



Deepfake as a New Form of Cybercrime: Evaluating the Adequacy of Indonesian Criminal Law in Protecting Digital Society

Sri Ayu Astuti

Universitas Wisnuwardhana, Indonesia

saar_1126@yahoo.co.id

Abstract

The rapid diffusion of generative artificial intelligence has made deepfake technology a low-cost instrument for fraud, defamation, non-consensual pornography, sextortion, identity misuse, and political disinformation, yet Indonesia has no criminal provision that names “deepfake” as a distinct offense. This article evaluates the adequacy of Indonesian criminal law in protecting digital society against deepfake-enabled cybercrime. The analysis maps how the ITE Law, the Penal Code, the Personal Data Protection Law, and the Pornography Law are stretched to reach deepfake conduct, identifies the harm categories most frequently reported in the literature, and evaluates enforcement capacity, victim protection, and reform proposals. The findings show that Indonesian positive law remains reactive, fragmented, and interpretively strained, lacking an explicit statutory definition of deepfake, a *lex specialis* offense, adequate digital forensic capacity, and coordinated platform accountability mechanisms. The article concludes that legal adequacy cannot be achieved through criminalization alone and proposes a multi-layered reform agenda combining statutory reform, forensic capacity building, platform and labeling obligations, and digital literacy programs.

Keywords: Deepfake; Cybercrime; Criminal Law; Indonesia; Digital Society; Legal Adequacy.

Introduction

Generative artificial intelligence has lowered the technical barrier for producing highly realistic synthetic audio, image, and video content commonly known as deepfakes, transforming what was once a specialized capability into a widely accessible tool for deception.¹ What began as a novelty in entertainment and satire has evolved into a vector for fraud, defamation, non-consensual pornography, sextortion, identity misuse, data theft, and coordinated political disinformation.² Indonesia, with one of the largest social media populations in

¹ A Rahayu and Kuswandi, “The Deepfake Phenomenon as a New Form of Cybercrime from a Criminological Perspective,” *Indonesian Journal of Law and Justice*, 2025, <https://doi.org/10.47134/ijlj.v3i2.5171>; Gede Sariasa et al., “The Existence of Deepfake Artificial Intelligence As a Means Of Crime In The Perspective Of Indonesia’s Positive Law,” in *Proceedings of the 6th International Conference on Law, Social Sciences and Education, ICLSSE 2024, 17 October 2024, Singaraja, Bali, Indonesia*, 2024, <https://doi.org/10.4108/eai.17-10-2024.2353690>.

² Putri Ramadhani Rangkuti et al., “Analisis Yuridis Terhadap Penggunaan Deepfake Dalam Pelanggaran UU ITE,” *Depositi: Jurnal Publikasi Ilmu Hukum*, 2025,

Southeast Asia, has already recorded deepfake-related incidents implicating public figures, financial victims, and political discourse, exposing the population to reputational, psychological, and financial harm at a scale that existing legal instruments were never designed to address.³

The core research gap addressed in this article is the absence of a systematic, comparative evaluation of whether Indonesian criminal law is doctrinally and institutionally adequate to respond to deepfake-enabled cybercrime. Existing Indonesian scholarship converges on the observation that positive law lacks an explicit deepfake offense and instead forces prosecutors toward general provisions in the ITE Law, the Penal Code (KUHP), the Personal Data Protection Law (UU PDP), and the Pornography Law.⁴ Several studies show that these provisions can reach deepfake conduct only indirectly, through strained interpretation that weakens the principle of legal certainty, or *lex certa*, and creates inconsistent case outcomes.⁵ What remains missing from the literature, however, is a single synthesis that (a) consolidates the fragmented statutory mapping into a structured comparative overview, (b) benchmarks Indonesia's normative position against the regulatory trajectories of the European Union, the United States, and China, and

<https://doi.org/10.59581/deposisi.v3i2.5080>; Wenggedes Frensh, "Criminal Policy Toward the Crime of Defamation in Cyberspace Through the Use of Deepfake AI," *JURNAL AKTA*, 2025, <https://doi.org/10.30659/akta.v12i2.44884>; Wayan Zenitia Devi, "Implikasi Hukum Terhadap Penyalahgunaan Teknologi Deepfake Untuk Pemerasan (Sextortion) Dalam Perspektif Hukum Teknologi Informasi Di Indonesia," *Majelis: Jurnal Hukum Indonesia*, 2026, <https://doi.org/10.62383/majelis.v3i1.1504>.

³ Fabrizio Richardo Marvil Wanggai, Made Sugi Hartono, and Ni Putu Ega Parwati, "Analisis Normatif Terhadap Penyebaran Deepfake Sebagai Bentuk Kejahatan Siber Di Indonesia," *Majelis: Jurnal Hukum Indonesia*, 2026, <https://doi.org/10.62383/majelis.v3i1.1509>; 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*, 2026, <https://doi.org/10.59188/eduvest.v6i2.52738>.

⁴ Siti Nurkholisah et al., "Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan Kriminalisasi Dalam Hukum Pidana Indonesia," *JURNAL USM LAW REVIEW*, 2025, <https://doi.org/10.26623/julr.v8i3.13060>; Alzet Rama, Wiki Lofandri, and Anggi Firmanjaya Saputra, "Legal Gaps in Indonesia's Electronic Information and Transactions Law in Addressing Deepfake Technology: Challenges and Regulatory Recommendations," *SCHOULID: Indonesian Journal of School Counseling*, 2025, <https://doi.org/10.23916/086155011>; Rafi Satrya Arvitto, "Implikasi Hukum Deepfake: Telaah Terhadap UU ITE Dan UU PDP," *Jurnal Ilmiah Hukum Dan Hak Asasi Manusia*, 2025, <https://doi.org/10.35912/jihham.v4i2.3937>; N Fitriani et al., "KEBIJAKAN FORMULASI TINDAK PIDANA DEEFAKE DALAM UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK (UU ITE) DAN UNDANG-UNDANG PELINDUNGAN DATA PRIBADI (UU PDP) DI INDONESIA," *Jurnal Hukum To-Ra: Hukum Untuk Mengatur Dan Melindungi Masyarakat*, 2026, <https://doi.org/10.55809/tora.v12i1.647>.

⁵ Rachmat Irvan and Junet Hariyo Setiawan, "CRIMINALIZATION POLICY OF DEEFAKE IN INDONESIAN ELECTIONS," *Constitutional Law Society*, 2026, <https://doi.org/10.36448/jcls.v5i1.125>; Rangkuti et al., "Analisis Yuridis Terhadap Penggunaan Deepfake Dalam Pelanggaran UU ITE."

(c) connects legal-doctrinal gaps to institutional constraints such as digital forensic capacity, cross-border jurisdiction, and public digital literacy.⁶

Technically, deepfakes are produced through generative adversarial networks and related deep-learning architectures capable of synthesizing highly realistic visual, audio, and textual content; a comprehensive survey of detection methods confirms that the sophistication of generation techniques is consistently outpacing the reliability of automated detection tools, which creates a structural asymmetry between offenders and both regulators and platforms.⁷ From a criminological standpoint, deepfakes are increasingly treated as a distinct cybercrime typology rather than a mere variant of existing offences, because they combine three features rarely found together in earlier forms of digital crime: low technical barriers to entry, high perceptual credibility, and rapid, borderless dissemination.⁸

No single Indonesian statute defines or criminalizes deepfake as such. Instead, prosecutors and scholars rely on a patchwork of general provisions: the Electronic Information and Transactions Law (UU ITE), which addresses the distribution of false information and defamatory electronic content but was not designed with AI-generated synthetic media in mind⁹; the Criminal Code's general provisions on fraud, defamation, and forgery¹⁰; the Personal Data Protection Law (UU PDP), which offers indirect protection where a deepfake involves unauthorized use of biometric or personal data¹¹; the Sexual Violence Crimes Law (UU TPKS) and the Pornography Law, both invoked in non-consensual deepfake

⁶ I Triana, Aniek Periani, and Arka Atyanta, "Closing Indonesia's Regulatory Gap on Deepfake Crimes: Comparative Lessons from the European Union, the United States, and China," *Kosmik Hukum*, 2026, <https://doi.org/10.30595/kosmikhukum.v26i2.25751>; Fheny Adilla Astari and Joko Setiyono, "The Criminalization of Deepfakes Through Blockchain: Constructing Transnational Criminal Law in the Era of Artificial Intelligence," *International Journal of Social Science and Human Research*, 2026, <https://doi.org/10.47191/ijsshr/v9-i5-126>.

⁷ Rami Mubarak et al., "A Survey on the Detection and Impacts of Deepfakes in Visual, Audio, and Textual Formats," *IEEE Access* 11 (2023): 144497–529, <https://doi.org/10.1109/access.2023.3344653>.

⁸ Rahayu and Kuswandi, "The Deepfake Phenomenon as a New Form of Cybercrime from a Criminological Perspective"; Wanggai, Hartono, and Parwati, "Analisis Normatif Terhadap Penyebaran Deepfake Sebagai Bentuk Kejahatan Siber Di Indonesia."

⁹ Rama, Lofandri, and Saputra, "Legal Gaps in Indonesia's Electronic Information and Transactions Law in Addressing Deepfake Technology: Challenges and Regulatory Recommendations"; Arvitto, "Implikasi Hukum Deepfake: Telaah Terhadap UU ITE Dan UU PDP."

