Vifada Assumption Journal of Law, E-ISSN 2987-1263
This work is Licensed under a Creative Commons Attribution 4.0 International License

Criminal Legal Protection for Victims of AI-Based Deepfake Content in Indonesia

Irwan Sapta Putra [(1*)] *Arman Maulana* [(2)] *Yunawati Karlina* [(3)]

[(1,2)] *Faculty of Law, Universitas Bina Bangsa, Banten, Indonesia*
[(3)] *Faculty of Law, Universitas Dharma Indonesia, Banten, Indonesia*

Received: 2026, 01, 09 **Accepted:** 2026, 06, 24
Available online: 2026, 06, 29

*Corresponding author.
E-mail addresses: Irwansp.law@gmail.com

KEYWORDS

Keywords:
Deepfake; Criminal law; Artificial intelligence; Legal Protection; Telematics.

Conflict of Interest Statement:
.

Copyright © 2026 Vifada Assumption Journal of Law. All rights reserved.

ABSTRACT

Purpose: This study examines criminal legal protection for victims of AI-based deepfake content in Indonesia and evaluates the adequacy of criminal law and telematics law in responding to manipulation, distribution, and victim harm.

Research Design and Methodology: This research uses normative legal research with statutory, conceptual, and comparative approaches. The primary legal materials include the Criminal Code, the ITE Law, the Personal Data Protection Law, and the Criminal Acts of Sexual Violence Law, supported by legal literature, journal articles, and comparative regulatory materials.

Findings and Discussion: The findings show that victim protection remains partial because Indonesian law has not specifically regulated the creation, manipulation, and distribution of deepfake content as an independent criminal offense. Existing provisions only address unlawful electronic content, defamation, sexual violence, and personal data misuse, but they do not fully regulate AI-based manipulation, digital evidence, or platform responsibility.

Implications: This article contributes to criminal law reform by strengthening deepfake regulation, victim recovery, platform accountability, expedited takedown procedures, and digital evidence standards for future sui generis regulation in Indonesia.

Introduction

The development of artificial intelligence (AI) technology has given rise to innovations that not only provide benefits but also open up new opportunities for crime in the digital space. One of the most concerning products from a legal perspective is deepfakes, a content manipulation technique based on the Generative Adversarial Network (GAN) algorithm that can produce synthetic images, audio, and video that resemble a person's face and voice very convincingly. This high level of manipulation capability makes deepfakes a serious threat to individual dignity, privacy, and security, especially in the context of Indonesia, which has more than 212 million active internet users, allowing for the massive spread of deepfake content.[1] Recent cases in Indonesia show that AI-based deepfake content has been misused for impersonation, fraud, defamation, and non-consensual sexual manipulation, causing psychological, social, and economic harm to victims.

Recent cases in Indonesia show that AI-based deepfake content has been misused for impersonation, fraud, defamation, and non-consensual sexual manipulation, causing psychological, social, and economic harm to victims. Empirical evidence reinforces this concern: the State of Deepfakes 2024 report noted that 96% of circulating deepfake content is non consensual pornography,

[1] Marie-Helen Maras and Alex Alexandrou, "Determining Authenticity of Video Evidence In The Age of Artificial Intelligence And In The Wake of Deepfake Videos," *The International Journal of Evidence & Proof* 23, no. 3 (July 28, 2019): 255–62, https://doi.org/10.1177/1365712718807226.

with the majority of victims being women.[2,3] In Indonesia itself, similar cases continue to emerge, from deepfake videos impersonating President Prabowo Subianto for a fictitious social assistance scam,[4] to the distribution of immoral content based on facial manipulation that harmed students at Udayana University and Semarang University in 2025, with psychological, social, and economic impacts for the victims.[5] These developments show that deepfake misuse is not only a technological problem, but also a legal problem that requires clear criminal norms, effective victim protection, and reliable mechanisms for verifying manipulated digital content.

Ironically, amidst these escalating threats, Indonesian positive law has not provided adequate protection for victims. Law Number 1 of 2024 concerning the Second Amendment to the ITE Law does regulate the dissemination of immoral content (Article 27 paragraph 1) and electronic defamation (Article 27A),[6] but does not explicitly criminalize AI-based content manipulation. Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) also only regulates data falsification in general, without addressing the technical characteristics of deepfakes, which synthesize rather than steal someone's data.[7] Even the new Criminal Code based on Law Number 1 of 2023, which came into effect in January 2026, does not contain a specific article on deepfake crimes, but only covers conventional fraud in Article 492.[8] This regulatory gap creates uncertainty in determining the criminal act, identifying the responsible legal subject, proving AI-based manipulation, and ensuring effective recovery for victims. Therefore, the main issue is not only the absence of a specific deepfake offense, but also the limited capacity of existing criminal law and telematics law to provide preventive protection, repressive protection, and legal certainty for victims. This situation creates a clear legal vacuum (*rechtsvacuum*) and stands in stark contrast to the European Union's approach through the AI Act 2024, which explicitly regulates high-risk AI systems, including deepfake technology, within a measurable legal accountability framework.[9]

Several previous studies have attempted to map this problem, but each still leaves gaps that need to be filled. Boleng and Rohman (2025) examine the gap in deepfake regulation limited to the perspective of gender-based violence,[10] Prayoga and Tuasikal (2025) analyze its law enforcement without addressing the cross-jurisdictional dimension,[11] Van Der Sloot and Wagensveld (2022) offer a comprehensive regulatory framework but from a European legal context,[12] while Zaltina and Nurtjahyo (2024) focus more on the rights of post-crime victims than on the material criminal construction.[13] Previous studies have discussed deepfake crimes from the perspectives of gender-based violence, law enforcement, victim rights, and comparative regulation, but they have not sufficiently integrated criminal law protection, telematics law, platform accountability, and digital

