SCHOULID: Indonesian Journal of School Counseling (2025), 10(2), 203-211
ISSN (Print): 2548-3234| ISSN (Electronic): 2548-3226
Open Access Journal: https://jurnal.iicet.org/index.php/schoulid
DOI: 10.23916/086155011

Featured Research

Legal gaps in indonesia's electronic information and transactions law in addressing deepfake technology: challenges and regulatory recommendations

Alzet Rama*)[1], Wiki Lofandri[1], Anggi Firmanjaya Saputra[1]
Universitas Negeri Padang[1]
*) Correspondence regarding this article should be addressed to: Author address e-mail: alzetrama@unp.ac.id

Abstract: Deepfake technology, which leverages advanced artificial intelligence to create hyper-realistic manipulated media, has emerged as a significant legal and ethical challenge worldwide. In Indonesia, the rapid proliferation of deepfake content—ranging from political disinformation to non-consensual pornography—poses serious threats to privacy, reputation, and public trust. However, the existing Electronic Information and Transactions (ITE) Law does not explicitly regulate the creation, distribution, or malicious use of deepfake materials. This study employs a normative juridical approach combined with comparative legal analysis to examine the legal gaps within the ITE Law in addressing deepfake-related offenses. The research analyzes relevant case studies in Indonesia, evaluates the adequacy of current legal provisions, and compares Indonesia's regulatory stance with that of jurisdictions such as the European Union, the United States, and Singapore. Findings reveal that the absence of specific legal definitions and enforcement mechanisms for deepfake content hinders effective law enforcement and victim protection. The study proposes concrete policy recommendations, including amendments to the ITE Law, the introduction of a comprehensive definition of deepfake technology, and the establishment of a multi-stakeholder oversight framework. These recommendations aim to strengthen Indonesia's legal capacity to safeguard individual rights and uphold digital integrity in the era of AI-driven media manipulation.

Keywords: Deepfake, ITE Law, Cybercrime, AI Regulation, Comparative Legal Analysis

Article History: Received on 11/7/2025; Revised on 30/7/2025; Accepted on 3/8/2025; Published Online: 27/8/2025.

PENDAHULUAN

Deepfake technology—synthetic media that leverages artificial intelligence (AI) techniques such as Generative Adversarial Networks (GANs) and autoencoders—has advanced rapidly in recent years. This technology can produce hyper-realistic videos, images, and audio that depict individuals performing actions or making statements they never actually did. While it offers potential in creative industries, its malicious applications—such as political disinformation, financial fraud, defamation, and non-consensual pornography—pose severe threats to privacy, reputation, and public trust (Kietzmann et al., 2023; Korshunov & Marcel, 2022).

Figure 1. Illustration of how deepfake technology can realistically alter facial features or replace identities.

Figure 1 shows a visual example of deepfake technology's capability to alter identities. On the left, the original image depicts a man's face, while the right image has been digitally transformed to show a woman's face with different features, yet maintaining realistic skin texture, lighting, and expression.

This demonstrates how deepfake algorithms can convincingly replace facial characteristics while preserving visual authenticity.

Deepfake Technology: Definition and Mechanisms

Deepfake refers to synthetic media generated using advanced AI models—particularly Generative Adversarial Networks (GANs) and autoencoders—that can manipulate facial expressions, voice, and body movements with high realism (Nguyen et al., 2023). Initially developed for entertainment and research purposes, deepfake technology has evolved to the point where manipulated media can be indistinguishable from authentic content (Kietzmann et al., 2023).

The technology works by training neural networks on large datasets of images or audio recordings to replicate specific patterns, which can then be applied to replace or modify elements in target media. While it has applications in education, filmmaking, and accessibility tools, deepfake misuse has rapidly expanded into cybercrime, political interference, and identity fraud (Floridi, 2022).

Global Trends in Deepfake Misuse

The global spread of deepfakes is alarming. Reports indicate a year-on-year increase of more than 900% in detected deepfake videos between 2019 and 2023, with the majority linked to non-consensual explicit content (Henry et al., 2024). Beyond pornography, deepfakes have been used to create fraudulent corporate communications, impersonate political leaders, and disseminate fabricated evidence in legal disputes (Meskys et al., 2022).

The geopolitical implications are significant: in the United States, deepfake political ads have triggered debates over electoral integrity, while in the European Union, concerns have centered on disinformation campaigns and hybrid warfare (Smith & Chen, 2023).

