

Criminal Liability for Deepfake Videos Falsely Depicting Individuals as Criminal Offenders

Teguh Prasetyo*, Indira Hertha Wibowo, Jingga Aura Cinta, Nadia Herdiana Putri, Cecilia Chrysilla Liem

Universitas Pelita Harapan, Indonesia

Email : teguh.prasetyo@uph.edu*, sallyroyaltycrownny@gmail.com,
auracintajingga@gmail.com, herdiananadia05@gmail.com, cecilialiem6@gmail.com

Keywords:

Deepfake Video; Artificial Intelligence; Criminal Liability; Victim Protection; Electronic Evidence

Abstract

Deepfake technology enables the creation of realistic manipulated audiovisual content that falsely portrays individuals as committing criminal acts, threatening personal reputation, privacy, personal data protection, and the integrity of electronic evidence. This normative juridical study examined Indonesia's criminal law framework governing deepfake creation and dissemination, criminal liability among perpetrators, and legal protection for falsely accused individuals. Employing statutory and conceptual approaches, the research reviewed the Electronic Information and Transactions (EIT) Law, particularly Article 35 and its criminal sanctions, the Personal Data Protection Law, relevant Constitutional Court interpretations, academic literature, and illustrative news reports. The findings revealed that Indonesian legislation lacks a specific criminal provision addressing deepfake technology. Consequently, criminal liability depends on fulfilling applicable statutory elements, including unlawful electronic information manipulation or dissemination, criminal intent, the purpose of presenting manipulated content as authentic, and sufficient evidence connecting perpetrators to prohibited conduct. Liability must be assessed individually because creators and disseminators may demonstrate different actions, knowledge, and intentions. Victim protection requires stronger personal data safeguards, restrictions on unlawful content, effective criminal investigations, and digital forensic examinations to verify electronic evidence. Reports involving artificial intelligence-generated sexually explicit deepfakes illustrate technological misuse but cannot replace final judicial decisions or justify criminal liability through analogy. Furthermore, legal enforcement must distinguish technological manipulation from legally established criminal conduct while maintaining evidentiary reliability and procedural fairness. This study proposed an integrated, role-based legal framework to clarify criminal responsibility, strengthen victim protection, and safeguard electronic evidence within Indonesia's evolving digital legal system.



This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.

Copyright © 2026 by Author. Published by
Riviera Publishing

INTRODUCTION

The rapid advancement of artificial intelligence (AI) has transformed the production and dissemination of audiovisual information. Generative AI systems can now synthesize or manipulate faces, voices, gestures, and entire scenes with a degree of realism that blurs the distinction between authentic and fabricated recordings. Deepfake technology represents one manifestation of this advancement, as it can make individuals appear to say or do things that never occurred (Maharani et al., 2025). Consequently, the legal implications extend beyond

misinformation: when synthetic content is presented as an authentic record of an individual's conduct, it can undermine personal identity, reputation, privacy, and the reliability of evidence used in social and legal decision-making. The global significance of this issue stems from the fact that the same technological capabilities can serve legitimate creative purposes or facilitate deception. Accordingly, legal assessments must consider the intent, context, and specific conduct involved rather than merely the use of AI technology.

In Indonesia, this issue is particularly urgent because digital content can spread rapidly among a substantial online population. The Indonesian Internet Service Providers Association reported that Indonesia had 221,563,479 internet users in 2024, representing an internet penetration rate of 79.5% (APJII, 2024). Meanwhile, the Ministry of Communication and Digital Affairs has warned that AI can generate increasingly realistic fabricated content, including synthetic representations of faces and voices, thereby complicating efforts to authenticate photographs, videos, and audio recordings (Komdigi, 2026). These circumstances present two interconnected challenges for criminal law. First, the legal system must provide effective mechanisms for addressing deliberate manipulation that causes harm. Second, it must avoid an overly expansive interpretation that criminalizes all forms of synthetic or edited audiovisual content. Establishing a precise legal framework is particularly important when deepfake videos have the potential to influence public perceptions of whether an individual has committed a criminal offense.