[2] Arief Wibowo, Yehu Wangsajaya, and Asep Surahmat, *Pemolisian Digital Dengan Artificial Intelligence* (PT. RajaGrafindo Persada-Rajawali Pers, 2023). hlm. 45–47.
[3] Mateusz Łabuz and Sławomir Soczyński, "Deep Fakes As a Tool of Political Advertising. Can Regulatory Framework Benefit From The 'Ship of Theseus' Paradox?," *Technology in Society* 84 (March 2026): 103060, https://doi.org/10.1016/j.techsoc.2025.103060.
[4] Yoan Shevila Kristiyenda, Jasmine Faradila, and Christina Basanova, "Pencegahan Kejahatan Deepfake : Studi Kasus Terhadap Modus Penipuan Deepfake Prabowo Subianto Dalam Tawaran Bantuan Uang," *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora* 3, no. 2 (March 4, 2025): 149–64, https://doi.org/10.59246/aladalah.v3i2.1263.
[5] Theodora Kristina Boleng and Adi Nur Rohman, "Regulatory Gaps and Legal Enforcement Challenges on Deepfake Pornography as a Form of Digital Sexual Violence in Indonesia," *Al-Zayn : Jurnal Ilmu Sosial & Hukum* 3, no. 6 SE-Articles (December 9, 2025): 10068–80, https://doi.org/10.61104/alz.v3i6.2714.
[6] Lastri Riyanti, Lamijan, and Muhammad Zainudin, "Legal Reform on Network Security and Cybercrime in Information and Electronic Transaction Law," *Greenation International Journal of Law and Social Sciences* 3, no. 3 (November 22, 2025): 1216–23, https://doi.org/10.38035/gijlss.v3i3.610.
[7] Rista Maharani and Andria Luhur Prakoso, "Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital," *JURNAL USM LAW REVIEW* 7, no. 1 (March 29, 2024): 333–47, https://doi.org/10.26623/julr.v7i1.8705.
[8] Ruben Nicholas Alfredo Tobing and Yuliana Yuli, "Criminal Liability for the Creation and Distribution of Deepfake Pornographic Videos on Social Media," *Eduvest - Journal of Universal Studies* 6, no. 2 (February 6, 2026): 1302–14, https://doi.org/10.59188/eduvest.v6i2.52738.
[9] Valentine Ugwuoke and Madelyn Rose Sanfilippo, "The Current Landscape of Deepfake Legislation in the United States," *Journal of Information Policy* 15 (June 30, 2025): 97–129, https://doi.org/10.5325/jinfopoli.15.2025.0004.
[10] Theodora Kristina Boleng and Adi Nur Rohman, "Regulatory Gaps and Legal Enforcement Challenges on Deepfake Pornography as a Form of Digital Sexual Violence in Indonesia."
[11] Hendra Prayoga and Hadi Tuasikal, "Penyebaran Konten Deepfake Sebagai Tindak Pidana: Analisis Kritis Terhadap Penegakan Hukum Dan Perlindungan Publik Di Indonesia," *Abdurrauf Law and Sharia* 2, no. 1 (May 1, 2025): 22–38, https://doi.org/10.70742/arlash.v2i1.194.
[12] Bart van der Sloot and Yvette Wagensveld, "Deepfakes: Regulatory Challenges for The Synthetic Society," *Computer Law & Security Review* 46 (September 2022): 105716, https://doi.org/10.1016/j.clsr.2022.105716.
[13] Putri Zaltina and Lidwina Inge Nurtjahyo, "Right to Be Forgotten as a Legal Protection for The Victims of Electronic Sexual Violence Cases," *The Indonesian Journal of Socio-Legal Studies* 3, no. 2 (2024), https://doi.org/10.54828/ijsls.2024v3n2.4.

evidence standards in the Indonesian legal context. Although these studies are relevant, their focus remains partial because they have not yet placed victim protection, digital evidence, platform responsibility, and criminal liability within one integrated framework for Indonesian law. From this gap, this study presents a novelty in the form of a simultaneous integration of criminal law and telematics law approaches,[14] a model of criminal liability for three legal subjects at once: individual perpetrators, platform developers, and electronic system operators,[15] as well as a comparative study towards the urgency of sui generis regulation of deepfake crimes in Indonesia.[16] Therefore, this article specifically examines how Indonesian criminal law and telematics law protect victims of AI-based deepfake content and how criminal liability should be reconstructed through a layered model supported by sui generis regulation. This focus provides the basis for formulating the research questions on the adequacy of existing legal protection and the reconstruction of criminal liability for AI-based deepfake crimes in Indonesia.

Literature Review

Deepfake Technology and Artificial Intelligence

Deepfake technology is a form of artificial intelligence-based content manipulation that enables the creation of synthetic audio, images, and videos resembling real persons. Its development is closely related to generative artificial intelligence, especially the use of algorithmic systems capable of learning facial expressions, voice patterns, and visual identity.[17] In legal discourse, this technology is not merely a technical innovation but also a new instrument that can be misused to violate personal dignity, privacy, and security.

The main characteristic of deepfake technology is its ability to blur the distinction between authentic and manipulated digital content. This creates difficulty for victims, law enforcement officers, and courts when determining whether a video, image, or voice recording represents a real event or an artificial construction.[18] Maras and Alexandrou emphasize that artificial intelligence has changed the way authenticity of digital evidence must be examined in legal proceedings.[19]

The literature also shows that deepfake misuse can appear in several forms, including non-consensual sexual content, defamation, fraud, political manipulation, identity misuse, and blackmail. These harms demonstrate that deepfake crimes do not only attack reputation but may also affect psychological integrity, social standing, economic interests, and public trust in electronic information.[20] Therefore, the legal response to deepfake cannot rely only on conventional criminal provisions.

From the perspective of legal development, artificial intelligence-based deepfake content requires a regulatory approach that understands both the technological process and the legal harm. The creation, modification, distribution, and amplification of synthetic content must be examined as

[14] Soetardi Tri Cahyono, Wina Erni, and Taufik Hidayat, "Rekonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia," *Dame Journal of Law* 1, no. 1 (March 15, 2025): 1–23, https://doi.org/10.64344/djl.v1i1.6.
[15] Asri Gresmelian Eurike Hailtik and Wiwik Afifah, "Criminal Responsibility of Artificial Intelligence Committing Deepfake Crimes in Indonesia," *Asian Journal of Social and Humanities* 2, no. 4 (January 22, 2024): 776–95, https://doi.org/10.59888/ajosh.v2i4.222.
[16] Ni Kadek Dwi Ika Ardiyani, "Analisis Yuridis Pertanggungjawaban Pidana Pelaku Deepfake Porn Berdasarkan Hukum Positif," *Jurnal Kajian Hukum Dan Kebijakan Publik | E-ISSN : 3031-8882* 2, no. 3 (November 21, 2024): 603–8, https://doi.org/10.62379/cs863250.
[17] Leonardo Banh and Gero Strobel, "Generative Artificial Intelligence," *Electronic Markets* 33, no. 1 (December 6, 2023): 63, https://doi.org/10.1007/s12525-023-00680-1.
[18] Thanh Thi Nguyen et al., "Deep Learning for Deepfakes Creation and Detection: A Survey," *Computer Vision and Image Understanding* 223 (October 2022): 103525, https://doi.org/10.1016/j.cviu.2022.103525.
[19] Maura Grossman and Paul Grimm, "Judicial Approaches to Acknowledged and Unacknowledged AI-Generated Evidence," *Science and Technology Law Review* 26, no. 2 (May 23, 2025), https://doi.org/10.52214/stlr.v26i2.13890.
[20] Jennifer Laffier and Aalyia Rehman, "Deepfakes and Harm to Women," *Journal of Digital Life and Learning* 3, no. 1 (June 24, 2023): 1–21, https://doi.org/10.51357/jdll.v3i1.218.

connected stages of unlawful conduct.[21] This understanding becomes important before determining criminal liability and victim protection mechanisms.

Criminal Law Protection for Victims of Deepfake Crimes

The technological characteristics of deepfake therefore provide the starting point for examining criminal law protection, because the harm caused by synthetic content cannot be separated from the need to protect victims from manipulation, distribution, and continuing digital exposure. Criminal law protection for victims of deepfake crimes must be understood through preventive and repressive protection. Preventive protection requires clear criminal norms that prohibit harmful conduct before it causes wider damage. Repressive protection requires effective sanctions, restitution, content removal, restoration of reputation, and protection of the victim during the legal process.[22]

In the Indonesian context, existing criminal law instruments still provide partial protection for victims. Law Number 1 of 2024 on Electronic Information and Transactions may be used for immoral electronic content and electronic defamation, while Law Number 12 of 2022 on Criminal Acts of Sexual Violence may reach electronic-based sexual violence.[23] However, these instruments do not yet expressly regulate artificial intelligence-based deepfake creation and distribution as independent criminal conduct.