¹⁰ Maria Karunia Putri Maan, Heryanto Amalo, and Ngongo Dede, "Analisis Perlindungan Hukum Terhadap Penyimpangan Artificial Intelligence Dalam Tindak Pidana Deepfake Pornografi Berdasarkan Hukum Pidana," *Jurnal Riset Rumpun Ilmu Sosial, Politik Dan Humaniora*, 2025, <https://doi.org/10.55606/jurrish.v4i1.5071>.

¹¹ Arvitto, "Implikasi Hukum Deepfake: Telaah Terhadap UU ITE Dan UU PDP"; L Judijanto, Andrew Shandy Utama, and Heri Setiyawan, "Implementation of Ethical Artificial Intelligence Law to Prevent the Use of AI in Spreading False Information (Deepfake) in Indonesia," *The Easta Journal Law and Human Rights*, 2025, <https://doi.org/10.58812/eslhr.v3i02.470>.

pornography cases¹²; and doctrines of criminal liability for AI-assisted conduct more broadly¹³. Several authors describe the resulting framework as reactive and structurally fragmented, harmonized neither for legal certainty nor for proportional sanctioning.¹⁴

Across the reviewed studies, deepfake harms in Indonesia cluster into four recurring domains: financial fraud through impersonation of public figures or trusted intermediaries¹⁵; non-consensual sexualized content targeting private individuals and public figures alike¹⁶; political disinformation and electoral manipulation¹⁷; and violations of informational privacy through unauthorized synthetic use of a person's likeness or biometric data.¹⁸

A second cluster of findings concerns enforcement rather than substantive law. Digital-forensic proof is described as especially difficult in deepfake cases, both in distinguishing authentic from manipulated media and in tracing anonymous or cross-border perpetrators.¹⁹ This is compounded by limited

¹² Maan, Amalo, and Dede, "Analisis Perlindungan Hukum Terhadap Penyimpangan Artificial Intelligence Dalam Tindak Pidana Deepfake Pornografi Berdasarkan Hukum Pidana"; Tobing and Yuli, "Criminal Liability for the Creation and Distribution of Deepfake Pornographic Videos on Social Media"; Decri Reza, M Utama, and Henny Yuningsih, "Artificial Intelligence-Generated Deepfake Pornography: A Normative Analysis of Criminal Liability and Victim Protection in Indonesian Law," *Ius Poenale*, 2026, <https://doi.org/10.25041/ip.v7i1.4738>.

¹³ Asri Gresmelian Eurike Hailtik and Wiwik Afifah, "Criminal Responsibility of Artificial Intelligence Committing Deepfake Crimes in Indonesia," *Asian Journal of Social and Humanities*, 2024, <https://doi.org/10.59888/ajosh.v2i4.222>.

¹⁴ Nurkholisah et al., "Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan Kriminalisasi Dalam Hukum Pidana Indonesia"; W Handoko, "Digital Crime In The Era Of Society 5.0: Juridical Analysis Of Cyber And Victim Protection," *Ipsa Jure*, 2025, <https://doi.org/10.62872/6991g409>; Tegar Raffi Putra Jumentoro and Muhammad Kuttub Firdausy, "Transhumanistic Cybercrime Analysis Using a Posthuman Criminology Approach to Digital Identity Threats in Artificial Intelligence Era," *Priviet Social Sciences Journal*, 2025, <https://doi.org/10.55942/pssj.v5i9.558>.

¹⁵ Wilma Silalahi and Fitri Natasha Dachi, "Pertanggung Jawaban Hukum Platform Media Sosial Terhadap Penyebaran Konten Deepfake Berbasis Artificial Intelligence Dalam Kasus Penipuan Berkedok Ritual Uang Gaib Ujang Busthomi," *Politika Progresif: Jurnal Hukum, Politik Dan Humaniora*, 2026, <https://doi.org/10.62383/progres.v3i2.3110>; Rahayu and Kuswandi, "The Deepfake Phenomenon as a New Form of Cybercrime from a Criminological Perspective."

¹⁶ Maan, Amalo, and Dede, "Analisis Perlindungan Hukum Terhadap Penyimpangan Artificial Intelligence Dalam Tindak Pidana Deepfake Pornografi Berdasarkan Hukum Pidana"; Tobing and Yuli, "Criminal Liability for the Creation and Distribution of Deepfake Pornographic Videos on Social Media"; Reza, Utama, and Yuningsih, "Artificial Intelligence-Generated Deepfake Pornography: A Normative Analysis of Criminal Liability and Victim Protection in Indonesian Law."

¹⁷ Nestia Lianingsih and Alim Jaizul, "Legal Implications of the Use of Deepfake in Politics and National Security in Indonesia," *International Journal of Humanities, Law, and Politics*, 2025, <https://doi.org/10.46336/ijhlp.v3i1.190>; Irvan and Setiawan, "CRIMINALIZATION POLICY OF DEEPFAKE IN INDONESIAN ELECTIONS."

¹⁸ Arvitto, "Implikasi Hukum Deepfake: Telaah Terhadap UU ITE Dan UU PDP"; Judijanto, Utama, and Setiawan, "Implementation of Ethical Artificial Intelligence Law to Prevent the Use of AI in Spreading False Information (Deepfake) in Indonesia."

¹⁹ Irvan and Setiawan, "CRIMINALIZATION POLICY OF DEEPFAKE IN INDONESIAN ELECTIONS"; Nurkholisah et al., "Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan

institutional capacity: law enforcement agencies frequently lack specialized forensic tools, trained personnel, and coordinated systems for AI-driven evidence analysis.²⁰ Low public digital literacy further amplifies exposure, since the public's limited capacity to recognize manipulated content accelerates dissemination and increases victimization, particularly during politically sensitive periods and in fraud schemes targeting vulnerable groups.²¹

The novelty of this article lies in three contributions. First, it synthesizes twenty recent Indonesian and comparative studies (2024–2026) into a structured legal-instrument map that quantifies how often each statute is invoked and what limitation each carries, an exercise not previously undertaken in the deepfake-criminal-law literature. Second, it triangulates doctrinal findings with a comparative benchmarking of EU, US, and Chinese regulatory approaches to derive transferable reform lessons.²² Third, it integrates legal-doctrinal, institutional, and social-literacy dimensions into a single multi-layered adequacy framework rather than treating criminalization as a stand-alone solution.²³

Based on this gap, the article addresses three research questions: (1) What are the legal regulations regarding deepfakes within the Indonesian legal system? (2) What is the ideal legal regulatory framework (*ius constituendum*) for addressing deepfakes in Indonesia?. Accordingly, this study aims to evaluate the doctrinal adequacy of Indonesian criminal law against deepfake cybercrime, to map the enforcement and victim-protection constraints reported in the literature, and to

Kriminalisasi Dalam Hukum Pidana Indonesia”; Hasnia Hasnia et al., “Reconstruction of Criminal Law Policy in Handling Cyber Crime: Perspectives of Technology Law and Human Rights,” *Jurnal Smart Hukum (JSH)*, 2025, <https://doi.org/10.55299/jsh.v3i3.1328>.

²⁰ Tagor Aruan and Rahmayanti Rahmayanti, “The Development of Cybercrime as a Criminal Offense in the Digital Era and Its Impact on Society,” *Discourse Journal on Law and Society*, 2025, <https://doi.org/10.70062/djls.v1i3.81>; Nopit Ernasari and Naib, “CRIMINAL LAW REFORM IN THE FACE OF THE SOCIETY 5.0 ERA AGAINST CYBER CRIME,” *International Journal of Accounting, Management, Economics and Social Sciences (IJAMESC)*, 2024, <https://doi.org/10.61990/ijamesc.v2i6.383>; Hasnia et al., “Reconstruction of Criminal Law Policy in Handling Cyber Crime: Perspectives of Technology Law and Human Rights.”

²¹ Judijanto, Utama, and Setiyawan, “Implementation of Ethical Artificial Intelligence Law to Prevent the Use of AI in Spreading False Information (Deepfake) in Indonesia”; Silalahi and Dachi, “Pertanggung Jawaban Hukum Platform Media Sosial Terhadap Penyebaran Konten Deepfake Berbasis Artificial Intelligence Dalam Kasus Penipuan Berkedok Ritual Uang Gaib Ujang Busthomi.”

²² Triana, Periani, and Atyanta, “Closing Indonesia’s Regulatory Gap on Deepfake Crimes: Comparative Lessons from the European Union, the United States, and China.”

²³ Ameena Syifa Dwiandari and R Arifin, “Criminal Law Enforcement on Digital Identity Misuse in AI Era for Commercial Interests in Indonesia,” *The Indonesian Journal of International Clinical Legal Education*, 2025, <https://doi.org/10.15294/iccle.v7i1.25525>; H Gunawan, “When Artificial Intelligence Becomes a Criminal Tool: Urgency of Criminal Law Policy Against Data Theft in Indonesia,” *Jurnal Idea Hukum*, 2025, <https://doi.org/10.20884/1.jih.2025.11.2.665>.

formulate a comparative, multi-layered reform agenda for protecting digital society.

