OPEN ACCESS

LAW RESEARCH
Review Quarterly

Law Research Review Quarterly is a **Journal for Law, Justice, and Crime in Indonesia and Southeast Asia**. The Journal is a peer-reviewed journal published by Faculty of Law, State University of Semarang, Indonesia. The Journal published quarterly on February, May, August, and November. ISSN 2716-3415 (Online)
Online at https://journal.unnes.ac.id/journals/snh

Policy on the Formulation of *Artificial Intelligence Accountability* for the Creation and Dissemination of Deepfake Videos from a Criminal Law Perspective in Indonesia

Athalia Pranata Putri S Meliala
Universitas Negeri Semarang, Semarang, Indonesia
athaliapranata02@students.unnes.ac.id

Indah Sri Utari
Universitas Negeri Semarang, Semarang, Indonesia
indahsuji@mail.unnes.ac.id

Abstract

The advancement of *Generative Adversarial Network* (GAN) technology has enabled deepfakes to facilitate serious crimes in Indonesia, including non-consensual pornography, public figure impersonation, and political disinformation. This study analyzes Indonesia's existing criminal law framework regarding *AI-based deepfake* accountability and proposes ideal policy reforms. Using normative legal research with legislative, conceptual, and comparative approaches, this study identifies significant normative gaps (lex lacuna) across the ITE Law, the New Criminal Code or *Kitab Undang-Undang Hukum Pidana* (KUHP), and the Personal Data Protection (PDP) Law. Key deficiencies include the absence of a legal definition of deepfakes, no comprehensive accountability mechanism

covering the AI production chain, and difficulties applying mens rea principles given AI system autonomy. Comparative analysis of the EU AI Act and China's Deep Synthesis Regulations reveals that effective regulation requires a layered accountability model: strict liability for AI developers, vicarious liability for platform operators, and direct liability for end users. This framework should be complemented by mandatory synthetic content labeling and harmonization with the PDP Law and New Criminal Code as lex generalis. This study recommends either enacting a dedicated Artificial Intelligence Bill or revising the ITE Law to explicitly criminalize deepfake creation and dissemination. Such reform is essential to establish legal certainty, close existing normative gaps, and strengthen public protection against AI-facilitated crimes in Indonesia.

Keywords: *Artificial Intelligence*; *Deepfake*; Criminal Liability; Formulation Policy; Indonesian Criminal Law.

Introduction

The development of artificial *intelligence* (AI) technology in the last two decades has brought fundamental changes in various aspects of human life, ranging from the economy, health, education, to communication and media. One of the most significant and controversial breakthroughs in AI advances is the emergence of *deepfake technology*, which is an artificial intelligence-based audiovisual content manipulation technique that allows the replacement, imitation, or hyper-realistic reconstruction of a person's face, voice, and expression in a video. The technology has its roots in the development *of Generative Adversarial Networks* (GAN), a deep learning architecture introduced in 2014, in which two artificial neural networks, namely generators and discriminators, compete with each other to produce

synthetic content that is increasingly close to reality.[1]GAN's ability to produce convincing visual content has opened the door to a wide range of legitimate creative applications, but at the same time creates a serious threat to the security, privacy, and public trust in digital content.

In Indonesia, *the deepfake* phenomenon has caused an increasingly worrying real impact. Various cases of abuse of this technology have been reported, ranging from the spread of *pornographic deepfake* videos that use the faces of public figures without consent known as *non-consensual intimate imagery* (NCII) to the creation of disinformation videos that show state officials or political leaders as if to make statements they have never spoken.[2] This phenomenon is compounded by the fact that deepfake creation tools are now freely available and easily accessible through internet-based applications, even by users without a deep technical background. Global research from cybersecurity agencies such as Sensity AI reveals that the vast majority of *deepfake* content circulating on the internet is pornographic, and the majority of victims are women.[3] This trend continues to increase exponentially, with recent reports noting a hundreds of percent spike in the volume of malicious deepfake content every year.[4] This data confirms that *deepfakes* are not just a technical issue, but an urgent human rights issue that needs to be dealt with legally.[5]

---

[1] Dara Sawitri, "Artificial Intelligence for a Digital Technology Smart Society in the Era of Society 5.0," *Journal of Artificial Intelligence and Software Engineering (J-AISE)* 5, no. 1 (March 2025): 135, https://doi.org/10.30811/jaise.v5i1.6441.