Falsely depicting an individual as a criminal offender presents a distinct legal challenge because the resulting harm may arise even before formal investigations or judicial proceedings commence. A realistic deepfake video may create an immediate impression that the depicted individual has committed violence, theft, fraud, or another criminal act, despite the underlying event never having occurred. Such representations may damage an individual's honor and reputation, compromise personal data, provoke social sanctions, and potentially influence criminal complaints, investigations, or the assessment of electronic evidence. Unlike conventional defamatory statements, deepfake content combines an allegation with an apparently authentic audiovisual recording, potentially increasing its credibility and persuasive impact. Therefore, the central legal question extends beyond establishing the falsity of the content to determining how Indonesian criminal law should classify the creation and dissemination of manipulated audiovisual material, which elements of criminal liability and unlawfulness must be established, and how the legal system can protect individuals from being falsely identified as criminal offenders based on unauthenticated audiovisual evidence (Al Alif et al., 2025; Alghiffary et al., 2026; Azis et al., 2026; McGlynn & Toparlak, 2025; Nurkholisah et al., 2025).

The practical severity of AI-based manipulation is illustrated by reports involving a female student at a state university in Solo whose facial image was allegedly incorporated into pornographic photographs and videos disseminated through social media. The victim reported the incident to the Directorate of Cybercrime Investigation of the Central Java Regional Police, and investigators subsequently identified and detained a suspect who reportedly used AI technology to manipulate the victim's facial image (Haq, 2026; Raihan, 2026; Sanjaya, 2026). This incident illustrates how an individual's facial identity can be appropriated and incorporated into fabricated representations of conduct in which the individual never

participated. Nevertheless, the case must be interpreted cautiously within the present study. The available information originates from news reports concerning an ongoing criminal investigation rather than a final and binding court judgment. Furthermore, the allegedly manipulated material involved pornographic content rather than fabricated audiovisual evidence depicting the victim committing a criminal offense. Accordingly, the incident is relevant as an illustration of technological misuse and investigative practices, but it does not constitute a direct judicial precedent that conclusively addresses the legal questions examined in this study.

Indonesia's existing legal framework contains several provisions potentially applicable to deepfake-related conduct, although it does not expressly establish a distinct criminal offense designated as a "deepfake offense." Law Number 11 of 2008 concerning Electronic Information and Transactions, as most recently amended by Law Number 1 of 2024, regulates the manipulation of Electronic Information and/or Electronic Documents under Article 35. This provision addresses the intentional and unlawful manipulation, creation, alteration, deletion, or destruction of Electronic Information and/or Electronic Documents with the intention that such information or documents be considered authentic data. Article 27A may also apply when electronic content contains allegations that attack an individual's honor or reputation, provided that the specific statutory elements and applicable legal interpretations are satisfied (Sukarta et al., 2025). Furthermore, Law Number 27 of 2022 concerning Personal Data Protection is relevant because facial characteristics used for unique identification may constitute biometric personal data, while unauthorized acquisition, processing, disclosure, creation, or falsification of personal data may entail legal consequences, depending on the applicable statutory provisions and the circumstances of the conduct (Djoen & Thamrun, 2026; Herlina et al., 2026).

Previous studies have examined various aspects of this regulatory framework, although their research objects and analytical perspectives differ. (Djoen & Thamrun, 2026) investigate criminal liability arising from AI-based manipulation of photographs containing pornographic material, whereas (Herlina et al., 2026) examine personal data protection in relation to deepfake technology and voice cloning. (Indriawati, 2026) explores the legal construction of criminal liability for AI-enabled deepfake offenses, while (Rahadian et al., 2026) analyze liability for deepfake content disseminated through social media under the Electronic Information and Transactions (ITE) Law and Indonesian criminal law. Meanwhile, (Maharani et al., 2025) discuss legal protection against the adverse consequences of AI technology more broadly. Collectively, these studies demonstrate that the misuse of deepfake technology intersects with offenses involving electronic information, personal data protection regulations, and broader concerns regarding victims' rights. Nevertheless, differences in their factual circumstances indicate that the elements establishing criminal liability cannot automatically be transferred from one category of deepfake misuse to another without examining the specific conduct, legal object, intent, and consequences associated with each case.