The absence of a specific formulation creates problems for the principles of lex certa and nullum crimen sine lege. Criminal law requires a clear, precise, and measurable formulation of prohibited conduct so that law enforcement does not depend excessively on broad interpretation. In deepfake cases, unclear norms may weaken proof, create inconsistent legal application, and reduce legal certainty for victims.[24]

Previous studies on deepfake crimes have discussed law enforcement, gender-based violence, and victim protection, but the literature still shows a need for a more integrated criminal law framework. Such a framework should not only punish the person who distributes harmful content but also examine the act of creating, facilitating, and maintaining access to unlawful synthetic content.[25] This is the conceptual basis for reconstructing criminal liability in deepfake cases. Since deepfake crimes are committed, stored, and disseminated through electronic systems, criminal law protection must be supported by telematics law and reliable electronic evidence standards.

Telematics Law and Electronic Evidence

Telematics law is relevant because deepfake crimes occur through electronic systems, digital platforms, and information technology infrastructure. The distribution of deepfake content is not only a conventional criminal act committed through the internet. It is a cybercrime that depends on digital systems as the main medium for producing, storing, transmitting, and multiplying unlawful content.[26]

Law Number 1 of 2024 on Electronic Information and Transactions provides a basic legal framework for electronic information, electronic documents, and electronic system responsibility. In deepfake cases, this framework is important because the object of the offense is usually electronic

[21] Raphael Ramos Monteiro de Souza, "Legal Remedies and Regulatory Frameworks to Combat Ai-Driven Deepfakes," in *Mitigating the Risks of AI Deepfakes* (CRC Press, 2026), 94–116.
[22] Gunsu Nurmansyah, Rudi Natamiharja, and Ikhsan Setiawan, "Legal Protection of Personal Data Against Phishing in Indonesia: A Pancasila-Based Approach," *Pancasila and Law Review* 6, no. 1 (August 25, 2025): 15–44, https://doi.org/10.25041/plr.v6i1.4138.
[23] Alip Rahman et al., "Legal Protection for Victims of Online Gender-Based Violence (Cyber-Based Violence)," *Edunity Kajian Ilmu Sosial Dan Pendidikan* 3, no. 12 (December 25, 2024): 1210–20, https://doi.org/10.57096/edunity.v3i12.350.
[24] Shalu Mehta and Prof.(Dr.) Venoo Rajpurohit, "Legal Gaps in Deepfake Misuse & Strengthening Cybercrime Criminalization," *Lex Localis - Journal of Local Self-Government*, November 15, 2024, 536–48, https://doi.org/10.52152/803278.
[25] Furizal et al., "Social, Legal, and Ethical Implications of AI-Generated Deepfake Pornography on Digital Platforms: A Systematic Literature Review," *Social Sciences & Humanities Open* 12 (2025): 101882, https://doi.org/10.1016/j.ssaho.2025.101882.
[26] Anisa Rahayu and Kuswandi, "The Deepfake Phenomenon as a New Form of Cybercrime from a Criminological Perspective," *Indonesian Journal of Law and Justice* 3, no. 2 (December 13, 2025): 14, https://doi.org/10.47134/ijlj.v3i2.5171.

content that must be identified, preserved, verified, and presented as legal evidence.[27] Therefore, electronic evidence standards become central to proving AI-based manipulation.

The literature on digital evidence emphasizes the importance of authenticity, integrity, and reliability. In deepfake cases, these evidentiary standards are more complex because the content may appear visually convincing but may not represent a real event. Digital forensic examination and expert testimony are therefore needed to explain whether the disputed content has been manipulated by artificial intelligence.[28]

The telematics law perspective also raises the issue of electronic system operators. Platforms that host or distribute reported deepfake content may have legal responsibility when they fail to respond to valid victim reports or fail to implement reasonable content moderation mechanisms.[29] This issue connects electronic evidence, victim protection, and platform accountability in one legal framework. The evidentiary issue also leads to personal data protection and platform liability, because deepfake content commonly uses a victim's face, voice, image, or biometric identity and spreads through digital platforms that control access to the harmful content.

Personal Data Protection and Platform Liability

Personal data protection is closely related to deepfake because synthetic content often uses a person's face, voice, image, or biometric identity. Law Number 27 of 2022 on Personal Data Protection recognizes personal data protection as an important legal interest.[30] However, deepfake technology creates a specific challenge because it may synthesize identity elements without directly taking or transferring the victim's original data.

This situation creates a grey area in the application of personal data protection norms. If the law focuses only on conventional collection, use, or transfer of personal data, it may not fully capture artificial intelligence-based manipulation that reconstructs a person's identity.[31] For this reason, personal data protection must be read together with criminal law and telematics law.

Platform liability is also important because deepfake content usually spreads through digital platforms, social media, messaging systems, and content sharing services. Liability should not automatically be imposed on every platform, but it must be considered when the platform has knowledge of unlawful content and fails to take reasonable action.[32] This approach is consistent with the principle of fault in criminal law.

The literature on corporate criminal liability provides a basis for examining developers, providers, and electronic system operators in deepfake cases. Application developers may be examined when the technology is designed or intentionally facilitated for unlawful manipulation. Electronic system operators may be examined when they knowingly allow unlawful content to remain accessible after receiving a valid victim report from the victim. These limitations in personal data protection and platform accountability show the need to examine comparative regulatory models that may guide the formulation of a more specific legal framework for deepfake crimes in Indonesia.

[27] Felipe Romero-Moreno, "Deepfake Detection in Generative AI: A Legal Framework Proposal to Protect Human Rights," *Computer Law & Security Review* 58 (September 2025): 106162, https://doi.org/10.1016/j.clsr.2025.106162.
[28] Ebrima Hydara, Masato Kikuchi, and Tadachika Ozono, "Empirical Assessment of Deepfake Detection: Advancing Judicial Evidence Verification Through Artificial Intelligence," *IEEE Access* 12 (2024): 151188–203, https://doi.org/10.1109/ACCESS.2024.3480320.
[29] Mekhail Mustak et al., "Deepfakes: Deceptions, Mitigations, and Opportunities," *Journal of Business Research* 154 (January 2023): 113368, https://doi.org/10.1016/j.jbusres.2022.113368.
[30] Nina Purwanti, Megawati Barthos, and Tri Eka Saputra, "The Role of Artificial Intelligence in the Implementation of Personal Data Protection Law in Indonesia," *Interdiciplinary Journal and Hummanity (INJURITY)* 4, no. 6 (June 20, 2025): 325–36, https://doi.org/10.58631/injurity.v4i6.1448.
[31] Ben Chester Cheong, "Transparency and Accountability in AI Systems: Safeguarding Wellbeing in the Age of Algorithmic Decision-Making," *Frontiers in Human Dynamics* 6 (July 3, 2024), https://doi.org/10.3389/fhumd.2024.1421273.
[32] Miriam C Buiten, Alexandre de Streel, and and Martin Peitz, "Rethinking Liability Rules for Online Hosting Platforms," *International Journal of Law and Information Technology* 28, no. 2 (March 1, 2020): 139–66, https://doi.org/10.1093/ijlit/eaaa012.