Methods

The research that forms the basis for this article uses the normative legal research method, a research method that examines law as written norms (law in books) with an emphasis on analysis of legal materials in the literature. This method was chosen because the problem being studied relates to the consistency and harmonization of legal norms, particularly those governing the criminal liability of cybercrimes in the ITE Law and the National Criminal Code. Therefore, an analysis of applicable doctrines, legal principles, and laws and regulations is necessary.²⁴ The approaches used in this research are the statute approach, the conceptual approach, and the comparative approach. The statute approach is carried out by examining all laws and regulations relevant to the legal issue being studied, including the Indonesian Penal Code (KUHP) Law Number 1 of 2023 concerning the Criminal Code, the ITE Law (Law No. 19/2016) and its amendments, the Personal Data Protection Law (Law No. 27/2022), and the Pornography Law (Law No. 44/2008) and its amendments, and other related laws and regulations. Meanwhile, the conceptual approach is used to analyze relevant criminal law concepts, such as the concepts of criminal liability, the principle of fault, *actus reus* and *mens rea*, and the concept of jurisdiction in international criminal law. Meanwhile, the comparative approach is An approach involving the comparison of legal systems or the laws of one country with those of one or more other countries regarding the same subject matter including court rulings. Legal comparison may be conducted on either a specific or a general basis. Such comparisons are undertaken to identify the similarities and differences between the respective systems or laws.

The legal materials used in this study consist of three types: primary legal materials, secondary legal materials, and Tertiary legal materials. Primary legal materials include legally binding laws and regulations, including the National Criminal Code, the ITE Law, the Personal Data Protection Law, the Pornography Law and their implementing regulations. Secondary legal materials include criminal law textbooks, national and international scientific journals discussing

²⁴Peter Mahmud Marzuki, sebagaimana dikutip dalam Aditya Wirawan, "Metode Penelitian Hukum Normatif dalam Kajian Pembaruan Hukum Pidana," *Jurnal Metodologi Penelitian Hukum*, Vol. 4, No. 2 (2021), hlm. 121-138.

deepfake technology and Indonesian criminal law, previous research results, retrieved and screened for thematic relevance to legal adequacy, enforcement capacity, victim protection, comparative regulation, and other relevant scientific works, with priority given to literature published within the last five years to ensure the topicality and relevance of the analysis. Tertiary legal materials include legal dictionaries and encyclopedias used to clarify technical terms used in the study.

The legal material collection technique is carried out through library research, namely by tracing, collecting, and inventorying legal materials relevant to the issue being studied. After the legal materials are collected, a qualitative analysis is conducted using descriptive-prescriptive analysis techniques, namely systematically explaining the applicable legal norms related to criminal liability for cybercrimes, then providing prescriptions or recommendations for the legal problems found. The analysis is carried out by comparing the provisions in the ITE Law and the National Criminal Code, identifying points of intersection and points of conflict between norms, and linking them to criminal law doctrine and relevant jurisprudential developments, so as to obtain a comprehensive picture of the construction of criminal liability for cybercrimes in the Indonesian criminal law system.

To maintain the validity and reliability of the analysis, this study applies several selection criteria to the secondary legal materials used, namely the relevance of the theme to the issue of criminal liability for cybercrime, the credibility of the publication source, and the topicality of the publication year. Priority is given to articles from nationally and internationally accredited scientific journals published between 2021 and 2026, while still referring to classical criminal law literature as long as it is relevant to explaining the fundamental and timeless basic principles of criminal law. This combination of classical and contemporary literature is intended to maintain a balance between the depth of doctrinal analysis and the topicality of the issues studied.

The analytical framework used in this study also takes into account the hierarchy of laws and regulations as stipulated in Law Number 12 of 2011 concerning the Formation of Legislation and its amendments, in order to ensure that each norm analyzed is placed according to its position in the national legal system. Thus, the potential for norm conflicts between the ITE Law and the National Criminal Code can be analyzed appropriately through the principles of norm conflict resolution that apply in legal science, such as the principle of *lex specialis derogat legi generali* and the principle of *lex posterior derogat legi priori*, so that

the results of the analysis obtained have a solid methodological foundation and can be academically accounted for. As a normative legal study, this article does not utilize field data or interviews as primary sources, but rather relies entirely on analysis of legal literature. The author fully acknowledges this limitation, and therefore the conclusions drawn are prescriptive and normative in nature and open to further enrichment through subsequent empirical research, for example, through a quantitative review of court decisions or in-depth interviews with law enforcement officials who directly handle cybercrime cases.²⁵

Discussion

The legal regulations regarding deepfakes within the Indonesian legal system

The synthesis confirms that Indonesia's deepfake-related deficiency is not primarily a conflict of norms-there is no reported instance in the literature of two valid Indonesian provisions producing contradictory outcomes for the same deepfake act. Rather, the dominant defect is a legal vacuum: no statute explicitly names, defines, or criminalizes the creation or malicious distribution of deepfake content as such.²⁶ Layered onto this vacuum is normative vagueness within the provisions that are nonetheless pressed into service: the ITE Law's concepts of "electronic information/document" and "false and misleading content" were not drafted to capture the evidentiary and authorship complexities of AI-synthesized media, producing genuine interpretive uncertainty when courts and prosecutors attempt to apply them.²⁷ This combination-absence at the definitional level, ambiguity at the operational level-explains why the literature consistently

²⁵Rina Anggraeni Putri, "Teknik Analisis Bahan Hukum dalam Penelitian Hukum Normatif," *Jurnal Ilmu Hukum dan Metodologi*, Vol. 7, No. 1 (2022), hlm. 44-59.

²⁶ Nurkholisah et al., "Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan Kriminalisasi Dalam Hukum Pidana Indonesia"; Lianingsih and Jaizul, "Legal Implications of the Use of Deepfake in Politics and National Security in Indonesia"; Hailtik and Afifah, "Criminal Responsibility of Artificial Intelligence Committing Deepfake Crimes in Indonesia"; Hendry Widjaya Ong, Windi Afdal, and Tantimin, "PERBANDINGAN PENGATURAN SANKSI PENIPUAN ONLINE BERBASIS ARTIFICIAL INTELLIGENCE: INDONESIA VS AMERIKA," *Jurnal Hukum To-Ra : Hukum Untuk Mengatur Dan Melindungi Masyarakat*, 2025, <https://doi.org/10.55809/tora.v11i2.579>.

²⁷ Judijanto, Utama, and Setiyawan, "Implementation of Ethical Artificial Intelligence Law to Prevent the Use of AI in Spreading False Information (Deepfake) in Indonesia"; Rama, Lofandri, and Saputra, "Legal Gaps in Indonesia's Electronic Information and Transactions Law in Addressing Deepfake Technology: Challenges and Regulatory Recommendations"; Tobing and Yuli, "Criminal Liability for the Creation and Distribution of Deepfake Pornographic Videos on Social Media"; Maan, Amalo, and Dede, "Analisis Perlindungan Hukum Terhadap Penyimpangan Artificial Intelligence Dalam Tindak Pidana Deepfake Pornografi Berdasarkan Hukum Pidana."

characterizes Indonesian regulation as reactive, fragmented, and insufficiently harmonized for legal certainty, victim protection, and proportional sanctioning.²⁸

Legal certainty and offense classification. The results confirm that Indonesia's reliance on general provisions produces a persistent *lex certa* problem: because no statute defines deepfake or synthetic media in operative legal terms, prosecutors must characterize the same underlying conduct differently depending on which statute is invoked, producing inconsistent charging practices and unpredictable case outcomes.²⁹ This is consistent with findings that identify the missing technical definition as the single most consequential defect in the current framework, since it cascades into difficulties in offense classification, evidentiary proof, and sanction proportionality.³⁰

Table 2 disaggregates the adequacy problem by harm domain, showing that even where a relevant statute nominally exists, its application to deepfake conduct remains incomplete or evidentially fragile.

Harm Domain	Typical Misuse	Why Current Law Struggles	Key Sources
Fraud	Public-figure impersonation and investment or ritual-themed scam content.	General fraud and ITE provisions apply, but deepfake-specific evidentiary proof remains difficult.	Silalahi & Dachi (2026); Rahayu & Kuswandi (2025)

²⁸ Nurkholisah et al., “Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan Kriminalisasi Dalam Hukum Pidana Indonesia”; Maan, Amalo, and Dede, “Analisis Perlindungan Hukum Terhadap Penyimpangan Artificial Intelligence Dalam Tindak Pidana Deepfake Pornografi Berdasarkan Hukum Pidana”; Handoko, “Digital Crime In The Era Of Society 5.0: Juridical Analysis Of Cyber And Victim Protection”; Jumentoro and Firdausy, “Transhumanistic Cybercrime Analysis Using a Posthuman Criminology Approach to Digital Identity Threats in Artificial Intelligence Era.”

²⁹ Nurkholisah et al., “Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan Kriminalisasi Dalam Hukum Pidana Indonesia”; Irvan and Setiawan, “CRIMINALIZATION POLICY OF DEEPFAKE IN INDONESIAN ELECTIONS”; Rangkuti et al., “Analisis Yuridis Terhadap Penggunaan Deepfake Dalam Pelanggaran UU ITE.”

³⁰ Nurkholisah et al., “Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan Kriminalisasi Dalam Hukum Pidana Indonesia”; Rama, Lofandri, and Saputra, “Legal Gaps in Indonesia’s Electronic Information and Transactions Law in Addressing Deepfake Technology: Challenges and Regulatory Recommendations”; Triana, Periani, and Atyanta, “Closing Indonesia’s Regulatory Gap on Deepfake Crimes: Comparative Lessons from the European Union, the United States, and China.”