[2] S.W. Nurdin and I.F. Nugraha, "Deepfake Threats and AI-Based Disinformation: Implications for Cybersecurity and Indonesian National Stability," *JIMR: Journal of International Multidisciplinary Research* 4, no. 1 (June 2025): 73-92, https://doi.org/10.62668/jimr.v4i01.1551.

[3] Sensity AI, State of Deepfakes 2024 (annual report); AI Asia Pacific Institute, "Unmasking the Era of Misinformation: Navigating the Threat of Deepfakes," February 15, 2024, https://aiasiapacific.org/2024/02/15/unmasking-the-era-of-misinformation-navigating-the-threat-of-deepfakes/.

[4] Arash Heidari et al., "Deepfake detection using deep learning methods: A systematic and comprehensive review," in *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 14, no. 2, preprint, John Wiley and Sons Inc, March 1, 2024, https://doi.org/10.1002/widm.1520.

[5] Ali Masyhar and Indah Sri Utari, "Policing and Human Rights: Analyzing Excessive Use of Force in Indonesian Law Enforcement," *Contemporary Issues on Indonesian Human Rights Law and Policy* 2, no. 2 (2025), https://doi.org/10.65815/6zp8et83.

This is where a fundamental legal issue arises: who should be held criminally responsible for the creation and dissemination of AI-based *deepfake* videos? This question is much more complex than it seems on the surface. When an individual uses a deep learning-based AI application to create *a deepfake* video that harms others, there are at least three parties involved in the chain of crime: the developer who creates the AI system, the platform operator who provides the AI-based service to the public, and the end user who actively operates the technology with malicious intent.[6] In conventional criminal law doctrine, the concept of criminal liability requires the existence of a perpetrator who can be identified as a subject of the law, namely a human or legal entity, who has the ability to be responsible, commit unlawful acts, and have mistakes in the form of intentionality (*dolus*) or forgetfulness (*culpa*). The problem is, when AI systems work autonomously in generating *deepfake* content, or when it is not clear whether users really understand the legal consequences of using such technology, the application of conventional criminal liability constructions becomes very problematic.[7] This ambiguity creates a legal loophole that can be exploited by criminals to evade the reach of the law.[8]

Examining the positive legal regulations that apply in Indonesia, it is clear that the existing legal apparatus has not been able to adequately respond to the challenges posed by *AI-based deepfakes*. Law Number 11 of 2008 concerning Electronic Information and Transactions as amended several times (ITE Law) does regulate a number of acts related to digital content, such as the dissemination of immoral content in Article 27 paragraph (1), the spread of fake news in Article 28 paragraph (1), and the

[6] Deva Wayan Zenitia, "Legal Implications for the Abuse of Deepfake Technology for Extortion in the Legal Perspective of Information Technology in Indonesia," *Assembly: Indonesian Law* Journal 3, no. 1(2026): 102-114, https://doi.org/10.62383/majelis.v3i1.1504.

[7] C.T. Noerman and A.L. Ibrahim, "Criminalization of Deepfakes in Indonesia as a Form of State Protection," *Journal of USM Law Review* 7, no. 2 (2024): 603, https://doi.org/10.26623/julr.v7i2.8995.

[8] Itok Kurniawan, "Analysis of Artificial Intelligence as a Subject of Criminal Law," *Mutiara: Indonesian Multidisciplinary Scientific Journal* 1, no. 1 (July 2023): 35-44, https://doi.org/10.61404/jimi.vli1.4.

manipulation of electronic documents in Article 35.[9] However, the ITE Law does not mention the term "*deepfake*" or "AI-based synthetic content" at all, so its application to deepfake cases requires extensive interpretation that has the potential to create legal uncertainty.[10] Similarly, Law Number 1 of 2023 concerning the Criminal Code (New Criminal Code) which replaces the colonial legacy, despite having adopted various developments in modern criminal law doctrine, still uses the paradigm of the subject of human law conventionally without special arrangements on artificial intelligence or generative technology-based crimes.[11] Meanwhile, Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) provides protection for biometric data, including face and voice, as the main components exploited by *deepfakes*.[12] However, the scope of its criminal sanctions is more focused on the aspect of data processing without consent, rather than on the creation of harmful manipulative content. The three legal instruments still contain significant gaps in norms (*lex lacuna*) in dealing with the threat of *deepfakes*.