Another critical issue concerns the admissibility, authenticity, and probative value of electronic evidence. Although a visually convincing deepfake may be mistaken for an authentic recording of an actual event, its evidentiary reliability depends on factors such as authenticity, integrity, provenance, and the ability to establish a verifiable connection between the electronic

file, the alleged conduct, and the individuals involved. (Mualfah & Ramadhan, 2021) highlight the importance of digital forensic methods in examining electronic recordings, while the present context requires particular attention to metadata, file provenance, source devices, digital accounts, and technical indicators of audiovisual manipulation. These evidentiary considerations are directly connected to criminal liability because investigators and prosecutors must establish not only whether a video has been manipulated but also who created, altered, uploaded, or redistributed it and the relevant knowledge or intent associated with those actions. This distinction becomes particularly important when the creator and disseminator are different individuals. Merely receiving a manipulated file does not necessarily establish the same degree or form of criminal responsibility as deliberately producing the fabrication. Similarly, individuals who redistribute deepfake content may be subject to different legal assessments depending on the applicable statutory provisions, the circumstances of dissemination, and their proven state of mind.

The research gap identified in the literature reviewed in this manuscript concerns the lack of an integrated legal analysis specifically addressing deepfake videos that falsely portray individuals as criminal offenders. In particular, existing scholarship has not comprehensively examined the distinctions between the criminal liability of creators and disseminators, the legal protection afforded to falsely depicted individuals, and the evidentiary safeguards necessary to prevent fabricated audiovisual content from being accepted as proof of criminal conduct. Previous studies have predominantly addressed pornographic manipulation, misuse of personal data, general criminal liability for deepfake technology, or the dissemination of manipulated content through social media as separate legal issues. Although these contributions provide valuable foundations, they do not fully explain the interaction between fabricated representations of criminal conduct and the risk that realistic synthetic videos may influence public perceptions, investigative decisions, or judicial assessments. Consequently, the identified research gap is primarily substantive and doctrinal rather than merely technological. The fundamental challenge lies in interpreting and coordinating existing criminal law provisions while respecting the principle of legality and avoiding the extension of criminal liability through analogy beyond the elements expressly established by law.

The urgency of this research arises from the simultaneous reputational, personal, and procedural harms associated with deepfake technology. Individuals falsely depicted as criminal offenders may experience damage to their dignity, reputation, and control over their biometric identity, while also facing the possibility that manipulated audiovisual content will be perceived as credible evidence of unlawful conduct. The novelty of this study lies in developing an integrated, role-based framework for assessing criminal liability. Rather than treating all individuals involved in deepfake-related conduct as a homogeneous category of offenders, the proposed framework distinguishes between the creation and dissemination of manipulated content, examines the statutory elements applicable to each role under Indonesian electronic information and personal data protection laws, and integrates these considerations with victim protection and electronic evidence authentication. Furthermore, the study explicitly differentiates investigative news reports from adjudicated court decisions and limits the relevance of pornography-related deepfake cases to factual illustrations. This approach avoids

assuming that criminal provisions governing different forms of misconduct are interchangeable simply because the underlying acts involve similar AI technologies.

Accordingly, this study aims to examine three interconnected legal issues: the criminal law provisions potentially applicable to the creation and dissemination of deepfake videos falsely depicting individuals as criminal offenders; the legal foundations and limitations of criminal liability for the creators and disseminators of such content; and the legal protections available to victims, particularly those concerning personal data, unlawful electronic content, and the authenticity of electronic evidence. The research focuses on doctrinal legal interpretation rather than the generation of new empirical findings. Its theoretical contribution lies in developing an integrated understanding of the relationship between statutory offense elements, differentiated actor roles, and evidentiary authenticity in cases involving AI-generated false representations of criminal conduct. Its practical contribution is to establish a structured analytical framework that can assist investigators, legal practitioners, policymakers, and future researchers in assessing manipulated audiovisual material without presuming an individual's criminal responsibility solely from the apparent content of a recording. Ultimately, the study seeks to strengthen legal accountability for unlawful deepfake-related conduct while safeguarding individuals against false accusations and the risk of being unjustly treated as criminal offenders.