Harm Domain	Typical Misuse	Why Current Law Struggles	Key Sources
Pornography	Non-consensual sexualized face-swap content.	Rules span Pornography, ITE, PDP, TPKS, and KUHP, yet remain non-specific and incomplete.	Maan et al. (2025); Tobing & Yuli (2026); Reza et al. (2026)
Politics	Election disinformation and black-campaign content.	Existing law does not explicitly regulate deepfakes in political manipulation.	Lianingsih & Jaizul (2025); Irvan & Setiawan (2026)
Privacy	Identity theft and unauthorized use of personal data/likeness.	PDP Law offers partial protection, but deepfake misuse is not directly regulated.	Arvitto (2025); Judijanto et al. (2025)

Table 2. *Deepfake harm domains and corresponding legal limitations in Indonesia.*

In the fraud domain, general provisions under the Criminal Code and the ITE Law can, in principle, be applied to deepfake-enabled scams, but establishing that a specific piece of synthetic content was both fabricated and used with fraudulent intent remains evidentially demanding, particularly where perpetrators operate anonymously or across borders.³¹ In the pornography domain, the overlapping architecture of the Pornography Law, the ITE Law, the Personal Data Protection Law, the Sexual Violence Crimes Law, and the Criminal Code offers multiple potential entry points for prosecution, yet none directly addresses the absence of consent that is specific to face-swapped or synthetically generated sexual content, leaving victims to rely on doctrines built for authentic, non-synthetic material.³² In

³¹ Silalahi and Dachi, “Pertanggung Jawaban Hukum Platform Media Sosial Terhadap Penyebaran Konten Deepfake Berbasis Artificial Intelligence Dalam Kasus Penipuan Berkedok Ritual Uang Gaib Ujang Busthomi”; Rahayu and Kuswandi, “The Deepfake Phenomenon as a New Form of Cybercrime from a Criminological Perspective.”

³² Maan, Amalo, and Dede, “Analisis Perlindungan Hukum Terhadap Penyimpangan Artificial Intelligence Dalam Tindak Pidana Deepfake Pornografi Berdasarkan Hukum Pidana”; Tobing and Yuli, “Criminal Liability for the Creation and Distribution of Deepfake Pornographic Videos on Social Media”;

the political domain, the literature is unambiguous that no existing provision explicitly regulates deepfakes used for election disinformation or black campaigns, a gap with particular urgency given Indonesia's electoral cycle and the demonstrated susceptibility of political communication to synthetic manipulation.³³ In the privacy domain, the Personal Data Protection Law offers only partial coverage, since it was designed around data processing rather than the synthetic re-creation of a person's likeness or voice, leaving deepfake-specific privacy harms only indirectly addressed.³⁴

Even where substantive law could in theory be stretched to cover a deepfake offence, enforcement faces three compounding barriers. First, digital-forensic authentication is difficult: distinguishing authentic from AI-manipulated media requires specialized technical expertise that is unevenly distributed across Indonesian law-enforcement institutions, and cross-border tracing of anonymous perpetrators remains a persistent obstacle.³⁵ Second, institutional capacity is limited: studies converge on the finding that law-enforcement agencies often lack dedicated forensic tools, trained personnel, and inter-agency coordination mechanisms necessary for AI-driven evidence analysis.³⁶ Third, low digital literacy among the general public accelerates the spread of manipulated content before it can be identified or corrected, disproportionately exposing users during politically sensitive periods and disproportionately exposing vulnerable groups to fraud schemes.³⁷

Reza, Utama, and Yuningsih, "Artificial Intelligence–Generated Deepfake Pornography: A Normative Analysis of Criminal Liability and Victim Protection in Indonesian Law."

³³ Lianingsih and Jaizul, "Legal Implications of the Use of Deepfake in Politics and National Security in Indonesia"; Irvan and Setiawan, "CRIMINALIZATION POLICY OF DEEPFAKE IN INDONESIAN ELECTIONS."

³⁴ Arvitto, "Implikasi Hukum Deepfake: Telaah Terhadap UU ITE Dan UU PDP"; Judijanto, Utama, and Setiawan, "Implementation of Ethical Artificial Intelligence Law to Prevent the Use of AI in Spreading False Information (Deepfake) in Indonesia."

³⁵ Irvan and Setiawan, "CRIMINALIZATION POLICY OF DEEPFAKE IN INDONESIAN ELECTIONS"; Nurkholisah et al., "Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan Kriminalisasi Dalam Hukum Pidana Indonesia"; Hasnia et al., "Reconstruction of Criminal Law Policy in Handling Cyber Crime: Perspectives of Technology Law and Human Rights."

³⁶ Aruan and Rahmayanti, "The Development of Cybercrime as a Criminal Offense in the Digital Era and Its Impact on Society"; Ernasari and Naib, "CRIMINAL LAW REFORM IN THE FACE OF THE SOCIETY 5.0 ERA AGAINST CYBER CRIME"; Hasnia et al., "Reconstruction of Criminal Law Policy in Handling Cyber Crime: Perspectives of Technology Law and Human Rights."

³⁷ Judijanto, Utama, and Setiawan, "Implementation of Ethical Artificial Intelligence Law to Prevent the Use of AI in Spreading False Information (Deepfake) in Indonesia"; Silalahi and Dachi, "Pertanggung Jawaban Hukum Platform Media Sosial Terhadap Penyebaran Konten Deepfake Berbasis Artificial Intelligence Dalam Kasus Penipuan Berkedok Ritual Uang Gaib Ujang Busthomi"; Rahayu and Kuswandi, "The Deepfake Phenomenon as a New Form of Cybercrime from a Criminological Perspective."

Enforcement and forensic capacity. Beyond doctrinal gaps, enforcement is systematically constrained by weak digital forensic infrastructure, limited institutional capacity to authenticate AI-generated media, the availability of anonymity tools, unresolved cross-border jurisdictional questions, and poor inter-agency coordination between cybercrime units, data-protection authorities, and communications regulators.³⁸ Comparative evidence suggests that provenance-verification technologies, such as blockchain-based content attribution, could partially offset these constraints by giving investigators a technically verifiable trail for synthetic content, a capability largely absent from Indonesia's current enforcement toolkit.³⁹

Victim protection and social vulnerability. Victim-centered studies show that survivors of deepfake pornography and sextortion face compounding harms because criminal procedure offers limited pathways for rapid content takedown, psychological support, or reputational remediation, and because the burden of proving synthetic origin often falls on victims themselves.⁴⁰ Low public digital literacy compounds this vulnerability, since it reduces the population's capacity to detect manipulated content before it spreads and increases the likelihood that victims will not recognize or report deepfake-enabled abuse promptly.⁴¹

The comparative review suggests that Indonesia's reform path need not choose between criminalization and expression-protective regulation, but can combine elements of both. South Korea's experience shows that targeted criminal

³⁸ Nurkholisah et al., "Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan Kriminalisasi Dalam Hukum Pidana Indonesia"; Irvan and Setiawan, "CRIMINALIZATION POLICY OF DEEPFAKE IN INDONESIAN ELECTIONS"; Triana, Periani, and Atyanta, "Closing Indonesia's Regulatory Gap on Deepfake Crimes: Comparative Lessons from the European Union, the United States, and China"; Rangkuti et al., "Analisis Yuridis Terhadap Penggunaan Deepfake Dalam Pelanggaran UU ITE"; Arvitto, "Implikasi Hukum Deepfake: Telaah Terhadap UU ITE Dan UU PDP."

³⁹ Astari and Setiyono, "The Criminalization of Deepfakes Through Blockchain: Constructing Transnational Criminal Law in the Era of Artificial Intelligence."

⁴⁰ Reza, Utama, and Yuningsih, "Artificial Intelligence–Generated Deepfake Pornography: A Normative Analysis of Criminal Liability and Victim Protection in Indonesian Law"; Siti Nur Hidayah and Gunawan Hadi Purwanto, "Legal Protection of Victims of AI-Driven Deepfake Pornography," *Al-Risalah Jurnal Ilmu Syariah Dan Hukum*, 2026, <https://doi.org/10.24252/al-risalah.vi.63687>; Athalia Pranata Putri Meliala and Indah Sri Utari, "POLICY ON THE FORMULATION OF ARTIFICIAL INTELLIGENCE ACCOUNTABILITY FOR THE CREATION AND DISSEMINATION OF DEEPFAKE VIDEOS FROM A CRIMINAL LAW PERSPECTIVE IN INDONESIA," *Law Research Review Quarterly*, 2026, <https://doi.org/10.15294/lrrq.v12i2.44714>; Tobing and Yuli, "Criminal Liability for the Creation and Distribution of Deepfake Pornographic Videos on Social Media."