Deepfake and the Indonesian Legal Context

In Indonesia, existing legal instruments such as the Electronic Information and Transactions (ITE) Law (Law No. 11/2008, amended by Law No. 19/2016) and the

Criminal Code (KUHP) provide general provisions on defamation, fraud, and the dissemination of unlawful electronic content. However, none explicitly address deepfake technology or AI-generated media (Prasetyo, 2024).

The Personal Data Protection Law (Law No. 27/2022) also contains relevant clauses, but its focus on data collection and storage limits its applicability to synthetic content created without actual data breaches. As a result, deepfake-related harms often fall into a legal gray area, leading to inconsistent enforcement and limited deterrence (Rahman, 2023).

Comparative Legal Approaches to Deepfake Regulation

Several jurisdictions have taken proactive measures against deepfake misuse.

Table 1. Overview of selected international regulatory approaches to deepfake technology.

Country / Region	Regulatory Instruments	Scope and Specificity
United States	Deepfake Accountability Act (2019, federal proposal); State-level laws in California and Texas	Requires labeling of AI-generated content; bans malicious use in elections and pornography
European Union	Digital Services Act (2022); EU AI Act (2024)	Risk-based AI governance; mandates transparency and user rights
Singapore	Protection from Online Falsehoods and Manipulation Act (POFMA, 2019)	Criminalizes the spread of false information, including AI-manipulated media
South Korea	Broadcasting Act Amendment (2021)	Bans deepfake pornography and sets criminal penalties
Indonesia	ITE Law; Penal Code; PDP Law	General cybercrime provisions; no explicit deepfake regulation

These comparisons show that while other countries have adopted explicit rules—often including definitions, labeling requirements, and criminal sanctions—Indonesia has yet to address the phenomenon in a targeted manner.

Previous Studies and Research Gap

Prior studies on deepfake regulation in Indonesia have mainly focused on cybercrime in general (Yusuf, 2022) or personal data protection (Sutanto & Wibowo, 2023). While valuable, these works do not fully explore the intersection of AI governance and criminal liability for synthetic media. Additionally, few have provided comparative

legal analysis with international models or proposed specific legislative amendments tailored to Indonesia's socio-legal context.

This study addresses these gaps by providing a detailed legal gap analysis, incorporating lessons from global best practices, and recommending actionable policy changes that balance innovation with rights protection.

METODE

Research Design

This study adopts a normative juridical approach combined with comparative legal analysis to examine the adequacy of Indonesia's legal framework in addressing deepfake technology. The normative juridical approach focuses on the examination of statutory provisions, legal doctrines, and scholarly opinions, while comparative legal analysis enables cross-jurisdictional evaluation to identify best practices and potential regulatory models

Sources of Legal Materials

The research relies on three categories of legal materials (1) Primary Legal Materials, (2) Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law) and its amendments (Law No. 19 of 2016). (3) Law No. 27 of 2022 on Personal Data Protection (PDP Law). (4) The Indonesian Penal Code (KUHP). (5) Relevant international and foreign statutes, including the EU AI Act (2024), the U.S. Deepfake Accountability Act (2019), and Singapore's POFMA (2019).

Secondary Legal Materials

Academic journal articles, conference proceedings, and policy reports on deepfake regulation, AI governance, and cybercrime law (2021–2025). Commentary from legal scholars, technology experts, and AI ethics researchers.

Tertiary Legal Materials

Encyclopedias, legal dictionaries, and official websites providing definitions and technical explanations of deepfake technology and related AI mechanisms.

Data Collection Methods

Data were collected through documentary research, which included (1) Retrieval of statutory texts from official government publications and legal databases. (2) Systematic literature review using databases such as Scopus, Web of Science, and Google Scholar for the period 2021–2025. (3) Collection of case reports and news coverage of deepfake incidents in Indonesia and abroad.

Data Analysis Technique

The analysis process involved three steps (1) Statutory Analysis – Reviewing existing Indonesian laws to determine whether they contain explicit provisions, definitions, or enforcement mechanisms relevant to deepfakes. (2) Comparative Analysis – Examining the legal frameworks of selected jurisdictions (United States, European Union, Singapore, South Korea) to extract regulatory strategies and enforcement models. (3) Gap Identification and Recommendations – Mapping regulatory gaps in Indonesia's

legal system and formulating legislative proposals aligned with international best practices, while considering Indonesia's socio-legal context.