This condition is in stark contrast to regulatory developments in various countries that have been more advanced in responding to deepfake threats. The European Union has established *Regulation* (EU) 2024/1689 or *the EU Artificial Intelligence Act* (*EU AI Act*) which comes into force in 2024, classifying the risks of AI systems and requiring transparency on synthetic content, in particular through Article 50 which regulates the

[9] Law Number 11 of 2008 concerning Information and Electronic Transactions as last amended by Law Number 1 of 2024, Statute Book of the Republic of Indonesia of 2024.
[10] R.S. Arvitto, "Legal Implications of Deepfakes: A Study of the ITE Law and the PDP Law," *Scientific Journal of Law and Human Rights* 4, no. 2 (2025): 77, https://doi.org/10.35912/jihham.v4i2.3937.
[11] Hartono, "Normative Analysis of the Abuse of Deepfake Technology in Digital Political Campaigns as a Cybercrime Act based on Article 28 paragraph (2) of the ITE Law," *Muqoddimah Journal: Journal of Social, Political, and Humanities Sciences* 10, no. 1 (2026): 591-601, https://doi.org/10.31604/jim.v10i1.2026.591-601.
[12] Law Number 27 of 2022 concerning Personal Data Protection, Statute Book of the Republic of Indonesia of 2022.

obligation to label *deepfakes*.[13] China through the Administrative Provisions on *Deep Synthesis* Internet Information Services published by *the Cyberspace Administration of China* (CAC) and effective from January 10, 2023 which requires the labeling of synthetic content, requires consent from the individual whose face is used, and imposes strict sanctions on violators.[14]The United States through a number of states such as California, Virginia, and Minnesota has enacted regulations that specifically criminalize *deepfakes*, pornography, and *deepfakes* in the context of elections. Indonesia's lagging behind in terms of this regulation not only creates legal uncertainty for victims and law enforcement, but also makes Indonesia a relatively free space for the spread of dangerous deepfake content, given the low criminal risk faced by perpetrators.[15]

Departing from this normative and empirical reality, the urgency of formulating criminal law policies that are adaptive to the development of AI and *deepfakes* in Indonesia can no longer be ignored. Criminal law reform in this context is not just a reactive effort to commit crimes, but rather a proactive step in building a legal architecture that is able to anticipate and prevent potential misuse of AI technology in the future. The policy of formulating the criminal law in question must be able to answer three crucial questions at once: what is criminalized (criminalization), who is responsible (the subject of accountability), and how to make the sanctions proportionate and effective (criminalization).[16] Within this framework, the approach needed is not just to add one or two articles to existing laws, but

[13] European Parliament and Council, Regulation (EU) 2024/1689 of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), Official Journal of the European Union L 2024/1689, July 12, 2024, art. 50.

[14] Cyberspace Administration of China (CAC), Ministry of Industry and Information Technology (MIT), and Ministry of Public Security (MPS), Provisions on the Administration of Deep Synthesis of Internet Information Services（深度合成互联网信息服务管理规定, November 25, 2022, effective January 10, 2023.

[15] Laili Rahmawati, "Legal Policy in the Regulation of Artificial Intelligence in Indonesia," *Journal of Law and Development* 54, no. 1 (2024).

[16] N.P.M. Putri, M.S. Hartono, and I.D.G.H. Yudiawan, "Analysis of Reformulation of Criminal Liability of Deepfake Technology Users in Artificial Intelligence-Based Defamation Crimes," *Pacta Sunt Servanda* Journal 5, no. 2 (2024), https://doi.org/10.23887/jpss.v512.5807.

rather a systematic and thorough rethinking of how Indonesia's criminal law should respond to the era of artificial intelligence.[17]

Based on the description above, this study formulates two main problems that will be studied in depth. *First*, what are the applicable criminal law arrangements in Indonesia in reaching out to accountability for the creation and dissemination of AI-based deepfake videos? *Second*, what is the ideal criminal law policy formulation to regulate AI accountability for the creation and dissemination of *deepfake* videos in Indonesia? These two questions are complementary: the first question is oriented to a diagnostic analysis of the existing positive legal conditions, while the second question is oriented towards a prescriptive construction in the form of policy formulations that can be used as a reference by lawmakers, law enforcers, and related stakeholders.