⁴¹ Rahayu and Kuswandi, "The Deepfake Phenomenon as a New Form of Cybercrime from a Criminological Perspective"; Irvan and Setiawan, "CRIMINALIZATION POLICY OF DEEPFAKE IN INDONESIAN ELECTIONS"; Rangkuti et al., "Analisis Yuridis Terhadap Penggunaan Deepfake Dalam Pelanggaran UU ITE"; Devi, "Implikasi Hukum Terhadap Penyalahgunaan Teknologi Deepfake Untuk Pemerasan (Sextortion) Dalam Perspektif Hukum Teknologi Informasi Di Indonesia."

offences for non-consensual sexual deepfakes can be defined with sufficient precision to avoid chilling legitimate expression, while the European Union's transparency-and-labelling model demonstrates that disclosure obligations can address political and informational deepfakes without resorting to criminal sanction for every instance of synthetic content.⁴² The United States' fragmented state-level approach, by contrast, illustrates the costs of leaving deepfake regulation to uncoordinated sub-national action, a cautionary lesson for Indonesia's own currently fragmented sectoral framework.⁴³

Comparative lessons and reform priorities. Benchmarked against the European Union's platform-accountability model, the United States' rapidly expanding statutory patchwork, and China's provider-obligation regime, Indonesia's current framework is comparatively reactive: it neither imposes labeling or provenance obligations on platforms nor establishes a dedicated criminal offense for synthetic-media misuse.⁴⁴ The reviewed literature converges on a multi-layered reform agenda rather than criminalization alone, combining an explicit statutory definition of deepfake, a *lex specialis* offense structured around intent and harm rather than technology alone, strengthened digital forensic capacity, platform and content-provenance obligations, and sustained digital literacy programming.⁴⁵ This layered framing is consistent with the broader finding that Indonesian criminal law, taken alone, is structurally unable to keep pace with a harm that is simultaneously legal, technological, and social in character.⁴⁶

⁴² Mubarak et al., "A Survey on the Detection and Impacts of Deepfakes in Visual, Audio, and Textual Formats"; Ong, Afdal, and Tantimin, "PERBANDINGAN PENGATURAN SANKSI PENIPUAN ONLINE BERBASIS ARTIFICIAL INTELLIGENCE: INDONESIA VS AMERIKA."

⁴³ Ong, Afdal, and Tantimin, "PERBANDINGAN PENGATURAN SANKSI PENIPUAN ONLINE BERBASIS ARTIFICIAL INTELLIGENCE: INDONESIA VS AMERIKA."

⁴⁴ Triana, Periani, and Atyanta, "Closing Indonesia's Regulatory Gap on Deepfake Crimes: Comparative Lessons from the European Union, the United States, and China"; Astari and Setiyono, "The Criminalization of Deepfakes Through Blockchain: Constructing Transnational Criminal Law in the Era of Artificial Intelligence."

⁴⁵ Irvan and Setiawan, "CRIMINALIZATION POLICY OF DEEPPFAKE IN INDONESIAN ELECTIONS"; Dwiandari and Arifin, "Criminal Law Enforcement on Digital Identity Misuse in AI Era for Commercial Interests in Indonesia"; Triana, Periani, and Atyanta, "Closing Indonesia's Regulatory Gap on Deepfake Crimes: Comparative Lessons from the European Union, the United States, and China"; Fitriani et al., "KEBIJAKAN FORMULASI TINDAK PIDANA DEEPPFAKE DALAM UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK (UU ITE) DAN UNDANG-UNDANG PELINDUNGAN DATA PRIBADI (UU PDP) DI INDONESIA"; Gunawan, "When Artificial Intelligence Becomes a Criminal Tool: Urgency of Criminal Law Policy Against Data Theft in Indonesia"; Patricia Morisa Banfatin et al., "Pengaturan Hukum Pidana Di Indonesia Terhadap Penyalahgunaan Teknologi Artificial Intelligence Deepfake Dalam Melakukan Tindak Pidana Cybercrime," *Pemuliaan Keadilan*, 2024, <https://doi.org/10.62383/pk.v2i1.402>.

⁴⁶ Dwiandari and Arifin, "Criminal Law Enforcement on Digital Identity Misuse in AI Era for Commercial Interests in Indonesia"; Sariasa et al., "The Existence of Deepfake Artificial Intelligence As a Means Of Crime In The Perspective Of Indonesia's Positive Law."

Comparative analysis remains underdeveloped in the Indonesian literature, with existing work largely limited to a bilateral comparison of online-fraud sanctions between Indonesia and the United States, which finds that Indonesia's general fraud and ITE provisions impose less predictable and less AI-specific liability than emerging US state-level frameworks.⁴⁷ Broadening this comparison, the international detection-and-impact literature suggests that jurisdictions have converged on three broad regulatory models: targeted criminalization of specific harms (notably non-consensual sexual deepfakes), transparency-and-disclosure mandates for AI-generated content, and platform-accountability regimes that shift part of the enforcement burden onto intermediaries.⁴⁸ Table 1 summarizes how these models are reflected in Indonesia, the United States, the European Union, and South Korea.

Jurisdiction	Regulatory Approach to Deepfake	Legal Basis	Key Limitation
Indonesia	No standalone deepfake statute; relies on general ITE, KUHP, PDP, TPKS, and Pornography provisions applied by analogy.	UU ITE, KUHP, UU PDP, UU TPKS, UU Pornografi	Fragmented, reactive, and lacking a technical-legal definition of deepfake.
United States	Mixed federal-state model; several states criminalize non-consensual deepfake pornography and election-related synthetic media, alongside emerging	State deepfake statutes; federal civil-remedy legislation	Jurisdictional fragmentation across states; uneven coverage of political deepfakes.

⁴⁷ Ong, Afdal, and Tantimin, "PERBANDINGAN PENGATURAN SANKSI PENIPUAN ONLINE BERBASIS ARTIFICIAL INTELLIGENCE: INDONESIA VS AMERIKA."

⁴⁸ Mubarak et al., "A Survey on the Detection and Impacts of Deepfakes in Visual, Audio, and Textual Formats."

Jurisdiction	Regulatory Approach to Deepfake	Legal Basis	Key Limitation
	federal civil remedies.		
European Union	Transparency-based regulation requiring disclosure/labelling of AI-generated or manipulated content, integrated with data-protection and platform-accountability rules.	EU AI Act; GDPR; Digital Services Act	Emphasis on disclosure rather than direct criminalization of malicious creation.
South Korea	Explicit criminal sanctions for the production and distribution of sexually exploitative deepfakes, with enhanced penalties for use against minors.	Sexual Violence Punishment Act (amended)	Narrower scope focused on sexual-content harms; limited coverage of fraud and disinformation.

Table 1. *Comparative regulatory approaches to deepfake across selected jurisdictions.*

This comparison indicates that, unlike South Korea's targeted criminalization of sexually exploitative deepfakes or the European Union's transparency-based model under the AI Act, Indonesia has neither a dedicated offence definition nor

a disclosure mandate, leaving synthetic-media harms to be absorbed-imperfectly-by statutes designed for earlier forms of electronic misconduct.⁴⁹

The Ideal Legal Regulatory Framework (*Ius Constituendum*) for Addressing Deepfakes in Indonesia

The ideal legal framework for regulating deepfake technology in Indonesia should be proactive rather than merely reactive to incidents that have already occurred. The existing literature demonstrates a consistent trend advocating a shift from relying on dispersed provisions contained in the Electronic Information and Transactions Law (ITE Law), the Personal Data Protection Law (PDP Law), the Pornography Law, the Law on the Crime of Sexual Violence (TPKS Law), the Copyright Law, and the Indonesian Criminal Code (KUHP) toward a comprehensive and dedicated legal regime specifically governing deepfake technology.⁵⁰ Such a framework should not focus solely on criminalization but should consistently encompass clear legal definitions, rules on liability, victim remedies, forensic standards, platform obligations, and the enhancement of public digital literacy.⁵¹

From the perspective of regulatory design, the ideal framework should begin by establishing a legal definition of deepfake that encompasses AI-generated or AI-manipulated audio, video, and image content created or altered with the intent to deceive, cause harm, or misuse another person's identity.⁵² The same legislation

⁴⁹ Ong, Afdal, and Tantimin, "PERBANDINGAN PENGATURAN SANKSI PENIPUAN ONLINE BERBASIS ARTIFICIAL INTELLIGENCE: INDONESIA VS AMERIKA"; Arvito, "Implikasi Hukum Deepfake: Telaah Terhadap UU ITE Dan UU PDP."

⁵⁰ Nurkholisah et al., "Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan Kriminalisasi Dalam Hukum Pidana Indonesia"; Triana, Periani, and Atyanta, "Closing Indonesia's Regulatory Gap on Deepfake Crimes: Comparative Lessons from the European Union, the United States, and China"; Wanggai, Hartono, and Parwati, "Analisis Normatif Terhadap Penyebaran Deepfake Sebagai Bentuk Kejahatan Siber Di Indonesia"; Ong, Afdal, and Tantimin, "PERBANDINGAN PENGATURAN SANKSI PENIPUAN ONLINE BERBASIS ARTIFICIAL INTELLIGENCE: INDONESIA VS AMERIKA."

⁵¹ Rama, Lofandri, and Saputra, "Legal Gaps in Indonesia's Electronic Information and Transactions Law in Addressing Deepfake Technology: Challenges and Regulatory Recommendations"; Ivan and Setiawan, "CRIMINALIZATION POLICY OF DEEPFAKE IN INDONESIAN ELECTIONS"; Triana, Periani, and Atyanta, "Closing Indonesia's Regulatory Gap on Deepfake Crimes: Comparative Lessons from the European Union, the United States, and China"; Adria Fathan Mahmuda, Mahesa Cakra Gusti, and Mhd. Faruq Anrusfi, "Exploring the Potential Crimes and Legal Liability of Artificial Intelligence within the Framework of Indonesian Criminal Law," *Ex Aequo Et Bono Journal Of Law*, 2025, <https://doi.org/10.61511/eaebjol.v2i2.2025.1385>.