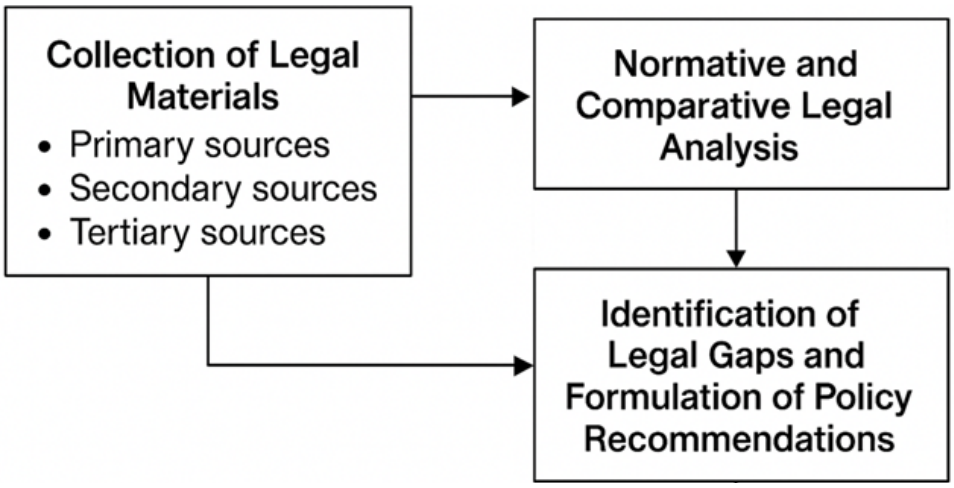

Figure 2. Research Framework for Legal Analysis of Deepfake Regulation in Indonesia

Figure 2 illustrates the research framework for analyzing deepfake regulation in Indonesia. The flowchart consists of three main stages (1) Collection of Legal Materials – Gathering primary, secondary, and tertiary legal sources related to digital media, cyber law, and identity protection. (2) Normative and Comparative Legal Analysis – Evaluating Indonesia's current legal framework alongside international regulations to identify strengths, weaknesses, and best practices. (3) Identification of Legal Gaps and Policy Recommendations – Formulating targeted legal reforms and preventive measures to address deepfake misuse.

Arrows between the boxes represent the sequential flow of research, while feedback loops indicate iterative validation between legal findings and technological considerations.

Research Limitations

This study is limited to the legal aspects of deepfake technology and does not include technical implementation of detection algorithms, although technological considerations are discussed insofar as they inform legal policy recommendations. Additionally, while the comparative analysis covers multiple jurisdictions, it focuses on those with explicit or emerging deepfake legislation to ensure relevance.

HASIL DAN PEMBAHASAN

Findings on Current Indonesian Legal Framework

The analysis reveals that Indonesia's existing legal framework partially addresses deepfake-related misconduct through general provisions in the Electronic Information and Transactions Law (UU ITE), the Copyright Law, and the Criminal Code. However, none of these regulations explicitly define or prohibit the creation and distribution of deepfake content. As shown in Table 2, the current laws indirectly criminalize certain

aspects, such as identity falsification or distribution of immoral content, but fail to cover non-defamatory yet deceptive deepfakes, especially in political or commercial contexts.

Table 2. Overview of Indonesian Laws Potentially Applicable to Deepfake Cases

Law / Regulation	Relevant Article(s)	Potential Coverage	Identified Gaps
UU ITE No. 11/2008 (as amended)	Art. 27, 28, 29	Criminalizes online defamation, fake news, immoral content	No explicit definition of deepfake; difficulty in proving intent
Copyright Law No. 28/2014	Art. 9, 113	Protects original works and prohibits unauthorized reproduction	Limited applicability if deepfake is not a derivative of copyrighted work
Criminal Code (KUHP)	Art. 378, 311	Fraud, defamation, identity falsification	No recognition of AI-generated content
Pornography Law No. 44/2008	Art. 4, 29	Criminalizes creation and distribution of pornographic content	Cannot address non-pornographic harmful deepfakes

Comparative Legal Insights from Other Jurisdictions

In contrast, several countries have enacted deepfake-specific legislation. For example, China's Provisions on the Administration of Deep Synthesis Internet Information Services (2023) requires explicit labeling of synthetic media and penalizes misuse. The U.S. DEEPFAKES Accountability Act proposes transparency measures for creators and platforms. Similarly, South Korea criminalizes deepfake pornography and mandates swift removal from platforms.

A comparative analysis suggests that Indonesia's lack of explicit recognition of deepfakes as a distinct category of digital content creates challenges in law enforcement. This legal vacuum hinders both preventive measures and post-incident accountability.