METHOD

This study employed a normative juridical research design using statutory and conceptual approaches to examine the interpretation and application of Indonesian legal provisions governing AI-based audiovisual manipulation. The statutory approach focused on the Electronic Information and Transactions Law, the Personal Data Protection Law, relevant criminal law provisions, and Constitutional Court interpretations. The conceptual approach examined criminal liability, intent, unlawfulness, electronic evidence, personal data protection, victim protection, and the legal distinctions between creators and disseminators of deepfake content.

Legal materials were collected through library research involving primary and secondary legal sources. Primary legal materials included relevant legislation, statutory provisions, and judicial interpretations concerning electronic information manipulation, defamation, personal data protection, and criminal sanctions. Secondary materials comprised scholarly books, peer-reviewed journal articles, and previous studies addressing deepfake technology, AI-based manipulation, criminal liability, digital forensics, and victim protection. Relevant news reports were used exclusively to illustrate investigative circumstances and were distinguished from binding judicial decisions. Materials were selected based on their relevance to the research objectives and their contribution to interpreting applicable legal provisions.

The collected materials were analyzed qualitatively using doctrinal legal analysis. The analysis involved identifying applicable legal provisions, examining the statutory elements of criminal offenses, and assessing their applicability to the creation and dissemination of deepfake videos falsely depicting individuals as criminal offenders. Scholarly perspectives were compared to identify similarities, differences, and limitations in existing legal

interpretations. The analysis also examined the integration of personal data protection, criminal law enforcement, victim protection, and digital forensic verification in addressing manipulated audiovisual evidence. This process provided the basis for determining the scope of criminal liability and the legal safeguards available to individuals falsely represented as criminal offenders

RESULTS AND DISCUSSION

Criminal-Law Regulation of Deepfake Creation and Dissemination

Indonesian criminal law does not currently regulate deepfake as a stand-alone offense defined by the technological method used to generate the content. The legal assessment therefore depends on the form of conduct, the protected legal interest, the purpose of the manipulation, and the consequences produced. In the context examined here, Article 35 of the ITE Law provides the most direct entry point for creation-related conduct because it addresses deliberate and unlawful manipulation, creation, alteration, elimination, or destruction of Electronic Information and/or Electronic Documents with the purpose of making the resulting information or document appear to be authentic data (Bervell et al., 2024). This structure is important because it prevents the technology itself from becoming the object of prohibition. A deepfake created for authorized entertainment, research, parody, or other legitimate purposes cannot automatically be equated with a manipulation designed to deceive others into believing that a fabricated criminal event actually occurred.

The elements of Article 35 must be read cumulatively and connected to the factual role of the alleged actor. For a creator, the relevant conduct is the technical manipulation or creation of electronic information. The prosecution must still establish intentionality, the absence of right or the unlawful character of the act, and the purpose that the manipulated output be regarded as authentic. The existence of an edited video alone does not establish all of these elements. Evidence must show that the accused participated in the manipulation process and that the purpose required by the provision can be inferred from admissible circumstances. The associated criminal sanction under the ITE Law consequently depends on proof of the underlying Article 35 conduct, rather than on the mere visual realism of the output (Ananda & Budianto, 2026; Gunawan, 2026).

Article 27A of the ITE Law may become relevant where a deepfake communicates an accusation that attacks the honor or good name of the depicted person. The Constitutional Court's interpretation discussed by (Sukarta et al., 2025) emphasizes the meaning of an act that degrades honor or reputation. In a false-criminal-offender scenario, the manipulated image may function as the vehicle through which the accusation is conveyed. Even so, application must remain tied to the statutory elements of the provision. It is not sufficient to reason that because a video is harmful or humiliating, every offense protecting honor automatically applies. The content, context of dissemination, identity of the targeted person, and nature of the accusation must be assessed within the specific legal formulation.

The Personal Data Protection Law adds another dimension because a deepfake may use a victim's facial characteristics as biometric data. The manuscript's cited scholarship explains that unauthorized use or falsification of personal data can engage the protection and criminal

provisions of Law Number 27 of 2022 (Djoen & Thamrun, 2026; Herlina et al., 2026; Rizky et al., 2026). In practice, this means that a single deepfake incident can intersect with more than one legal interest: authenticity of electronic information, honor and reputation, and control over personal data. These provisions should not be collapsed into one generalized 'deepfake offense.' Instead, each provision should be applied only when its own elements are independently established, consistent with the legality principle and the prohibition on expanding criminal liability merely by technological analogy.