⁵² Rama, Lofandri, and Saputra, "Legal Gaps in Indonesia's Electronic Information and Transactions Law in Addressing Deepfake Technology: Challenges and Regulatory Recommendations"; Judijanto, Utama, and Setiyawan, "Implementation of Ethical Artificial Intelligence Law to Prevent the Use

should also establish specific criminal offenses for the malicious creation, dissemination, and use of deepfake technology, rather than requiring law enforcement authorities to broadly interpret general provisions relating to false information, defamation, or public morality.⁵³ The structure of these offenses should distinguish among different categories of harm according to their context, as the literature consistently identifies deepfake pornography, fraud, political disinformation, identity misuse, and privacy violations as distinct forms of legal harm.⁵⁴ Furthermore, several studies emphasize that sanctions must comply with the principles of legal certainty, proportionality, and an appropriate balance with freedom of expression. Accordingly, criminal liability should depend on factors such as intent, the harm caused, the existence or absence of consent, and exceptions serving the public interest, rather than imposing broad restrictions on speech.⁵⁵

At the institutional level, the ideal framework requires harmonization between a new Deepfake Law and the existing ITE Law, PDP Law, Pornography Law, TPKS Law, Copyright Law, and the Indonesian Criminal Code.⁵⁶ Legal responsibility should be attributed to natural persons—including developers, operators, users, or distributors of deepfake content—rather than to artificial

of AI in Spreading False Information (Deepfake) in Indonesia”; Nurkholisah et al., “Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan Kriminalisasi Dalam Hukum Pidana Indonesia.”

⁵³ Judijanto, Utama, and Setiyawan, “Implementation of Ethical Artificial Intelligence Law to Prevent the Use of AI in Spreading False Information (Deepfake) in Indonesia”; Muhammad Ilham Alfathoni, B Pratama, and Cherilla Izzata Putri Lubis, “Legal Protection for Victims of Deepfake Pornography in Terms of Criminal Law,” *Andalas Law Journal*, 2024, <https://doi.org/10.25077/alj.v9i2.90>; Ocktave Ferdinal and Herman Bakir, “Legal Protection Efforts and Policies to Combat Deepfake Porn Crimes with Artificial Intelligence (AI) in Indonesia,” *Journal of Multidisciplinary Sustainability Asean*, 2024, <https://doi.org/10.70177/ijmsa.v1i6.1822>; Wanggai, Hartono, and Parwati, “Analisis Normatif Terhadap Penyebaran Deepfake Sebagai Bentuk Kejahatan Siber Di Indonesia.”

⁵⁴ Triana, Periani, and Atyanta, “Closing Indonesia’s Regulatory Gap on Deepfake Crimes: Comparative Lessons from the European Union, the United States, and China”; Sariasa et al., “The Existence of Deepfake Artificial Intelligence As a Means Of Crime In The Perspective Of Indonesia’s Positive Law”; Wanggai, Hartono, and Parwati, “Analisis Normatif Terhadap Penyebaran Deepfake Sebagai Bentuk Kejahatan Siber Di Indonesia”; Mahmuda, Gusti, and Anrusfi, “Exploring the Potential Crimes and Legal Liability of Artificial Intelligence within the Framework of Indonesian Criminal Law.”

⁵⁵ Nurkholisah et al., “Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan Kriminalisasi Dalam Hukum Pidana Indonesia”; Judijanto, Utama, and Setiyawan, “Implementation of Ethical Artificial Intelligence Law to Prevent the Use of AI in Spreading False Information (Deepfake) in Indonesia”; Mugi Lestari and Riza Ibrahim, “Legal Aspects of Using Deepfake in Political Campaigns: A Threat to Democracy?,” *International Journal of Humanities, Law, and Politics*, 2025, <https://doi.org/10.46336/ijhlp.v3i1.193>.

⁵⁶ Nurkholisah et al., “Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan Kriminalisasi Dalam Hukum Pidana Indonesia”; Ferdinal and Bakir, “Legal Protection Efforts and Policies to Combat Deepfake Porn Crimes with Artificial Intelligence (AI) in Indonesia”; Guntur Permana Putra and M Multazam, “LAW ENFORCEMENT AGAINST DEEPPAKE PORN AI,” *European Journal of Contemporary Business Law & Technology: Cyber Law, Blockchain, and Legal Innovations*, 2024, <https://doi.org/10.61796/ejcbt.v1i9.1015>.

intelligence systems themselves.⁵⁷ In addition, digital platform providers should be legally required to implement content labeling, content removal (takedown) procedures, content traceability mechanisms, and active cooperation with law enforcement authorities.⁵⁸ Strengthening AI forensic capabilities and establishing standardized evidentiary protocols should likewise constitute integral components of this framework⁵⁹, together with guarantees of victims' rights to file complaints, obtain prompt removal of harmful content, invoke the right to be forgotten, and pursue both civil remedies and criminal prosecution.⁶⁰

Victim protection represents one of the defining characteristics consistently identified in the proposed legal framework, particularly in cases involving non-consensual deepfake pornography, given that the current legal regime continues to leave victims vulnerable to psychological, social, privacy-related, and dignitary harms.⁶¹ This necessitates explicit legal rights to the prompt removal of unlawful content, assistance in obtaining and presenting evidence, accessible complaint mechanisms, and comprehensive remedies through both civil and criminal proceedings.⁶² Several studies further argue that victim protection should adopt a gender-sensitive and substantively equitable approach, considering that non-consensual deepfake pornography disproportionately affects women, while

⁵⁷ Mahmuda, Gusti, and Anrusfi, "Exploring the Potential Crimes and Legal Liability of Artificial Intelligence within the Framework of Indonesian Criminal Law"; Ong, Afdal, and Tantimin, "PERBANDINGAN PENGATURAN SANKSI PENIPUAN ONLINE BERBASIS ARTIFICIAL INTELLIGENCE: INDONESIA VS AMERIKA."

⁵⁸ Triana, Periani, and Atyanta, "Closing Indonesia's Regulatory Gap on Deepfake Crimes: Comparative Lessons from the European Union, the United States, and China"; Lianingsih and Jaizul, "Legal Implications of the Use of Deepfake in Politics and National Security in Indonesia"; Lestari and Ibrahim, "Legal Aspects of Using Deepfake in Political Campaigns: A Threat to Democracy?"

⁵⁹ Irvan and Setiawan, "CRIMINALIZATION POLICY OF DEEPFAKE IN INDONESIAN ELECTIONS"; Nurkholisah et al., "Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan Kriminalisasi Dalam Hukum Pidana Indonesia"; Triana, Periani, and Atyanta, "Closing Indonesia's Regulatory Gap on Deepfake Crimes: Comparative Lessons from the European Union, the United States, and China."

⁶⁰ Putra and Multazam, "LAW ENFORCEMENT AGAINST DEEPFAKE PORN AI"; Evyta Rosiyanti Ramadhani, Ayudya Rizqi Rachmawati, and Roro Hera Kurnikova, "Integrating Islamic Values with the Right to Be Forgotten: A Legal Approach to Addressing Deepfake Pornography in Indonesia," *De Jure: Jurnal Hukum Dan Syar'iah*, 2025, <https://doi.org/10.18860/j-fsh.v17i1.28880>.

⁶¹ Elang Rinjani Utara and Anis Widiyati, "Analysis of Criminal Law Enforcement on Non-Consensual Deepfake Pornography in the Dissemination of Manipulative Content in Indonesia," *Al-Jinayah : Jurnal Hukum Pidana Islam*, 2025, <https://doi.org/10.15642/aj.2025.11.1.125-153>; Ferdinal and Bakir, "Legal Protection Efforts and Policies to Combat Deepfake Porn Crimes with Artificial Intelligence (AI) in Indonesia"; Ramadhani, Rachmawati, and Kurnikova, "Integrating Islamic Values with the Right to Be Forgotten: A Legal Approach to Addressing Deepfake Pornography in Indonesia."

⁶² Ferdinal and Bakir, "Legal Protection Efforts and Policies to Combat Deepfake Porn Crimes with Artificial Intelligence (AI) in Indonesia"; Putra and Multazam, "LAW ENFORCEMENT AGAINST DEEPFAKE PORN AI"; Ramadhani, Rachmawati, and Kurnikova, "Integrating Islamic Values with the Right to Be Forgotten: A Legal Approach to Addressing Deepfake Pornography in Indonesia."

existing law enforcement practices frequently create additional procedural obstacles for victims.⁶³ Strengthening the implementation of the right to be forgotten under the Personal Data Protection Law—particularly through amendments to existing limitations on data deletion that currently undermine the removal of non-consensual deepfake content—has repeatedly been proposed as an essential legal reform.⁶⁴

Finally, the governance model proposed in the literature extends beyond a purely criminal law approach by integrating multi-stakeholder oversight, artificial intelligence ethics, forensic technologies, and public education.⁶⁵ Scholars consistently recommend embedding the principles of transparency, accountability, and fairness from the earliest stages of legislative drafting so that the regulation of deepfake technology does not depend solely on the imposition of sanctions after harm has occurred.⁶⁶ Comparative studies identify three regulatory features as particularly relevant for Indonesia: the risk-based and transparency-oriented regulatory model adopted by the European Union, the use of specific criminal offenses and liability rules developed in the United States, and broader expectations regarding platform accountability and mandatory content labeling.⁶⁷ Preventive measures also receive considerable emphasis, as low levels of digital literacy, inadequate detection systems, and the rapid dissemination of content through digital platforms are repeatedly identified as major obstacles to effective law enforcement. Consequently, the ideal legal framework should also incorporate

⁶³ Utara and Widyawati, “Analysis of Criminal Law Enforcement on Non-Consensual Deepfake Pornography in the Dissemination of Manipulative Content in Indonesia”; Alfathoni, Pratama, and Lubis, “Legal Protection for Victims of Deepfake Pornography in Terms of Criminal Law.”

