues, L. (2024). Threat of deepfakes to the criminal justice system: a systematic review. Crime Science 2024 13:1, 13(1), 41-. https://doi.org/10.1186/S40163-024-00239-1

Siregar, Z. A., Rafiqi, R., & Sitorus, N. T. (2024). Tinjauan Yuridis Pembuktian Elektronik dalam Perkara Tindak Pidana Penipuan Online. Arbiter, 6(2). https://doi.org/10.31289/arbiter.v6i2.5343

Suryana, D. (2022). Problematika autentikasi bukti digital dalam hukum acara pidana. Fiat Justisia: Jurnal Ilmu Hukum, 16(3), 445–462. https://garuda.kemdikbud.go.id/documents/detail/3054135

Suteki. (2021). Rekonstruksi Hukum di Era Disrupsi Teknologi. Thafa Media.

Syukri, F. (2024). Penggunaan Bukti Digital Dalam Persidangan Pidana: Antara Validitas Dan Keadilan. Causa: Jurnal Hukum dan Kewarganegaraan, 6(6), 51–60. https://doi.org/10.3783/CAUSA.V6I6.6299

Vaccari, C., & Chadwick, A. (2020). Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News. Social Media and Society, 6(1). https://doi.org/10.1177/2056305120903408;Website:Website:Sage;Journal:Journal:Smsa;Issue:Issue:Doi

Verdoliva, L. (2020). Media Forensics and Deepfakes: An Overview. IEEE Journal of Selected Topics in Signal Processing, 14(5), 910–932. https://doi.org/10.1109/JSTSP.2020.3002101

West, D. M., & Farrell, J. (2023). Algorithmic Trust and the Future of Digital Evidence. Harvard Journal of Law & Technology, 36(1), 145–182.

West, S., & Farrell, T. (2023). Deepfakes and evidentiary integrity: Reassessing digital authenticity standards. Harvard Journal of Law & Technology, 36(2), 145–182. https://jolt.law.harvard.edu/

Yuliana, E. (2023). Adaptasi hukum terhadap bukti elektronik di era digital. Jurnal Hukum & Pembangunan, 53(2), 155–172. https://garuda.kemdikbud.go.id/documents/detail/3367120