The dispersed character of the present framework creates both flexibility and uncertainty. It allows existing rules to respond to different harms, but it also requires investigators and courts to identify the precise legal basis for each act. The regulatory gap is therefore not a complete absence of law; it is the absence of a dedicated framework that expressly distinguishes creation, alteration, deceptive presentation, dissemination, biometric misuse, and evidentiary consequences. This finding supports the view that future legal development should prioritize clarity of elements and actor roles rather than simply adding the term 'deepfake' to criminal legislation. A technology-neutral rule can remain effective if it clearly identifies prohibited conduct and the required fault element.

Criminal Liability of Creators and Disseminators

Criminal liability must be individualized according to the conduct and culpability of each participant. The creator is the person who generates or materially manipulates the audiovisual content, while the disseminator is the person who uploads, transmits, republishes, or otherwise makes the content available to others. These roles may be performed by the same person, but they may also be separated. Treating them as a single category would obscure differences in *actus reus*, knowledge, purpose, and evidentiary linkage. Indriawati (2026) and Rahadian et al. (2026) support an element-based approach in which the use of AI does not eliminate ordinary requirements of criminal responsibility.

For the creator, liability under Article 35 of the ITE Law requires evidence of the manipulation process and the required purpose. Relevant digital evidence may include source files, project files, model outputs, metadata, device traces, account records, or communications that connect the accused with the generation or alteration of the content. The fact that a victim's face appears in a fabricated video is not, by itself, proof of who created the manipulation. The evidentiary inquiry must therefore connect the accused to the technical act and establish that the manipulation was performed intentionally and unlawfully so that it would be treated as authentic. This prevents criminal responsibility from resting solely on suspicion arising from the content's appearance.

The disseminator requires a separate assessment. A person who merely receives or views a deepfake is not equivalent to a person who intentionally circulates it. Where the disseminator did not participate in the manipulation, Article 35 cannot simply be assumed to apply in the same manner as it does to the creator; the relevant legal basis must correspond to the act of dissemination and the content or harm involved. Proof should address whether the person actually distributed the file, knew or had the legally relevant state of mind concerning its manipulated character, and fulfilled the elements of the specific provision relied upon. This distinction is particularly important for viral content, where a file may pass through many accounts and users with different levels of knowledge and participation.

The Solo student case provides a useful illustration of how investigators may connect AI manipulation, use of a victim's face, social-media distribution, witness examination, and suspect identification (Haq, 2026; Railhan, 2026; Sanjaya, 2026). However, the reports cited in this manuscript describe an investigation and suspect designation, not a final judicial determination of guilt. They should therefore not be presented as proof that a particular legal interpretation has been confirmed by a court. Moreover, the reported conduct involved pornographic manipulation. The case can demonstrate the technical possibility of attaching a person's identity to fabricated conduct and the kinds of digital evidence that may be investigated, but it cannot be used to extend pornography-specific legal reasoning automatically to a deepfake falsely depicting an unrelated criminal offense.

This limitation is central to the legality analysis. Criminal provisions must be applied to conduct that satisfies their elements, not by analogy from the moral seriousness of another deepfake case. Pornographic manipulation, reputational accusation, biometric-data misuse, and false depiction of criminal conduct may overlap factually, but they protect different legal interests and may require different elements of intent or consequence. The appropriate method is therefore to use prior cases and studies as interpretive context while preserving the distinction between factual analogy and legal equivalence. The role-based framework proposed in this study is designed to make that distinction explicit.

Electronic evidence is the bridge between the legal elements and the attributed actor. Deepfake content should not be treated as self-authenticating merely because it appears realistic. Digital-forensic examination can assist in evaluating metadata, file provenance, editing traces, device associations, and account activity, as illustrated more generally by the forensic approach discussed by (Mualfah & Ramadhan, 2021). In a false-criminal-offender scenario, this verification serves two functions at once: it helps establish whether a manipulation occurred and it protects the falsely depicted person from the risk that fabricated audiovisual content will be mistaken for proof of the underlying criminal event.