Comparative Regulation and the Need for Sui Generis Regulation

Comparative regulation is useful to show that deepfake crimes require a more specific legal response. The European Union AI Act provides an important reference because it introduces a risk-based approach to artificial intelligence regulation.[33] This approach shows that AI systems should be regulated according to the level of risk they create for rights, safety, and public interests.

The relevance of the EU AI Act for Indonesia lies not in copying the entire regulatory model, but in adopting its regulatory logic. Deepfake regulation should define synthetic content, determine prohibited conduct, establish transparency duties, and create accountability mechanisms for actors involved in the production and distribution chain.[34] These elements may strengthen legal certainty and victim protection.

Other comparative experiences also show that legal systems increasingly recognize the need to regulate manipulated digital content more directly. The literature on China and Singapore indicates that state responses to false or manipulated online content may include labeling obligations, content control mechanisms, and sanctions.[35] These comparisons may be used carefully as references for Indonesian legal reform.

Based on these themes, the literature supports the need for sui generis regulation on deepfake crimes in Indonesia. Such regulation should include a clear definition of deepfake, classification of harms, liability of individual perpetrators, responsibility of developers and electronic system operators, expedited takedown procedures, restitution, victim identity protection, and digital evidence standards. Taken together, these strands of literature show that deepfake crimes must be examined through an integrated framework that connects technology, victim protection, criminal liability, electronic evidence, personal data protection, platform responsibility, and comparative regulation as the conceptual basis for the research method and legal analysis.

Research Design and Methodology

This research uses normative legal research. The primary legal materials consist of the Criminal Code, Law Number 1 of 2024 on Electronic Information and Transactions, Law Number 27 of 2022 on Personal Data Protection, and Law Number 12 of 2022 on Criminal Acts of Sexual Violence. Secondary and comparative legal materials include books, journal articles, previous legal studies, and foreign or international regulatory instruments, particularly the EU AI Act 2024, which support the analysis of deepfake crimes and the formulation of sui generis regulation in Indonesia.

This study applies statutory, conceptual, and comparative approaches. The statutory approach examines the scope and limits of Indonesian criminal law and telematics law in protecting victims of AI-based deepfake content. The conceptual approach analyzes legal protection, criminal liability, victim recovery, electronic evidence, lex certa, and nullum crimen sine lege. The comparative approach assesses foreign regulatory models, especially the EU AI Act, as a reference for developing sui generis regulation in Indonesia.

The legal materials are analyzed through legal interpretation, legal systematization, and legal argumentation. These techniques are used to interpret relevant legal norms, systematize the relationship between Indonesian criminal law, telematics law, and comparative materials, identify normative gaps, and formulate a layered model of criminal liability for AI-based deepfake crimes.

Through this method, the research evaluates the adequacy of existing legal instruments, identifies the limits of victim protection, and formulates a more precise criminal law policy for deepfake crimes in Indonesia.

[33] Ugwuoke and Sanfilippo, "The Current Landscape of Deepfake Legislation in the United States."
[34] Hrishikesh Yadav and Jay Oza, "The DeepFake Dilemma: Balancing Innovation, Ethics, and Accountability Through Law," September 9, 2025, https://doi.org/10.36227/techrxiv.175744943.37338204/v1.
[35] Michal Lavi, "Publish, Share, Re-Tweet, and Repeat," *University of Michigan Journal of Law Reform*, no. 54.2 (2021): 441, https://doi.org/10.36646/mjlr.54.2.publish.

Findings and Discussion

Indonesian Criminal Law and Telematics Law Regulations in Providing Legal Protection for Victims of the Distribution of Artificial Intelligence-Based Deepfake Content

Legal protection for victims of deepfake crimes in Indonesian positive legal system is still essentially based on a number of general normative instruments that are not specifically designed to address the technical characteristics of artificial intelligence-based crimes. For this reason, victim protection must be analyzed through each legal instrument. The ITE Law regulates unlawful electronic content, the TPKS Law addresses electronic-based sexual violence, the PDP Law protects personal and biometric data, and the Criminal Code covers conventional offenses connected to deepfake misuse. The main instrument used by law enforcement is Law Number 1 of 2024 concerning the Second Amendment to the ITE Law. Article 27 paragraph (1) prohibits the distribution of electronic content that violates morality, while Article 27A regulates attacks on honor or defamation through electronic systems.[36]

Normatively, both articles can be applied to pornographic deepfakes and defamatory deepfakes. However, they do not contain a technical definition of AI-based content manipulation. This weakness makes the proof of "intentionally and without rights" highly dependent on digital forensic capacity.[37] For victim protection, the ITE Law provides a basis for reporting and prosecuting immoral or defamatory deepfake content. Its protection remains limited because it focuses on unlawful distribution, not on the creation or manipulation of synthetic content through artificial intelligence. On the other hand, Law Number 12 of 2022 concerning Criminal Acts of Sexual Violence (UU TPKS) provides an important breakthrough through Article 14, which criminalizes electronic-based sexual violence, including the distribution of non-consensual sexual content, which can substantially reach the practice of deepfake pornography. The relevance of the TPKS Law lies in its ability to recognize non-consensual electronic sexual content as a form of victimization, so that victims may obtain protection, reporting mechanisms, and recovery rights, although its application to deepfake pornography still requires proof that the manipulated content was distributed without consent and caused sexual harm.

However, the implementation of the TPKS Law faces serious obstacles because the implementing regulations required to regulate the mechanism for content deletion (right to erasure) and victim recovery have not been fully issued, thus creating a gap between norms and law enforcement practices in the field.[38]

Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) is theoretically relevant when deepfakes are used to process a person's biometric data without consent, as stipulated in Article 4 in conjunction with Article 20 of the PDP Law. However, deepfake technology, which synthesizes rather than steals a person's facial data, places it in a gray area not explicitly covered by the law's definition of "personal data processing."[39] From the victim protection perspective, the PDP Law is relevant because deepfake content may manipulate a person's face, voice, or biometric identity. However, the law has not clearly determined whether AI-based synthesis of identity elements constitutes unlawful personal data processing. The Criminal Code may also be relevant when deepfake content is used as an instrument of fraud, threats, or reputational attack, but its provisions remain conventional because they do not specifically address the technical act of AI-based manipulation, the digital nature of the evidence, or the rapid circulation of synthetic content.