The purpose of this study is to analyze and identify the inadequacy of Indonesia's positive criminal law regulations in reaching accountability for crimes involving AI-based *deepfake* technology and to formulate an ideal and comprehensive criminal law policy formulation model as an answer to the norm vacuum. The benefits of this research can be reviewed from two aspects. Theoretically, this research is expected to contribute to the development of cyber criminal law in Indonesia, especially in building a concept of criminal accountability that is responsive to the dynamic and complex characteristics of AI technology. Practically, the results of this research are expected to be constructive input for the House of Representatives and the Government in the preparation of the Artificial Intelligence Bill, for law enforcement officials in understanding and handling *deepfake cases* that are increasingly rampant, and for the wider community in understanding the legal framework that protects them from the threat of AI-based crime.

[17] N. Cantika et al., "Criminal Liability for the Misuse of Artificial Intelligence (AI) in the Production of Hoax and Deepfake Content on Social Media," *Journal of School Leadership and Management* 10, no. 4 (December 2025): 2590-2599, https://doi.org/10.34125/jkps.v10i4.1435.

Method

This research uses the *normative legal research* method, which is research that examines law as norms, principles, principles, and doctrines to answer the legal problems faced.[18] The choice of this method is based on the consideration that the problems studied are normative, namely regarding the existence and adequacy of positive legal norms in reaching criminal liability for AI-based *deepfakes*, as well as formulating legal norms that should exist to fill these gaps. Legal science in the normative paradigm is prescriptive and applied in nature that does not only describe the law as it is (*lex lata*), but also provides an assessment of the law that should apply (*lex ferenda*).[19]

This study uses three approaches simultaneously. First, the statute approach by examining the ITE Law, the New Criminal Code, and the PDP Law and identifying the gaps in the norms in them. Second, a conceptual approach to build a concept of criminal accountability that is responsive to the characteristics of AI, departing from the views and doctrines that have developed in legal science. Third, a comparative approach by comparing Indonesian regulations with other country regulations such as the EU AI Act and China's Deep Synthesis regulations in order to obtain a comparative perspective that enriches the formulated legal prescriptions.[20]

The sources of legal materials used are divided into three types. Primary legal materials are in the form of authoritative and binding laws and regulations, including the 1945 Constitution of the Republic of Indonesia, the ITE Law, the New Criminal Code, the PDP Law, the EU AI Act (*Regulation* (EU) 2024/1689), and the *Deep Synthesis CAC 2022*

[18] Muhaimin, Legal Research Methods (Mataram: Mataram University Press, 2020), 59-60.
[19] Nur Solikin, Introduction to Legal Research Methodology (Pasuruan: CV. Qiara Media Publisher, 2021), 39.
[20] Muhaimin, Legal Research Methods, 69-70.

regulation. Secondary legal materials are in the form of law books, scientific journals, legal articles, and scientific papers related to criminal law, cyber law, and artificial intelligence. Tertiary legal materials are in the form of legal dictionaries, encyclopedias, and relevant technical reports.[21]

The technique of collecting legal materials is carried out through library *research* and *document study*, namely by searching, reading, identifying, and reviewing relevant legal materials both through physical libraries, digital legal databases, and official websites of state institutions and authorized international institutions.[22] The analysis of legal materials is carried out qualitatively through legal interpretation techniques, including grammatical, systematic, telelogical, and comparative interpretations, with a prescriptive-analytical nature of analysis. The conclusion is drawn using deductive reasoning, namely from general propositions in the form of legal norms and doctrines to answers to concrete legal issues that are the focus of this research, thus producing a prescription that can be used as a reference for the reform of Indonesian criminal law in the field of artificial intelligence.[23]

Results and Discussion

1. Criminal Law Regulations on the Making and Dissemination of Deepfake Videos in Indonesia

The development of artificial intelligence (AI) technology has given birth to the phenomenon of deepfakes, which is synthetic audiovisual content produced through advanced algorithms based on deep learning to manipulate a person's face, voice, and identity in such a way that it appears

[21] Muhaimin, Legal Research Methods, 72-75.
[22] Nur Solikin, Introduction to Legal Research Methods, 97.
[23] Muhaimin, Legal Research Methods, 81, 84.