Legal Protection for Victims of False Criminal Representation

Victims of deepfake false representation may suffer simultaneous harms to identity, privacy, reputation, and procedural security. The use of a person's face without a lawful basis implicates personal-data protection, especially where the facial image is used as biometric information capable of identifying the individual. The PDP Law therefore provides an important protective layer against unlawful acquisition, use, disclosure, creation, or falsification of personal data under the conditions specified by the statute (Herlina et al., 2026; Rizky et al., 2026). This protection is relevant regardless of whether the manipulated video ultimately leads to a separate prosecution for an electronic-information offense.

Protection must also address the continuing circulation of harmful content. Because digital files can be copied and redistributed rapidly, the victim's loss may increase even after a report has been made. The mechanisms available under the ITE framework for restricting access to unlawful electronic content can therefore function as preventive and restorative measures alongside criminal investigation. In practical terms, effective protection should combine preservation of evidence for law-enforcement purposes with proportionate steps to reduce further dissemination. Removing or restricting access without preserving necessary

forensic material could weaken proof, whereas leaving clearly unlawful content continuously accessible could magnify the victim's harm.

A third protective dimension is procedural. When a deepfake falsely depicts the victim as a criminal offender, authorities and other decision-makers should verify authenticity before treating the video as evidence of the depicted conduct. The victim should not bear the consequences of a visual accusation that has not been technically authenticated. Forensic analysis of metadata, file sources, editing history, and associated devices can help distinguish an original recording from manipulated content (Mualfah & Ramadhan, 2021). This approach protects the integrity of the evidentiary process while preserving the possibility of prosecuting the actual creator or disseminator where the required legal elements are proven.

The investigative reports concerning the Solo student also illustrate why victim protection extends beyond punishment of a suspect. The victim's report initiated an investigative process, but legal protection also requires recognition that the circulating content may not represent reality. In the context of false criminal representation, this recognition becomes especially important because reputational damage can merge with the risk of wrongful suspicion. Public authorities, platforms, and investigators therefore have complementary roles: authorities must assess criminal elements and preserve due process; platforms may be required to respond to unlawful content within the applicable legal framework; and forensic specialists must establish authenticity and attribution without presuming that visual realism equals factual truth.

Taken together, the results indicate that Indonesian law already provides several legal pathways for responding to harmful deepfakes, but their effectiveness depends on careful coordination. Article 35 of the ITE Law addresses manipulation intended to appear authentic; provisions concerning honor may address qualifying accusations; the PDP Law protects biometric and other personal data; and digital-forensic examination supports evidentiary integrity. The main interpretive contribution of this study is that these mechanisms should be organized around the actor's role and the specific legal element at issue. This reduces the risk of both under-enforcement, where harmful manipulation falls between fragmented rules, and over-extension, where criminal liability is imposed merely because AI was used.

The discussion also identifies a policy implication. A future deepfake-specific framework, if considered necessary, should not criminalize synthetic media in general. It should define deceptive or harmful conduct with sufficient precision, distinguish creators from disseminators and other intermediaries, identify the required fault element, provide mechanisms for rapid victim protection and content preservation, and establish standards for authenticating audiovisual evidence. Until such a framework exists, the legality principle requires disciplined use of existing provisions. This approach allows Indonesian law to address serious misuse while protecting legitimate technological uses and reducing the risk that fabricated content itself becomes the basis for unjustified criminal suspicion.

CONCLUSION

This study concludes that Indonesian law does not yet explicitly recognize deepfake-related conduct as a distinct criminal offense; however, harmful uses of deepfake technology may be prosecuted under existing legal provisions when the applicable statutory elements are

satisfied. Article 35 of the Electronic Information and Transactions (ITE) Law provides a legal basis for addressing the intentional and unlawful manipulation of electronic information or documents intended to be perceived as authentic. Meanwhile, provisions concerning defamation and the Personal Data Protection Law may apply depending on the nature of the manipulated content, the unauthorized use of biometric data, and the resulting harm. Criminal liability must be assessed individually, as creators and disseminators of deepfake content cannot automatically be subjected to identical legal responsibility. Each actor's liability depends on establishing the prohibited conduct, the requisite mental element, unlawfulness, and the evidentiary connection required under the applicable legal provisions. Furthermore, effective victim protection requires an integrated legal response involving personal data safeguards, restrictions on unlawful content, investigations of responsible individuals, and digital forensic verification. These measures are essential to preventing manipulated audiovisual material from being misinterpreted as authentic evidence that the depicted individual committed a criminal offense.