⁶⁴ Ramadhani, Rachmawati, and Kurnikova, “Integrating Islamic Values with the Right to Be Forgotten: A Legal Approach to Addressing Deepfake Pornography in Indonesia”; Judijanto, Utama, and Setiawan, “Implementation of Ethical Artificial Intelligence Law to Prevent the Use of AI in Spreading False Information (Deepfake) in Indonesia.”

⁶⁵ Rama, Lofandri, and Saputra, “Legal Gaps in Indonesia’s Electronic Information and Transactions Law in Addressing Deepfake Technology: Challenges and Regulatory Recommendations”; Juan Pratama, “Ethical Deepfake Governance: EU AI Act Benchmarks and Indonesia Multi-Stakeholder Responses,” *Jurist-Diction*, 2026, <https://doi.org/10.20473/jd.v9i1.80885>; Irvan and Setiawan, “CRIMINALIZATION POLICY OF DEEFAKE IN INDONESIAN ELECTIONS”; Lianingsih and Jaizul, “Legal Implications of the Use of Deepfake in Politics and National Security in Indonesia.”

⁶⁶ Judijanto, Utama, and Setiawan, “Implementation of Ethical Artificial Intelligence Law to Prevent the Use of AI in Spreading False Information (Deepfake) in Indonesia.”

⁶⁷ Triana, Periani, and Atyanta, “Closing Indonesia’s Regulatory Gap on Deepfake Crimes: Comparative Lessons from the European Union, the United States, and China”; Judijanto, Utama, and Setiawan, “Implementation of Ethical Artificial Intelligence Law to Prevent the Use of AI in Spreading False Information (Deepfake) in Indonesia”; Lianingsih and Jaizul, “Legal Implications of the Use of Deepfake in Politics and National Security in Indonesia.”

nationwide digital literacy campaigns, inter-agency coordination, and collaboration with technology companies.⁶⁸

Building on the doctrinal and comparative findings, four reform priorities emerge from the literature. First, Indonesia should enact a clear statutory definition of deepfake and explicitly criminalize its malicious creation and distribution, closing the legal vacuum identified in Section 4.1.⁶⁹ Second, the ITE Law, the Personal Data Protection Law, the Criminal Code, the Pornography Law, and the Sexual Violence Crimes Law should be harmonized into a more integrated framework, reducing the normative vagueness documented across harm domains.⁷⁰ Third, forensic capacity, automated detection systems, and platform accountability mechanisms should be expanded to enable faster identification and takedown of harmful synthetic content, addressing the enforcement barriers identified in Section 4.3.⁷¹ Fourth, any criminalization strategy must be calibrated against freedom-of-expression and human-rights safeguards, since vague digital-speech provisions risk chilling legitimate satire, commentary, and artistic use of synthetic media.⁷²

Conclusion

This article set out to evaluate whether Indonesian criminal law is doctrinally and institutionally adequate to protect digital society against deepfake-

⁶⁸ Irvan and Setiawan, “CRIMINALIZATION POLICY OF DEEPPAKE IN INDONESIAN ELECTIONS”; Lianingsih and Jaizul, “Legal Implications of the Use of Deepfake in Politics and National Security in Indonesia”; Lestari and Ibrahim, “Legal Aspects of Using Deepfake in Political Campaigns: A Threat to Democracy?”; Ramadhani, Rachmawati, and Kurnikova, “Integrating Islamic Values with the Right to Be Forgotten: A Legal Approach to Addressing Deepfake Pornography in Indonesia.”

⁶⁹ Nurkholisah et al., “Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan Kriminalisasi Dalam Hukum Pidana Indonesia”; Rama, Lofandri, and Saputra, “Legal Gaps in Indonesia’s Electronic Information and Transactions Law in Addressing Deepfake Technology: Challenges and Regulatory Recommendations”; Rahayu and Kuswandi, “The Deepfake Phenomenon as a New Form of Cybercrime from a Criminological Perspective.”

⁷⁰ Nurkholisah et al., “Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan Kriminalisasi Dalam Hukum Pidana Indonesia”; Handoko, “Digital Crime In The Era Of Society 5.0: Juridical Analysis Of Cyber And Victim Protection”; Jumentoro and Firdausy, “Transhumanistic Cybercrime Analysis Using a Posthuman Criminology Approach to Digital Identity Threats in Artificial Intelligence Era.”

⁷¹ Rahayu and Kuswandi, “The Deepfake Phenomenon as a New Form of Cybercrime from a Criminological Perspective”; Silalahi and Dachi, “Pertanggung Jawaban Hukum Platform Media Sosial Terhadap Penyebaran Konten Deepfake Berbasis Artificial Intelligence Dalam Kasus Penipuan Berkedok Ritual Uang Gaib Ujang Busthomi”; Mubarak et al., “A Survey on the Detection and Impacts of Deepfakes in Visual, Audio, and Textual Formats.”

⁷² Judijanto, Utama, and Setiawan, “Implementation of Ethical Artificial Intelligence Law to Prevent the Use of AI in Spreading False Information (Deepfake) in Indonesia”; Hasnia et al., “Reconstruction of Criminal Law Policy in Handling Cyber Crime: Perspectives of Technology Law and Human Rights.”

enabled cybercrime. The findings demonstrate that the current legal framework is not yet adequate, as no statute explicitly defines or criminalizes deepfake as a distinct offense. Instead, existing laws including the Electronic Information and Transactions Law (ITE Law), the Indonesian Criminal Code (KUHP), the Personal Data Protection Law (PDP Law), and the Pornography Law address deepfake-related conduct only through indirect and interpretive application, resulting in legal uncertainty and inconsistent enforcement. The study further concludes that Indonesia requires a proactive and comprehensive legal framework that moves beyond fragmented sectoral regulations toward a dedicated legal regime specifically governing deepfake technology. Such a framework should incorporate an explicit statutory definition of deepfake, a purpose-built *lex specialis* offense, stronger digital forensic capacity, platform accountability, and sustained public digital literacy initiatives to ensure more effective protection of digital society.

For policymakers, these findings provide a practical basis for designing a comprehensive regulatory framework that is harmonized with existing criminal, data protection, and electronic transaction laws while responding to the evolving risks posed by AI-generated content. Strengthening inter-agency coordination, expanding AI-based digital forensic capabilities, and establishing standardized evidentiary procedures should become key priorities to improve the effectiveness of law enforcement against deepfake-related cybercrime. In addition, law enforcement agencies and digital platform providers should adopt both preventive and responsive measures through transparent content-labeling mechanisms, rapid takedown procedures, and stronger cooperation in identifying harmful synthetic media. Expanding nationwide digital literacy programs will further complement these legal reforms by increasing public awareness of deepfake risks and strengthening Indonesia's capacity to protect its digital society from emerging forms of AI-enabled cybercrime.

References

- Arvitto, R. S. (2025). Implikasi hukum deepfake: Telaah terhadap UU ITE dan UU PDP. *Jurnal Ilmiah Hukum dan Hak Asasi Manusia*, 4(2). <https://doi.org/10.35912/jihham.v4i2.3937>
- Astari, F. A., & Setiyono, J. (2026). The criminalization of deepfakes through blockchain: Constructing transnational criminal law in the era of artificial intelligence. *International Journal of Social Science and Human Research*, 9(5). <https://doi.org/10.47191/ijsshr/v9-i5-126>
- Banfatin, P. M., Medan, K., F.Ng, D., & Fallo. (2024). Pengaturan hukum pidana di Indonesia terhadap penyalahgunaan teknologi artificial intelligence deepfake