authentic and difficult to distinguish from the original content.[24] Technically, *deepfakes* utilize *the Generative Adversarial Network* (GAN), an artificial neural network architecture consisting of two competing components, namely a generator and a discriminator, to produce high-quality synthetic content.[25] In Indonesia, the misuse of this technology has led to various real crimes ranging from the creation of *deepfake pornographic content* that manipulates the victim's face without consent, impersonation of public figures and state officials for the purpose of fraud, to the spread of political disinformation that endangers democratic stability. This reality demands a thorough evaluation of the extent to which Indonesia's positive criminal law is able to reach crimes that were basically unknown when existing regulations were formed.[26]

The first legal instrument that is most often used in dealing with dangerous deepfake content is the Electronic Information and Transaction Law (ITE Law), especially as amended for the second time through Law Number 1 of 2024. Article 27 paragraph (1) of the ITE Law prohibits everyone from deliberately and without the right to broadcast, perform, distribute, transmit, and/or make accessible information or electronic documents that have content that violates morality.[27] In the context of *deepfake* pornography, this article can literally reach the act of distributing content, considering that *deepfake videos* with sexual content disseminated through social media or digital platforms clearly meet the element of "distributing electronic information that violates morality". However, there is a fundamental problem that overshadows the application of this article:

[24] Indah Rohmawati, Amir Junaidi, and Ariy Khaerudin, "The Urgency of Deeptake Abuse Regulation as Online-Based Sexual Violence," *Innovative: Journal of Social Science Research* 4, no. 6 (2024): 1779-1794, https://doi.org/10.31004/innovative.v4i6.16559.

[25] R.S. Arvitto, "Legal Implications of Deepfake: A Study of the ITE Law and the PDP Law," 74.

[26] Muhammad Fagih Faathurrahman and Enni Soerjati Priowirjanto, "Accountability Arrangements for Perpetrators of Deepfakes Abuse in Artificial Intelligence Technology on Pornographic Content Based on Indonesian Positive Law," *Indonesian Journal of Social Technology* 3, no. 11 (November 2022): 1157-1158.

[27] Article 27 paragraph (1) jo. Article 45 paragraph (1) of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions.

the element *of dolus malus* or "deliberately" becomes particularly problematic when *deepfake* content is generated autonomously by an AI system without the direct involvement of the user in any stage of production.[28] The more sophisticated the AI systems used, the blurred the line between the "human intent" required by criminal law and the "algorithmic decisions" executed by machines.

In addition to the issue of immoral content, *deepfakes* are also often used to damage someone's good name by putting the victim's face in a situation of embarrassment or degradation of dignity that never happened at all. To reach this act, Article 27A of the ITE Law 1/2024 can be used which prohibits everyone from deliberately attacking the honor or good name of others by accusing something, with the intention that it is known to the public through an electronic system. However, the application of this article to *deepfakes* requires a special condition that is not always met, namely that the *deepfake* content is not accompanied by a description explaining its manipulative nature because if it is given information that the content is fabricated, the element of "alleging something" becomes unfulfilled.[29] This creates a protective vacuum: if *deepfake content* is spread under the label of satire or entertainment but still damages the reputation of the victim in real terms, the law does not provide an adequate instrument to ensnare the perpetrators.

Another dimension of *deepfake abuse* that is no less dangerous is its use as an instrument of disinformation and the spread of fake news. Article 28 paragraph (1) of the ITE Law 1/2024 prohibits the dissemination of electronic information containing false and misleading notifications that result in consumer losses, while Article 28 paragraph (2) prohibits the dissemination of information containing elements of hatred based on

[28] Faathurrahman and Priowirjanto, "Accountability Arrangements for Perpetrators of Deepfake Abuse," 1163.
[29] Directed by Amanda Uly Sijabat and Diana Lukitasari, "Deepfake Pornographic Image and Video Content as a Form of Defamation Crime," *Recidive: Journal of Criminal Law and Crime Prevention* 13, no. 2 (July 2024): 179-194, https://doi.org/10.20961/recidive.v13i2.86771.

ethnicity, religion, race, and intergroup (SARA).[30] The deepfake case of former President Joko Widodo's face giving a speech in Chinese in 2023 is a real example of how *deepfakes* are used to produce and spread political disinformation that has the potential to shake public trust. Although Article 28 of the ITE Law can in principle be applied in such cases, the fundamental weakness is that the articles are designed to reach the dissemination of static texts or content, rather than AI-based synthetic audiovisual content that has much higher persuasiveness and the potential for systemic damage to public trust and the stability of state institutions.