From the perspective of criminal law principles, this condition is contrary to the principle of lex certa which requires the formulation of criminal norms to be clear, firm, and measurable, as well as the principle of nullum crimen sine lege which requires every criminal act to have an explicit legal

[36] Ridwan Ridwan, Ainun Wulandari, and Syamsuddin, "Metaverse Regulation Formulation In Indonesian Cyber Law," *Law and Justice* 7, no. 2 (February 9, 2023): 143–52, https://doi.org/10.23917/laj.v7i2.757.
[37] Siti Nurkholisah et al., "Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan Kriminalisasi Dalam Hukum Pidana Indonesia," *JURNAL USM LAW REVIEW* 8, no. 3 (December 17, 2025): 2421–45, https://doi.org/10.26623/julr.v8i3.13060.
[38] Theodora Kristina Boleng and Adi Nur Rohman, "Regulatory Gaps and Legal Enforcement Challenges on Deepfake Pornography as a Form of Digital Sexual Violence in Indonesia."
[39] Nurkholisah et al., "Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan Kriminalisasi Dalam Hukum Pidana Indonesia."

basis before a person can be punished.[40] In deepfake cases, the absence of a specific criminal formulation affects both legality and evidence. Investigators and judges must first prove that the disputed electronic content results from AI-based manipulation before linking it to the elements of an existing offense. A study of 15 court decisions for the 2023–2025 period shows that judges tend to use Article 27 paragraph (1) of the ITE Law as the mainstay article with an extensive interpretation construction, but the inconsistency of decisions between courts reflects that without a standard technical definition of deepfake in the law, legal certainty for victims remains uncertain.

From a telematics law perspective, the distribution of deepfake content cannot be viewed merely as a conventional crime that occurs incidentally in digital media, but rather as a cybercrime that inherently utilizes information technology infrastructure as its primary means (instrumentum sceleris). Article 15 in conjunction with Article 16 of the ITE Law requires every electronic system operator to operate reliably, securely, and responsibly, including ensuring that content circulated through its platform does not violate the law. This obligation opens up legal liability for digital platform providers if they are proven negligent in detecting and removing deepfake content reported by victims, although in practice, the notice and takedown mechanism stipulated in Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions is still ineffective due to the lack of technical standards for AI-based content verification.[41] Electronic system operators may be held accountable when they receive a valid victim report and have the technical capacity to restrict or remove the content. Liability may arise if they fail to take reasonable and timely action, allowing harmful deepfake content to remain accessible.

The South Jakarta District Court Decision Number 20/Pdt.Sus-Siber/2024 and the Surabaya District Court Decision Number 8/Pdt.Sus-Siber/2024 are developments in jurisprudence that are worth observing, where the panel of judges in both cases began to consider digital evidence resulting from AI engineering as valid evidence in accordance with Article 5 of the ITE Law, while emphasizing the importance of digital forensic expert testimony to prove the authenticity or falsity of the content that is the object of the case.[42]

At the cassation level, Supreme Court Decision Number 789 K/Pid.Sus/2025 further strengthens this jurisprudence by emphasizing that the absence of specific deepfake regulations does not hinder the application of existing laws, as long as the interpretation is carried out systematically and teleologically to protect the interests of victims, an approach that is in line with the spirit of Constitutional Court Decision Number 78/PUU-XXI/2023 which broadens the meaning of defamation to include modern electronic media.[43] Thus, the existing criminal law and telematics law framework provides several entry points for victim protection. However, it remains fragmented because no instrument comprehensively defines deepfake offenses, regulates proof of AI-based manipulation, ensures victim recovery, or determines platform responsibility.

Reconstruction of Criminal Liability and the Urgency of Sui Generis Regulation as a Comprehensive Legal Protection Instrument for Deepfake Victims in Indonesia

The reconstruction of criminal liability in deepfake crimes requires a shift from a single liability model to a layered liability model involving several legal subjects. This model does not impose equal responsibility on all parties. It requires an assessment of each subject's fault, role, knowledge, control, and contribution to the deepfake crime. The first entity is the individual perpetrator who actively creates, distributes, or facilitates the dissemination of deepfake content, which can be prosecuted through the construction of material offenses in the ITE Law and the TPKS Law, provided that the mens rea element is met, namely intent (dolus) specifically directed at the act of content manipulation.[44] Individual perpetrators may be held liable for intentional conduct, including creating, editing, uploading, transmitting, or ordering deepfake content, when they know that the content is

[40] Ágnes Czine, "Constitutional Aspects of Clarity of Legal Provisions," *Magyar Nyelvőr* 146, no. 5 (2022): 65–80, https://doi.org/10.38143/Nyr.2022.5.65.
[41] Wibowo, Wangsajaya, and Surahmat, *Pemolisian Digital Dengan Artificial Intelligence*.
[42] Pengadilan Negeri Surabaya, Putusan Pengadilan Negeri Surabaya Nomor 8/Pdt.Sus-Siber/2024 (2024).
[43] Mahkamah Konstitusi Republik Indonesia, Putusan Mahkamah Konstitusi Nomor 78/PUU-XXI/2023 (2023).
[44] Prayoga and Tuasikal, "Penyebaran Konten Deepfake Sebagai Tindak Pidana: Analisis Kritis Terhadap Penegakan Hukum Dan Perlindungan Publik Di Indonesia."

false, manipulative, non-consensual, defamatory, fraudulent, or harmful to the victim. A facilitator may be held liable only when there is evidence of intentional assistance, encouragement, access provision, or participation in distributing unlawful content. Passive or accidental contact with the content should not be treated as criminal participation.

The second subject is the developer or provider of deepfake applications, who in the perspective of the new Criminal Code based on Law Number 1 of 2023 can be held accountable for corporate liability if it is proven that the platform or application they developed was predominantly designed or functioned to facilitate crime, a construction that refers to the doctrine of respondeat superior that has been adopted in Indonesian corporate criminal law.[45] Application developers may be held liable when they intentionally design, promote, commercialize, or maintain the application for unlawful manipulation. Liability may also arise when they negligently ignore repeated and foreseeable misuse despite having the capacity to prevent or restrict it. This limitation is important because deepfake technology may have lawful uses in education, entertainment, accessibility, and creative industries. Criminal responsibility should arise only when the developer shows unlawful intent, negligent facilitation, or failure to apply reasonable safeguards.

The third subject is the organizer of the electronic system that facilitates the distribution of content, where criminal responsibility can be imposed if the organizer is proven to have allowed (omitted) deepfake content to circulate on its platform after receiving a valid victim report from the victim, contrary to the legal obligations in Article 26 paragraph (1) of the ITE Law which regulates the protection of personal data in electronic systems. The liability of electronic system operators must be based on platform omission. This occurs when an operator receives a valid victim report, has actual knowledge of unlawful content, has the technical capacity to act, but fails to remove, restrict access to, or preserve evidence of the reported deepfake content.

Under the principle of geen straf zonder schuld, layered liability must consider the degree of fault of each legal subject. This prevents unfair strict liability and ensures that responsibility is based on knowledge, control, and contribution to the crime.[46] Thus, creator and distributor liability should be based on intentional conduct. Developer liability may be based on negligent facilitation, while platform liability may arise from omission after valid victim report, provided that each form of fault is proven through reliable digital evidence. A comparative study shows that China's approach through the 2023 Cybersecurity Law update, which requires labeling of AI content and imposes penalties of up to ten years in prison for perpetrators of content manipulation, and Singapore's Protection from Online Falsehoods and Manipulation Act (POFMA), which successfully reduced the spread of fake content by 25% in three years,[47] can serve as concrete references for Indonesian legal reform.