- dalam melakukan tindak pidana cybercrime. *Pemuliaan Keadilan*, 2(1).
<https://doi.org/10.62383/pk.v2i1.402>
- Devi, W. Z. (2026). Implikasi hukum terhadap penyalahgunaan teknologi deepfake untuk pemerasan (sextortion) dalam perspektif hukum teknologi informasi di Indonesia. *Majelis: Jurnal Hukum Indonesia*, 3(1).
<https://doi.org/10.62383/majelis.v3i1.1504>
- Dwiandari, A. S., & Arifin, R. (2025). Criminal law enforcement on digital identity misuse in AI era for commercial interests in Indonesia. *The Indonesian Journal of International Clinical Legal Education*, 7(1).
<https://doi.org/10.15294/iccle.v7i1.25525>
- Fitriani, N., & Wahyudi, E. (2026). Kebijakan formulasi tindak pidana deepfake dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Pelindungan Data Pribadi (UU PDP) di Indonesia. *Jurnal Hukum To-ra: Hukum untuk Mengatur dan Melindungi Masyarakat*, 12(1).
<https://doi.org/10.55809/tora.v12i1.647>
- Frensh, W. (2025). Criminal policy toward the crime of defamation in cyberspace through the use of deepfake AI. *Jurnal Akta*, 12(2).
<https://doi.org/10.30659/akta.v12i2.44884>
- Gunawan, H. (2025). When artificial intelligence becomes a criminal tool: Urgency of criminal law policy against data theft in Indonesia. *Jurnal Idea Hukum*, 11(2).
<https://doi.org/10.20884/1.jih.2025.11.2.665>
- Hidayah, S. N., & Purwanto, G. H. (2026). Legal protection of victims of AI-driven deepfake pornography. *Al-Risalah: Jurnal Ilmu Syariah dan Hukum*.
<https://doi.org/10.24252/al-risalah.vi.63687>
- Irvan, R., & Setiawan, J. H. (2026). Criminalization policy of deepfake in Indonesian elections. *Constitutional Law Society*, 5(1). <https://doi.org/10.36448/jcls.v5i1.125>
- Meliala, A. P. P., & Utari, I. S. (2026). Policy on the formulation of artificial intelligence accountability for the creation and dissemination of deepfake videos from a criminal law perspective in Indonesia. *Law Research Review Quarterly*, 12(2). <https://doi.org/10.15294/lrrq.v12i2.44714>
- Nurkholisah, S., Rismana, 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).
<https://doi.org/10.26623/julr.v8i3.13060>

- Rahayu, A., & Kuswandi. (2025). The deepfake phenomenon as a new form of cybercrime from a criminological perspective. *Indonesian Journal of Law and Justice*, 3(2). <https://doi.org/10.47134/ijlj.v3i2.5171>
- Rama, A., Lofandri, W., & Saputra, A. F. (2025). Legal gaps in Indonesia's electronic information and transactions law in addressing deepfake technology: Challenges and regulatory recommendations. *SCHOULID: Indonesian Journal of School Counseling*. <https://doi.org/10.23916/o86155011>
- Rangkuti, P. R., Hasibuan, R. F. A., Witama, V., Nasution, M. A., Kholizah, S., Andini, N., & Salmiah, S. (2025). Analisis yuridis terhadap penggunaan deepfake dalam pelanggaran UU ITE. *Depositi: Jurnal Publikasi Ilmu Hukum*, 3(2). <https://doi.org/10.59581/deposisi.v3i2.5080>
- Reza, D., Utama, M., & Yuningsih, H. (2026). Artificial intelligence-generated deepfake pornography: A normative analysis of criminal liability and victim protection in Indonesian law. *Ius Poenale*, 7(1). <https://doi.org/10.25041/ip.v7i1.4738>
- Aruan, T., & Rahmayanti, R. (2025). The development of cybercrime as a criminal offense in the digital era and its impact on society. *Discourse Journal on Law and Society*. <https://doi.org/10.70062/djls.v1i3.81>
- Arvitto, R. S. (2025). Implikasi hukum deepfake: Telaah terhadap UU ITE dan UU PDP. *Jurnal Ilmiah Hukum dan Hak Asasi Manusia*, 4(2). <https://doi.org/10.35912/jihham.v4i2.3937>
- Ernasari, N., & Naib. (2024). Criminal law reform in the face of the society 5.0 era against cyber crime. *International Journal of Accounting, Management, Economics and Social Sciences (IJAMESC)*, 2(6). <https://doi.org/10.61990/ijamesc.v2i6.383>
- Hailtik, A. G. E., & Afifah, W. (2024). Criminal responsibility of artificial intelligence committing deepfake crimes in Indonesia. *Asian Journal of Social and Humanities*, 2(4). <https://doi.org/10.59888/ajosh.v2i4.222>
- Handoko, W. (2025). Digital crime in the era of society 5.0: Juridical analysis of cyber and victim protection. *Ipsa Jure*. <https://doi.org/10.62872/6991g409>
- Hasnia, H., Hafiz, A., Rasna, R., Nurahman, D., & Parhusip, J. (2025). Reconstruction of criminal law policy in handling cyber crime: Perspectives of technology law and human rights. *Jurnal Smart Hukum (JSH)*, 3(3). <https://doi.org/10.55299/jsh.v3i3.1328>
- Irvan, R., & Setiawan, J. H. (2026). Criminalization policy of deepfake in Indonesian elections. *Constitutional Law Society*, 5(1). <https://doi.org/10.36448/jcls.v5i1.125>

- Judijanto, L., Utama, A. S., & Setiyawan, H. (2025). Implementation of ethical artificial intelligence law to prevent the use of AI in spreading false information (deepfake) in Indonesia. *The Easta Journal Law and Human Rights*, 3(2). <https://doi.org/10.58812/eslhr.v3i02.470>
- Jumantoro, T. R. P., & Firdausy, M. K. (2025). Transhumanistic cybercrime analysis using a posthuman criminology approach to digital identity threats in artificial intelligence era. *Priviet Social Sciences Journal*, 5(9). <https://doi.org/10.55942/pssj.v5i9.558>
- Lianingsih, N., & Jaizul, A. (2025). Legal implications of the use of deepfake in politics and national security in Indonesia. *International Journal of Humanities, Law, and Politics*, 3(1). <https://doi.org/10.46336/ijhlp.v3i1.190>
- Maan, M. K. P., Amalo, H., & Dede, N. (2025). Analisis perlindungan hukum terhadap penyimpangan artificial intelligence dalam tindak pidana deepfake pornografi berdasarkan hukum pidana. *Jurnal Riset Rumpun Ilmu Sosial, Politik dan Humaniora*, 4(1). <https://doi.org/10.55606/jurrish.v4i1.5071>
- Mubarak, R., Alsboui, T. A. A., Alshaikh, O., Inuwa-Dutse, I., Khan, S., & Parkinson, S. (2023). A survey on the detection and impacts of deepfakes in visual, audio, and textual formats. *IEEE Access*, 11, 144497-144529. <https://doi.org/10.1109/access.2023.3344653>
- Nurkholisah, S., Rismana, 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). <https://doi.org/10.26623/julr.v8i3.13060>
- Ong, H. W., Afdal, W., & Tantimin. (2025). Perbandingan pengaturan sanksi penipuan online berbasis artificial intelligence: Indonesia vs Amerika. *Jurnal Hukum To-ra: Hukum Untuk Mengatur dan Melindungi Masyarakat*, 11(2). <https://doi.org/10.55809/tora.v11i2.579>
- Rama, A., Lofandri, W., & Saputra, A. F. (2025). Legal gaps in Indonesia's electronic information and transactions law in addressing deepfake technology: Challenges and regulatory recommendations. *SCHOULID: Indonesian Journal of School Counseling*. <https://doi.org/10.23916/086155011>
- Reza, D., Utama, M., & Yuningsih, H. (2026). Artificial intelligence-generated deepfake pornography: A normative analysis of criminal liability and victim protection in Indonesian law. *Ius Poenale*, 7(1). <https://doi.org/10.25041/ip.v7i1.4738>
- Silalahi, W., & Dachi, F. N. (2026). Pertanggungjawaban hukum platform media sosial terhadap penyebaran konten deepfake berbasis artificial intelligence dalam kasus penipuan berkedok ritual uang gaib Ujang Busthomi. *Politika Progresif: Jurnal Hukum, Politik dan Humaniora*, 3(2). <https://doi.org/10.62383/progres.v3i2.3110>

- Tobing, R. N. A., & Yuli, Y. (2026). Criminal liability for the creation and distribution of deepfake pornographic videos on social media. *Eduvest - Journal of Universal Studies*, 6(2). <https://doi.org/10.59188/eduvest.v6i2.52738>
- Wanggai, F. R. M., Hartono, M. S., & Parwati, N. P. E. (2026). Analisis normatif terhadap penyebaran deepfake sebagai bentuk kejahatan siber di Indonesia. *Majelis: Jurnal Hukum Indonesia*, 3(1). <https://doi.org/10.62383/majelis.v3i1.1509>
- Sariasa, G., Madhusodani, N. L. M., A.P, D. A. A., & Parwati, N. P. E. (2024). The existence of deepfake artificial intelligence as a means of crime in the perspective of Indonesia's positive law. *Proceedings of the 6th International Conference on Law, Social Sciences and Education (ICLSSE 2024)*. <https://doi.org/10.4108/eai.17-10-2024.2353690>
- Tobing, R. N. A., & Yuli, Y. (2026). Criminal liability for the creation and distribution of deepfake pornographic videos on social media. *Eduvest – Journal of Universal Studies*, 6(2). <https://doi.org/10.59188/eduvest.v6i2.52738>
- Triana, I., Periani, A., & Atyanta, A. (2026). Closing Indonesia's regulatory gap on deepfake crimes: Comparative lessons from the European Union, the United States, and China. *Kosmik Hukum*, 26(2). <https://doi.org/10.30595/kosmikhukum.v26i2.25751>
- Wanggai, F. R. M., Hartono, M. S., & Parwati, N. P. E. (2026). Analisis normatif terhadap penyebaran deepfake sebagai bentuk kejahatan siber di Indonesia. *Majelis: Jurnal Hukum Indonesia*, 3(1). <https://doi.org/10.62383/majelis.v3i1.1509>.