Another legal norm in the relevant ITE Law is Article 35 which prohibits everyone from deliberately and without rights or against the law from manipulating, creating, altering, disappearing, destroying electronic information and/or electronic documents with the aim of making the information considered as if it were authentic.[31] In terms of substance, Article 35 is technically most appropriate to ensnare the creation of *deepfakes*, because the act of manipulating someone's face using AI to then present it as if authentic is the essence of what the article means. The juridical analysis shows that the perpetrators of creating *deepfake* pornography meet all the elements of Article 35, given that the perpetrators consciously use AI to manipulate, alter, and create a person's face without permission into pornographic content which is all a form of manipulation of electronic documents. With a maximum penalty of 12 years in prison, Article 35 is actually a more appropriate instrument than Article 27 to reach the act of making *deepfakes*. But the problem remains the same, this article does not explicitly mention AI technology or *deepfakes*, so its application still depends on the interpretation of judges who require a deep technical understanding of how AI works.

[30] R.S. Arvitto, "The Legal Implications of Deepfake: A Study of the ITE Law and the PDP Law," 75.
[31] Article 35 jo. Article 51 paragraph (1) of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions.

The New Criminal Code passed through Law Number 1 of 2023 (hereinafter referred to as the New Criminal Code) carries several provisions that are partially relevant to deepfakes, although they have not yet explicitly regulated them. Article 407 of the New Criminal Code regulates the crime of pornography with a threat of imprisonment for a minimum of 6 months and a maximum of 10 years, expanding the scope of the previous pornography provisions.[32] In the context *of deepfake* pornography, this article can be applied to the act of producing, disseminating, and providing AI-based pornographic content. In addition, Articles 263 and 264 of the New Criminal Code on forgery of letters can historically be interpreted to include the forgery of audiovisual electronic documents, although their application to *deepfakes* still requires progressive interpretation by law enforcement officials. The most crucial thing is the fact that the New Criminal Code, like its predecessor, remains based on the paradigm that the subject of criminal law is human beings and corporations as persona standi in judicio. AI is not recognized as a legal subject so it cannot be held criminally accountable independently.[33] Moreover, the New Criminal Code philosophically still uses the doctrine *of geen straf zonder schuld* (no crime without fault) which requires that there be mistakes (*schuld*) in the form of intentionality or negligence on the part of the perpetrator, which is an element that is inherently not found in an AI system that works algorithmically.

The dimension of personal data protection in *deepfake crimes* is reached by Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). A person's face, voice, and biometric data are personal data that are specific and sensitive. Deepfakes inherently capture and process the victim's biometric data, specifically facial and voice imagery, without the legitimate consent of the owner. Article 65 paragraph (1) of the PDP Law

[32] Article 407 of Law Number 1 of 2023 concerning the Criminal Code.
[33] Ahmad Sofian, "The Conception of Legal Subjects and Criminal Responsibility of Artificial Intelligence," *Halu Oleo Law Review* 9, no. 1 (March 2025), https://doi.org/10.33561/holrev.v9i1.129.

prohibits everyone from obtaining or collecting personal data that does not belong to them or who does not have authority, and Article 67 paragraph (1) threatens the violation with a maximum prison sentence of 5 years and/or a maximum fine of IDR 5 billion.[34] Furthermore, Article 68 of the PDP Law also prohibits the falsification of personal data which can reach the use of biometric data to create false digital identities in *deepfakes*.[35] However, the PDP Law has significant structural limitations where it is designed with the main orientation on data protection and the relationship between data controllers and data subjects, rather than on the direct criminalization of AI-based manipulative content. The criminal dimension is limited and does not touch the entire spectrum of *deepfake* crimes, especially crimes related to content produced not just from data processing, but from identity engineering as a whole.