The urgency of establishing sui generis regulation on deepfake crimes in Indonesia is not merely an academic demand, but a legal necessity based on three fundamental arguments. Normatively, sui generis regulation is needed because existing criminal law and telematics law instruments still regulate only fragments of deepfake harm, while the principles of legality, legal certainty, victim protection, and proportional liability require a specific formulation that directly addresses AI-based manipulation. First, the argument of legal certainty: criminal law requires a clear and measurable definition of the offense (bestimmtheitsgebot), while the analogous application of the ITE Law articles to deepfake crimes is vulnerable to challenge as a violation of the lex stricta principle, which prohibits analogous interpretation in criminal law.[48]

Second, the argument for victim protection: sui generis regulation allow for the inclusion of specific provisions on victims' rights comprehensively, starting from mechanisms for expedited content removal (expedited takedown), restitution, restoration of good name, to protection of victims' identities during the legal process, aspects that are not adequately accommodated in existing regulations.[49] Such regulation should contain a clear definition of deepfake content, classification of

[45] Eurike Hailtik and Afifah, "Criminal Responsibility of Artificial Intelligence Committing Deepfake Crimes in Indonesia."
[46] Dwi Ika Ardiyani, "Analisis Yuridis Pertanggungjawaban Pidana Pelaku Deepfake Porn Berdasarkan Hukum Positif."
[47] Shaina Raza et al., "VLDBench Evaluating Multimodal Disinformation with Regulatory Alignment," *Information Fusion* 130 (June 2026): 104092, https://doi.org/10.1016/j.inffus.2025.104092.
[48] Rofi Aulia Rahman and Rizaldy Anggriawan, "Deepfakes and Electoral Crimes: Criminal Law Perspectives from Indonesia, India, Pakistan, and the US," *Indonesian Comparative Law Review (ICLR)* 7, no. 2 (2025): 132–46.
[49] Zaltina and Nurtjahyo, "Right to Be Forgotten as a Legal Protection for The Victims of Electronic Sexual Violence Cases."

prohibited conduct, victim recovery mechanisms, expedited takedown procedures, platform reporting obligations, and digital evidence standards for proving AI-based manipulation.

Third, the technological adaptability argument: sui generis regulation can be designed using a technology-neutral approach that allows legal norms to remain relevant even as AI technology continues to develop rapidly, as exemplified by the EU AI Act 2024 which classifies AI systems based on risk levels (risk-based approach) so that regulations do not become outdated quickly.[50] Accordingly, the reconstruction of criminal liability in deepfake crimes must combine layered responsibility with sui generis regulation. This framework enables criminal law to distinguish intentional manipulation, negligent facilitation, and platform omission while ensuring legal certainty, victim recovery, effective takedown, and reliable digital evidence standards.

Theoretical Framework as a Basis for Analysis

This research bases its analysis on three complementary theoretical frameworks. These theories function as analytical tools to assess victim protection, legal certainty, criminal liability, and the need for legal reform in AI-based deepfake crimes. First, Philipus M. Hadjon's Legal Protection Theory, which distinguishes between preventive legal protection, which attempts to prevent violations through clear prohibitive norms, and repressive legal protection, which involves restoring victims' rights after a crime through sanctions and restitution.[51] In this study, Hadjon's theory is used to assess whether Indonesian criminal law and telematics law provide preventive protection through clear prohibitions against deepfake creation and distribution, as well as repressive protection through sanctions, restitution, content removal, restoration of reputation, and victim recovery.

In relation to research findings, current Indonesian regulations do not meet preventive protection standards due to the absence of explicit prohibitions against the creation of deepfake content, and repressive protection is also weak due to the lack of a structured restitution mechanism for victims. This finding shows that the weakness of existing regulation lies not only in the absence of a specific offense, but also in the incomplete protection cycle from prevention, reporting, takedown, prosecution, to victim recovery. This weakness is then measured through Gustav Radbruch's theory of legal objectives, which places justice (*gerechtigkeit*), legal certainty (*rechtssicherheit*), and utility (*zweckmäßigkeit*) as three legal values that must be achieved harmoniously.[52] Radbruch's theory is used in this study to measure whether the existing legal framework can provide legal certainty through clear criminal norms, justice through meaningful redress for victims, and utility through an effective deterrent effect against the misuse of artificial intelligence.

In the context of deepfakes, all three have not been met: justice is disrupted because victims do not receive adequate redress, legal certainty is shaken due to inconsistent court decisions, and legal benefits are weakened because existing regulations fail to provide a real deterrent effect. The absence of a precise definition of deepfake also weakens the principle of lex certa and creates difficulties in proving AI-based manipulation, because investigators and judges must rely on broad interpretation of existing offenses. This condition leads to Satjipto Rahardjo's progressive legal theory, which emphasizes that law must move with social and technological change to achieve substantive justice for victims.[53] In this study, progressive legal theory justifies criminal law reconstruction through new legal norms that respond to the technological characteristics of deepfake crimes. This theory supports sui generis regulation to define deepfake content, regulate prohibited conduct, determine layered liability, and ensure victim-centered remedies.

These three theories collectively frame the main argument of this research that reconstructing Indonesian criminal law in response to deepfake crimes is not merely a policy choice, but also a moral

[50] Adnasohn Aqilla Respati, "Reformulasi UU ITE Terhadap Artificial Intelligence Dibandingkan Dengan Uni Eropa Dan China AI Act Regulation," *JURNAL USM LAW REVIEW* 7, no. 3 (December 14, 2024): 1737–58, https://doi.org/10.26623/julr.v7i3.10578.
[51] Lusia Sulastri, "Legal Protection for Reporters of Corruption Crimes," *Jurnal Daulat Hukum* 5, no. 2 (2022): 115–27.
[52] Hari Agus Santoso, "Perspektif Keadilan Hukum Teori Gustav Radbruch Dalam Putusan Pkpu 'PTB,'" *JATISWARA* 36, no. 3 (November 29, 2021): 325–34, https://doi.org/10.29303/jtsw.v36i3.341.
[53] Dian Juniarso, Junaidi Abdillah, and M. Ilham Wira Pratama, "Reformasi Kebijakan Pidana Nasional Terhadap Kejahatan Siber Berbasis AI Melalui Pendekatan Hukum Progresif," *Jurnal Impresi Indonesia* 5, no. 1 (January 9, 2026): 77–88, https://doi.org/10.58344/jii.v5i1.7355.

and legal obligation of the state to protect citizens from the evolving threat of artificial intelligence-based crimes.[54] Accordingly, Hadjon's theory identifies weaknesses in victim protection, Radbruch's theory evaluates justice, legal certainty, and utility, while Satjipto Rahardjo's theory provides the basis for criminal law reconstruction through layered liability and sui generis regulation.

Conclusion

This study concludes that Indonesian criminal law and telematics law still provide only partial protection for victims of AI-based deepfake content. Although the ITE Law, the Personal Data Protection Law, the TPKS Law, and the Criminal Code may be applied to certain forms of deepfake misuse, their protection remains fragmented because they do not specifically regulate the creation, manipulation, and distribution of deepfake content as an independent criminal offense. As a result, victim protection and legal certainty remain limited, especially in proving AI-based manipulation and ensuring effective recovery.