The principal finding of this study emphasizes that criminal liability arising from deepfake technology must be determined through a systematic examination of statutory elements and individual roles rather than technological classifications or analogical interpretations alone. Reports concerning the female student in Solo illustrate AI-based identity manipulation and relevant investigative practices. However, because the reported incident involved allegedly manipulated pornographic material and was documented through investigative news reports rather than a final judicial decision, it cannot be regarded as binding legal precedent for cases involving fabricated representations of criminal conduct. This limitation highlights the need for future research incorporating final court decisions, prosecutorial and investigative practices, and comparative legal frameworks to examine how judicial authorities assess criminal intent, dissemination, biometric data misuse, and the authenticity of synthetic audiovisual evidence. Further research should also investigate procedural mechanisms for the timely restriction or removal of unlawful deepfake content while ensuring the preservation of digital forensic evidence and compliance with due process requirements. Such investigations could contribute to a more comprehensive and legally precise framework that strengthens victim protection, ensures accountability for unlawful conduct, and safeguards legitimate uses of synthetic media technology.

FUNDING

This study did not receive any specific funding from governmental institutions, private organizations, or other funding agencies.

CONFLICT OF INTEREST

The authors declare that there are no conflicts of interest related to the conduct of the research, preparation, or publication of this article.

AUTHOR CONTRIBUTION

All authors contributed to the preparation of this article. Teguh Prasetyo, Indira Hertha Wibowo, Jingga Aura Cinta, Nadia Herdiana Putri, and Cecilia Chrysilla Liem contributed to the conceptualization of the study, data collection and analysis, interpretation of the results, manuscript preparation, review, editing, and final approval of the manuscript.

GENERATIVE ARTIFICIAL INTELLIGENCE USAGE STATEMENT

Generative artificial intelligence was used to assist with language refinement, structural revision, and manuscript editing. All legal sources, interpretations, substantive claims, and the final content must be reviewed and approved by the authors, who retain full responsibility for the accuracy and integrity of the manuscript.

REFERENCES

- Al Alif, S. S., Rindiani, A., & Marhayati, C. (2025). Konstruksi Hukum Pidana Dalam Penanggulangan Kejahatan Siber Berbasis Teknologi Deepfake di Indonesia. *Legal Standing: Jurnal Ilmu Hukum*, 9(5), 1169–1183. <https://doi.org/10.24269/lis.v9i5.12406>
- Alghiffary, H. H., Rapik, M., & Wahyudhi, D. (2026). Dalam Pusaran Deepfake Pornografi: Menakar Pertanggungjawaban Pidana Platform Digital. *PAMPAS: Journal of Criminal Law*, 7(1). <https://doi.org/10.22437/pampas.v7i1.53737>
- Ananda, F., & Budianto, R. (2026). Does loan restructuring policy affect credit risk? The case of Indonesian banking firms. *Bilancia: Jurnal Ilmiah Akuntansi*, 10(1), 1–14. <https://doi.org/10.35145/bilancia.v10i1.5807>
- APJII. (2024). *Survei Internet Indonesia 2024*.
- Azis, M. A., Pujiyono, & Putri, R. A. K. (2026). Reconstructing Reliability Standards for Deepfake Detectors as Electronic Evidence in Indonesia's Criminal Justice System. *West Science Law and Human Rights*, 4(3). <https://doi.org/10.58812/wslhr.v4i03.3022>
- Bervell, B., Nyagorme, P., Armah, J. K., Arthur-Nyarko, E., Arkorful, V., & Eduafo Arthur, B. (2024). Modeling the Determinants of Students' Satisfaction and Continuance-Intention Toward a Mathematics and Science Distance Education Program. *SAGE Open*, 14(1). <https://doi.org/10.1177/21582440241234743>
- Djoen, T. M., & Thamrun, J. (2026). Pertanggungjawaban Pidana atas Manipulasi Foto Berbasis Kecerdasan Buatan (AI) Bermuatan Pornografi dalam Hukum Pidana Indonesia. *JIHHP (Jurnal Ilmu Hukum, Humaniora Dan Politik)*, 6(5), 3472–3482.
- Gunawan. (2026). Limitasi Normatif Pertanggungjawaban Pidana atas Penyalahgunaan Deepfake Berbasis Artificial Intelligence di Indonesia. *JIHHP (Jurnal Ilmu Hukum, Humaniora Dan Politik)*, 6(5), 3929–3936.
- Haq, A. Z. U. (2026). Mahasiswi di Solo Jadi Objek Deepfake AI Porno, Korban Lapor Polisi. *Detik News*.
- Herlina, L., Arfiani, N., & Sumampouw, W. (2026). Tinjauan Yuridis Perlindungan Data Pribadi Atas Deepfake dan Voice Cloning Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 4(4), 20641–20655.
- Indriawati, S. E. (2026). Konstruksi Pertanggungjawaban Pidana atas Pemanfaatan Kecerdasan Buatan dalam Tindak Pidana Berbasis Deepfake. *Judge: Jurnal Hukum*, 6(10), 1933–1943.
- Maharani, B. A., Rahajeng, H. A., Triana, & Arianti, Z. D. (2025). Perlindungan Hukum Masyarakat dari Dampak Negatif Penggunaan AI. *Media Hukum Indonesia (MHI)*, 3(2), 666–673.