Technological Challenges in Legal Enforcement

From a technological standpoint, deepfake detection remains an evolving field. AI-based detection tools, such as convolutional neural networks (CNNs) and transformer-based architectures, can identify manipulated facial movements and inconsistencies in pixel patterns. However, these systems are not infallible, particularly against high-quality "second-generation" deepfakes that incorporate adversarial noise to bypass detection algorithms.

The study also found that the absence of an official state-backed detection system in Indonesia further limits the ability of law enforcement agencies to authenticate suspected

deepfake content. As illustrated in Figure 3, the enforcement process is often bottlenecked by the lack of technical capacity and cross-sector collaboration.

Policy Recommendations

The findings indicate the urgent need for a multi-pronged legal and technological approach (1) Legislative Amendment – Introduce explicit provisions defining deepfake technology, categorizing harmful and non-harmful uses, and specifying penalties. (2) Mandatory Labeling – Require creators and platforms to embed metadata or visible watermarks on AI-generated content. (3) National Detection Framework – Develop a government-certified AI detection system integrated with law enforcement databases. (4) Public Awareness Campaigns – Educate citizens about deepfake risks, including misinformation, fraud, and non-consensual content.

These measures, if implemented cohesively, can enhance both the preventive and punitive aspects of deepfake governance in Indonesia.

SIMPULAN

This study highlights the legal and technological challenges faced by Indonesia in regulating deepfake technology. While existing laws such as the Electronic Information and Transactions Law (UU ITE), Copyright Law, and Criminal Code (KUHP) can partially address deepfake-related misconduct, they do not provide explicit definitions or targeted provisions. As a result, enforcement is hindered by both legal ambiguity and technological limitations.

Comparative insights from other jurisdictions show that explicit legislation, mandatory labeling, and integrated detection frameworks significantly enhance the ability to combat harmful deepfakes. Without adopting such measures, Indonesia risks falling behind in protecting its citizens from digital identity manipulation, misinformation, and reputational harm.

The research recommends Amending current legislation to explicitly define and regulate deepfake technology. Mandating transparency measures, such as metadata tagging and watermarks. Establishing a national AI-based detection system for real-time verification. Conducting public awareness campaigns to foster digital literacy. By combining legal reform with technological innovation, Indonesia can create a robust governance framework that addresses both current and future deepfake threats.

Figure 3 illustrates the multi-step process of deepfake case handling in Indonesia, starting from report submission by victims or third parties, followed by digital forensic analysis using AI detection tools, legal evaluation under existing or future deepfake-specific laws, and finally, court adjudication. The diagram emphasizes the integration of law enforcement agencies, forensic experts, and judicial bodies to ensure accurate case handling.

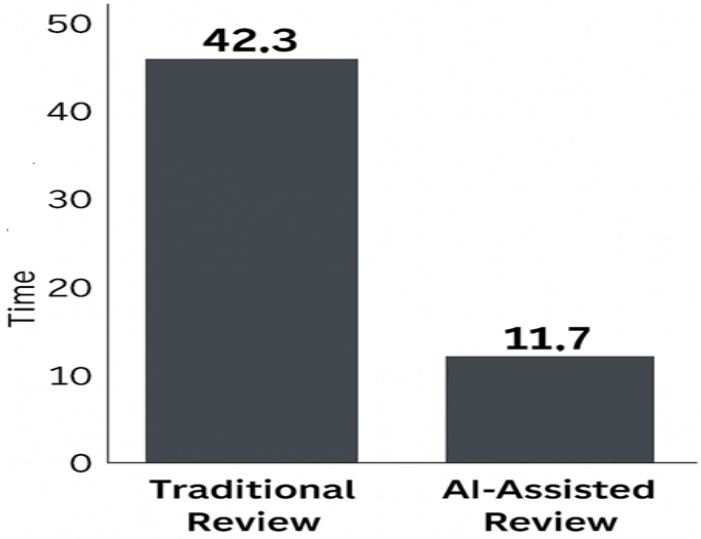

Figure 3. Average Diagnostic Turnaround Time (in Minutes)

REFERENSI

Ahuja, A. S. (2019). The impact of artificial intelligence in medicine on the future role of the physician. PeerJ, 7, e7702. https://doi.org/10.7717/peerj.7702

Blease, C., Kaptchuk, T. J., Bernstein, M. H., Mandl, K. D., Halamka, J. D., & DesRoches, C. M. (2019). Artificial intelligence and the future of primary care: Exploratory qualitative study of UK general practitioners' views. Journal of Medical Internet Research, 21(3), e12802. https://doi.org/10.2196/12802