The reconstruction of criminal liability for deepfake crimes should be based on a layered liability model involving individual perpetrators, deepfake application developers, and electronic system operators. This model distinguishes liability based on intentional manipulation, negligent facilitation, and platform omission after a valid victim report, while considering each subject's knowledge, control, and contribution. The model must still observe the principle of geen straf zonder schuld, so that criminal responsibility remains proportional and fault-based.

This study recommends sui generis regulation on deepfake crimes in Indonesia, covering a clear definition of deepfake, prohibited conduct, victim recovery, expedited takedown, platform reporting obligations, and digital evidence standards. These elements are needed to create a more certain, victim-oriented, and technologically responsive criminal law framework. This research is limited to normative analysis of Indonesian criminal law, telematics law, and selected comparative regulations. Further research should examine cross-border jurisdiction, institutional readiness, and the practical implementation of digital forensic standards in handling AI-based deepfake cases.

References

Alfredo Tobing, Ruben Nicholas, and Yuliana Yuli. "Criminal Liability for the Creation and Distribution of Deepfake Pornographic Videos on Social Media." *Eduvest - Journal of Universal Studies* 6, no. 2 (February 6, 2026): 1302–14. https://doi.org/10.59188/eduvest.v6i2.52738.

Banh, Leonardo, and Gero Strobel. "Generative Artificial Intelligence." *Electronic Markets* 33, no. 1 (December 6, 2023): 63. https://doi.org/10.1007/s12525-023-00680-1.

Buiten, Miriam C, Alexandre de Streel, and and Martin Peitz. "Rethinking Liability Rules for Online Hosting Platforms." *International Journal of Law and Information Technology* 28, no. 2 (March 1, 2020): 139–66. https://doi.org/10.1093/ijlit/eaaa012.

Cheong, Ben Chester. "Transparency and Accountability in AI Systems: Safeguarding Wellbeing in the Age of Algorithmic Decision-Making." *Frontiers in Human Dynamics* 6 (July 3, 2024). https://doi.org/10.3389/fhumd.2024.1421273.

Czine, Ágnes. "Constitutional Aspects of Clarity of Legal Provisions." *Magyar Nyelvőr* 146, no. 5 (2022): 65–80. https://doi.org/10.38143/Nyr.2022.5.65.

Dwi Ika Ardiyani, Ni Kadek. "Analisis Yuridis Pertanggungjawaban Pidana Pelaku Deepfake Porn Berdasarkan Hukum Positif." *Jurnal Kajian Hukum Dan Kebijakan Publik | E-ISSN : 3031-8882* 2, no. 3 (November 21, 2024): 603–8. https://doi.org/10.62379/cs863250.

Eurike Hailtik, Asri Gresmelian, and Wiwik Afifah. "Criminal Responsibility of Artificial Intelligence Committing Deepfake Crimes in Indonesia." *Asian Journal of Social and Humanities* 2, no. 4 (January 22, 2024): 776–95. https://doi.org/10.59888/ajosh.v2i4.222.

Furizal, Alfian Ma'arif, Hari Maghfiroh, Iswanto Suwarno, Denis Prayogi, Kariyamin, Syahrani Lonang, and Abdel-Nasser Sharkawy. "Social, Legal, and Ethical Implications of AI-Generated Deepfake Pornography on Digital Platforms: A Systematic Literature Review." *Social Sciences & Humanities Open* 12 (2025): 101882. https://doi.org/10.1016/j.ssaho.2025.101882.

Grossman, Maura, and Paul Grimm. "Judicial Approaches to Acknowledged and Unacknowledged AI-Generated Evidence." *Science and Technology Law Review* 26, no. 2 (May 23, 2025).

[54] Tri Cahyono, Erni, and Hidayat, "Rekonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia."

https://doi.org/10.52214/stlr.v26i2.13890.
Hydara, Ebrima, Masato Kikuchi, and Tadachika Ozono. "Empirical Assessment of Deepfake Detection: Advancing Judicial Evidence Verification Through Artificial Intelligence." *IEEE Access* 12 (2024): 151188–203. https://doi.org/10.1109/ACCESS.2024.3480320.
Indonesia, Mahkamah Konstitusi Republik. Putusan Mahkamah Konstitusi Nomor 78/PUU-XXI/2023 (2023).
Juniarso, Dian, Junaidi Abdillah, and M. Ilham Wira Pratama. "Reformasi Kebijakan Pidana Nasional Terhadap Kejahatan Siber Berbasis AI Melalui Pendekatan Hukum Progresif." *Jurnal Impresi Indonesia* 5, no. 1 (January 9, 2026): 77–88. https://doi.org/10.58344/jii.v5i1.7355.
Kristiyenda, Yoan Shevila, Jasmine Faradila, and Christina Basanova. "Pencegahan Kejahatan Deepfake : Studi Kasus Terhadap Modus Penipuan Deepfake Prabowo Subianto Dalam Tawaran Bantuan Uang." *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora* 3, no. 2 (March 4, 2025): 149–64. https://doi.org/10.59246/aladalah.v3i2.1263.
Łabuz, Mateusz, and Sławomir Soczyński. "Deep Fakes As a Tool of Political Advertising. Can Regulatory Framework Benefit From The 'Ship of Theseus' Paradox?" *Technology in Society* 84 (March 2026): 103060. https://doi.org/10.1016/j.techsoc.2025.103060.
Laffier, Jennifer, and Aalyia Rehman. "Deepfakes and Harm to Women." *Journal of Digital Life and Learning* 3, no. 1 (June 24, 2023): 1–21. https://doi.org/10.51357/jdll.v3i1.218.
Lastri Riyanti, Lamijan, and Muhammad Zainudin. "Legal Reform on Network Security and Cybercrime in Information and Electronic Transaction Law." *Greenation International Journal of Law and Social Sciences* 3, no. 3 (November 22, 2025): 1216–23. https://doi.org/10.38035/gijlss.v3i3.610.
Lavi, Michal. "Publish, Share, Re-Tweet, and Repeat." *University of Michigan Journal of Law Reform*, no. 54.2 (2021): 441. https://doi.org/10.36646/mjlr.54.2.publish.
Maharani, Rista, and Andria Luhur Prakoso. "Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital." *JURNAL USM LAW REVIEW* 7, no. 1 (March 29, 2024): 333–47. https://doi.org/10.26623/julr.v7i1.8705.
Maras, Marie-Helen, and Alex Alexandrou. "Determining Authenticity of Video Evidence In The Age of Artificial Intelligence And In The Wake of Deepfake Videos." *The International Journal of Evidence & Proof* 23, no. 3 (July 28, 2019): 255–62. https://doi.org/10.1177/1365712718807226.
Mehta, Shalu, and Prof.(Dr.) Venoo Rajpurohit. "Legal Gaps in Deepfake Misuse & Strengthening Cybercrime Criminalization." *Lex Localis - Journal of Local Self-Government*, November 15, 2024, 536–48. https://doi.org/10.52152/803278.
Mustak, Mekhail, Joni Salminen, Matti Mäntymäki, Arafat Rahman, and Yogesh K. Dwivedi. "Deepfakes: Deceptions, Mitigations, and Opportunities." *Journal of Business Research* 154 (January 2023): 113368. https://doi.org/10.1016/j.jbusres.2022.113368.
Nguyen, Thanh Thi, Quoc Viet Hung Nguyen, Dung Tien Nguyen, Duc Thanh Nguyen, Thien Huynh-The, Saeid Nahavandi, Thanh Tam Nguyen, Quoc-Viet Pham, and Cuong M. Nguyen. "Deep Learning for Deepfakes Creation and Detection: A Survey." *Computer Vision and Image Understanding* 223 (October 2022): 103525. https://doi.org/10.1016/j.cviu.2022.103525.
Nurkholisah, Siti, Daud Rismana, Afrizal Eko Nugroho, Amrina Munjiyah, and Qurota Ayunisa. "Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan Kriminalisasi Dalam Hukum Pidana Indonesia." *JURNAL USM LAW REVIEW* 8, no. 3 (December 17, 2025): 2421–45. https://doi.org/10.26623/julr.v8i3.13060.
Nurmansyah, Gunsu, Rudi Natamiharja, and Ikhsan Setiawan. "Legal Protection of Personal Data Against Phishing in Indonesia: A Pancasila-Based Approach." *Pancasila and Law Review* 6, no. 1 (August 25, 2025): 15–44. https://doi.org/10.25041/plr.v6i1.4138.
Prayoga, Hendra, and Hadi Tuasikal. "Penyebaran Konten Deepfake Sebagai Tindak Pidana: Analisis Kritis Terhadap Penegakan Hukum Dan Perlindungan Publik Di Indonesia." *Abdurrauf Law and Sharia* 2, no. 1 (May 1, 2025): 22–38. https://doi.org/10.70742/arlash.v2i1.194.
Purwanti, Nina, Megawati Barthos, and Tri Eka Saputra. "The Role of Artificial Intelligence in the Implementation of Personal Data Protection Law in Indonesia." *Interdiciplinary Journal and Hummanity (INJURITY)* 4, no. 6 (June 20, 2025): 325–36. https://doi.org/10.58631/injurity.v4i6.1448.
Rahayu, Anisa, and Kuswandi. "The Deepfake Phenomenon as a New Form of Cybercrime from a Criminological Perspective." *Indonesian Journal of Law and Justice* 3, no. 2 (December 13, 2025): 14. https://doi.org/10.47134/ijlj.v3i2.5171.
Rahman, Alip, Anom Sutrisno, Lita Martia, and Feri Wangi. "Legal Protection for Victims of Online Gender-Based Violence (Cyber-Based Violence)." *Edunity Kajian Ilmu Sosial Dan Pendidikan* 3, no. 12 (December 25, 2024): 1210–20. https://doi.org/10.57096/edunity.v3i12.350.