- McGlynn, C., & Toparlak, R. T. (2025). The “new voyeurism”: Criminalizing the creation of “deepfake porn.” *Journal of Law and Society*, 52(2), 204–228. <https://doi.org/10.1111/jols.12527>
- Mualfah, D., & Ramadhan, R. A. (2021). Analisis Digital Forensik Rekaman Kamera CCTV Menggunakan Metode NIST (National Institute of Standards Technology). *IT Journal Research and Development (ITJRD)*, 5(2), 171–182.
- Nurkholisah, S., Risma, D., Nugroho, A. E., Munjiyah, A., & Ayunisa, Q. (2025). Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan Kriminalisasi Dalam Hukum Pidana Indonesia. *Jurnal USM Law Review*, 8(3), 2421–2445. <https://doi.org/10.26623/julr.v8i3.13060>
- Rahadian, R., Sadjat, R. M. E. M., & Pratama, R. I. (2026). Konstruksi Pertanggungjawaban Pidana terhadap Konten Deepfake di Media Sosial Berdasarkan UU ITE dan Hukum Pidana Indonesia. *Jurnal Tana Mana*, 7(2).
- Raihan, A. (2026). Mahasiswi di Solo Jadi Korban Pornografi Deepfake AI, Konten Disebar di Medsos. *Kumparan News*. <https://kumparan.com/kumparannews/mahasiswi-di-solo-jadi-korban-pornografi-deepfake-ai-konten-disebar-di-medsos-27s5G7fB2Km/full>
- Rizky, M., Apriyani, R., & Aripkhan, N. (2026). Perlindungan Hukum dan Kepastian Hukum Terhadap Perdagangan Data Pribadi dalam UU PDP. *Desentralisasi: Jurnal Hukum, Kebijakan Publik, Dan Pemerintahan*, 3(1).
- Sanjaya, Y. C. A. (2026). Motif Mahasiswa Semarang Bikin Deepfake AI Wajah Mantan, Terancam 12 Tahun Penjara. *Kompas Regional*. <https://regional.kompas.com/read/2026/08/07/133400678/motif-mahasiswa-semarang-bikin-deepfake-ai-wajah-mantan-terancam-12-tahun?page=all>
- Sukarta, D. T. W., Akbar, M. G. G., & Abas, M. (2025). Akibat Hukum Pasca Putusan Mahkamah Konstitusi Tentang Kerusakan dalam Ruang Siber Bukan Sebagai Tindak Pidana (Studi Putusan Nomor 105/PUU-XXII/2024). *JIHHP (Jurnal Ilmu Hukum, Humaniora Dan Politik)*, 6(1), 306–315.