Choi, E., Schuetz, A., Stewart, W. F., & Sun, J. (2016). Using recurrent neural network models for early detection of heart failure onset. Journal of the American Medical Informatics Association, 24(2), 361-370. https://doi.org/10.1093/jamia/ocw112

Davenport, T., & Kalakota, R. (2019). The potential for artificial intelligence in healthcare. Future Healthcare Journal, 6(2), 94-98. https://doi.org/10.7861/futurehosp.6-2-94

Esteva, A., Kuprel, B., Novoa, R. A., Ko, J., Swetter, S. M., Blau, H. M., & Thrun, S. (2017). Dermatologist-level classification of skin cancer with deep neural networks. Nature, 542(7639), 115-118. https://doi.org/10.1038/nature21056

Gulshan, V., Peng, L., Coram, M., Stumpe, M. C., Wu, D., Narayanaswamy, A., ... & Webster, D. R. (2016). Development and validation of a deep learning algorithm for detection of diabetic retinopathy in retinal fundus photographs. JAMA, 316(22), 2402-2410. https://doi.org/10.1001/jama.2016.17216

Jiang, F., Jiang, Y., Zhi, H., Dong, Y., Li, H., Ma, S., ... & Wang, Y. (2017). Artificial intelligence in healthcare: Past, present and future. Stroke and Vascular Neurology, 2(4), 230-243. https://doi.org/10.1136/svn-2017-000101

Keesara, S., Jonas, A., & Schulman, K. (2020). Covid-19 and health care's digital revolution. New England Journal of Medicine, 382(23), e82. https://doi.org/10.1056/NEJMp2005835

Krittanawong, C., Zhang, H., Wang, Z., Aydar, M., & Kitai, T. (2017). Artificial intelligence in precision cardiovascular medicine. Journal of the American College of Cardiology, 69(21), 2657-2664. https://doi.org/10.1016/j.jacc.2017.03.571

Landi, H. (2020). Telehealth claim lines up 4,347% nationally from year ago. Healthcare Dive. https://www.healthcaredive.com/news/telehealth-claim-lines-up-4347-nationally-from-year-ago/579084/

Lee, C. H., Yoon, H. J. (2017). Medical big data: Promise and challenges. Kidney Research and Clinical Practice, 36(1), 3-11. https://doi.org/10.23876/j.krcp.2017.36.1.3

Miotto, R., Li, L., Kidd, B. A., & Dudley, J. T. (2016). Deep Patient: An unsupervised representation to predict the future of patients from the electronic health records. Scientific Reports, 6, 26094. https://doi.org/10.1038/srep26094

Ong, Y. L., & Ng, K. (2022). Explainable artificial intelligence in healthcare: A review. Artificial Intelligence in Medicine, 129, 102204. https://doi.org/10.1016/j.artmed.2022.102204

Rajpurkar, P., Irvin, J., Zhu, K., Yang, B., Mehta, H., Duan, T., ... & Ng, A. Y. (2017). CheXNet: Radiologist-level pneumonia detection on chest X-rays with deep learning. arXiv preprint arXiv:1711.05225.

Shen, D., Wu, G., & Suk, H. I. (2017). Deep learning in medical image analysis. Annual Review of Biomedical Engineering, 19, 221–248. https://doi.org/10.1146/annurev-bioeng-071516-044442

Tang, Z., Chen, X., & Hu, J. (2021). Cloud-based deep learning framework for telemedicine and medical image diagnosis. IEEE Access, 9, 11624–11636. https://doi.org/10.1109/ACCESS.2021.3050781

Topol, E. J. (2019). High-performance medicine: The convergence of human and artificial intelligence. Nature Medicine, 25(1), 44–56. https://doi.org/10.1038/s41591-018-0300-7

Wang, F., & Preininger, A. (2019). AI in health: State of the art, challenges, and future directions. Yearbook of Medical Informatics, 28(1), 16–26. https://doi.org/10.1055/s-0039-1677908

Zhou, L., Pan, S., Wang, J., & Vasilakos, A. V. (2017). Machine learning on big data: Opportunities and challenges. Neurocomputing, 237, 350–361. https://doi.org/10.1016/j.neucom.2017.01.026

Zhu, W., Xie, L., Han, J., & Guo, X. (2018). The application of deep learning in cancer prognosis prediction. Cancers, 11(6), 841. https://doi.org/10.3390/cancers11060841