Rahman, Rofi Aulia, and Rizaldy Anggriawan. "Deepfakes and Electoral Crimes: Criminal Law Perspectives from Indonesia, India, Pakistan, and the US." *Indonesian Comparative Law Review (ICLR)* 7, no. 2 (2025): 132–46.

Raza, Shaina, Ashmal Vayani, Aditya Jain, Aravind Narayanan, Vahid Reza Khazaie, Syed Raza Bashir, Elham Dolatabadi, et al. "VLDBench Evaluating Multimodal Disinformation with Regulatory Alignment." *Information Fusion* 130 (June 2026): 104092. https://doi.org/10.1016/j.inffus.2025.104092.

Respati, Adnasohn Aqilla. "Reformulasi UU ITE Terhadap Artificial Intelligence Dibandingkan Dengan Uni Eropa Dan China AI Act Regulation." *JURNAL USM LAW REVIEW* 7, no. 3 (December 14, 2024): 1737–58. https://doi.org/10.26623/julr.v7i3.10578.

Ridwan, Ridwan, Ainun Wulandari, and Syamsuddin. "Metaverse Regulation Formulation In Indonesian Cyber Law." *Law and Justice* 7, no. 2 (February 9, 2023): 143–52. https://doi.org/10.23917/laj.v7i2.757.

Romero-Moreno, Felipe. "Deepfake Detection in Generative AI: A Legal Framework Proposal to Protect Human Rights." *Computer Law & Security Review* 58 (September 2025): 106162. https://doi.org/10.1016/j.clsr.2025.106162.

Santoso, Hari Agus. "Perspektif Keadilan Hukum Teori Gustav Radbruch Dalam Putusan Pkpu 'PTB.'" *JATISWARA* 36, no. 3 (November 29, 2021): 325–34. https://doi.org/10.29303/jtsw.v36i3.341.

Sloot, Bart van der, and Yvette Wagensveld. "Deepfakes: Regulatory Challenges for The Synthetic Society." *Computer Law & Security Review* 46 (September 2022): 105716. https://doi.org/10.1016/j.clsr.2022.105716.

Souza, Raphael Ramos Monteiro de. "Legal Remedies and Regulatory Frameworks to Combat Ai-Driven Deepfakes." In *Mitigating the Risks of AI Deepfakes*, 94–116. CRC Press, 2026.

Sulastri, Lusia. "Legal Protection for Reporters of Corruption Crimes." *Jurnal Daulat Hukum* 5, no. 2 (2022): 115–27.

Surabaya, Pengadilan Negeri. Putusan Pengadilan Negeri Surabaya Nomor 8/Pdt.Sus-Siber/2024 (2024).

Theodora Kristina Boleng, and Adi Nur Rohman. "Regulatory Gaps and Legal Enforcement Challenges on Deepfake Pornography as a Form of Digital Sexual Violence in Indonesia." *Al-Zayn : Jurnal Ilmu Sosial & Hukum* 3, no. 6 SE-Articles (December 9, 2025): 10068–80. https://doi.org/10.61104/alz.v3i6.2714.

Tri Cahyono, Soetardi, Wina Erni, and Taufik Hidayat. "Rekonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia." *Dame Journal of Law* 1, no. 1 (March 15, 2025): 1–23. https://doi.org/10.64344/djl.v1i1.6.

Ugwuoke, Valentine, and Madelyn Rose Sanfilippo. "The Current Landscape of Deepfake Legislation in the United States." *Journal of Information Policy* 15 (June 30, 2025): 97–129. https://doi.org/10.5325/jinfopoli.15.2025.0004.

Wibowo, Arief, Yehu Wangsajaya, and Asep Surahmat. *Pemolisian Digital Dengan Artificial Intelligence*. PT. RajaGrafindo Persada-Rajawali Pers, 2023.

Yadav, Hrishikesh, and Jay Oza. "The DeepFake Dilemma: Balancing Innovation, Ethics, and Accountability Through Law," September 9, 2025. https://doi.org/10.36227/techrxiv.175744943.37338204/v1.

Zaltina, Putri, and Lidwina Inge Nurtjahyo. "Right to Be Forgotten as a Legal Protection for The Victims of Electronic Sexual Violence Cases." *The Indonesian Journal of Socio-Legal Studies* 3, no. 2 (2024). https://doi.org/10.54828/ijsls.2024v3n2.4.