Based on the analysis of the three legal instruments, the ITE Law, the New Criminal Code, and the PDP Law, it can be concluded that Indonesia's positive criminal law faces a significant normative gap *(lex lacuna*) in reaching criminal liability for the creation and dissemination of AI-based *deepfake* videos. There are at least four norm gaps identified. First, there is no single regulation that provides a clear and firm legal definition of "*deepfake*", "AI-based synthetic content", or "artificial intelligence-engineered audiovisual content", so any application of the law relies on potentially inconsistent interpretations of judges.[36] Second, there is no provision on criminal liability that specifically targets *the deepfake* production chain from AI system developers, platform operators, to end-users, so the distribution of liability among these actors has no clear legal basis. Third, there is no legal obligation that requires digital platforms to proactively detect, label, and remove harmful *deepfake* content, so that

[34] Article 65 paragraph (1) and Article 67 paragraph (1) of Law Number 27 of 2022 concerning Personal Data Protection.
[35] Article 68 of Law Number 27 of 2022 concerning Personal Data Protection.
[36] Hukumonline, "What is Deepfake Porn and Criminal Snares for the Perpetrators," January 19, 2024, https://share.google/ptiF4ekrPt4VlYLM9.

platforms can take refuge behind the *safe harbor principle* regulated in the Minister of Communication and Information. Fourth and most fundamental, the principle *of mens rea* (malicious intent) in criminal law cannot be mechanically applied to AI systems that operate autonomously based on algorithms, not on free will.[37] These loopholes collectively create legal uncertainty that harms victims, opens loopholes for perpetrators to escape criminal accountability, and hinders law enforcement from effectively handling deepfake cases.[38]

Thus, the positive criminal law condition in Indonesia today can be described as being in a dilemma between an *inadequate* lex lata and an *urgent lex ferenda* that is urgently realized. The articles spread across the ITE Law, the New Criminal Code, and the PDP Law can be used as an emergency bridge in ensnaring *deepfakes* in certain contexts, but they cannot be relied upon as a comprehensive, systematic, and predictable legal foundation. The absence of specific regulations regulating *deepfakes* and AI as instruments of crime not only creates a legal vacuum, but also has implications for weak protection for victims, the difficulty of proving in court due to the absence of standard digital forensic standards, and the lack of technical capacity of law enforcement officials in identifying and processing AI-based evidence.[39] This situation reinforces the urgency of reformulating criminal law policies that are adaptive and responsive to the threat *of AI-based deepfakes*, which will be discussed in more depth in the next sub-chapter.

[37] DSAP Law Firm, "Artificial Intelligence and Criminal Accountability: Reconstruction of Legal Subjects and Criminal Mechanisms in the Paradigm of the National Criminal Code," January 29, 2026, https://dsaplawfirm.com/.
[38] N. Syam et al., "Reconstructing the Legal Accountability Paradigm for the Absence of Mens Rea in the Era of Artificial Intelligence," *DEDICATION: Journal of Social, Law, and Cultural Studies* (December 2025).
[39] Ahmad Sofian, "The Conception of Legal Subjects and Criminal Liability of Artificial Intelligence," 20.

2. Policy on the Formulation of Artificial Intelligence Accountability in the Perspective of Criminal Law

Based on the analysis of Indonesia's positive criminal law that has been described earlier, there is an undeniable conclusion: the vacuum of existing legal norms is not just a technical gap that can be closed by interpretation alone, but an urgent need for a systematic, comprehensive, and forward-looking reformulation of criminal law policy. Penal *policy formulation* is the process of determining new criminal acts and their criminal threats which aims to answer legal problems that have not been reached by existing norms.[40] In the context of *AI-based deepfakes*, the formulation of this policy should be based on three foundations at once: first, comparative lessons from jurisdictions that have been more advanced in regulating AI and *deepfakes*; second, the reconstruction of the concept of criminal accountability that is adaptive to the specificities of AI technology; and third, the formulation of new norms that explicitly and quantively span the entire spectrum of *deepfake* crimesin the context of Indonesian criminal law.[41]

A comparative study of *deepfake regulation* in various jurisdictions is a starting point that cannot be ignored in building an ideal policy formulation. The European Union, through *the Artificial Intelligence Act* (EU AI Act) which officially came into effect on 1 August 2024 (*Regulation* (EU) 2024/1689), has built the world's most comprehensive AI regulatory framework using a *risk-based approach*.[42] In the structure *of the EU AI Act*, *deepfake* content is categorized as *limited risk AI* regulated in Article 50 by requiring transparency and labeling. Article 50 paragraph (4) requires

[40] C.T. Noerman and A.L. Ibrahim, "Criminalization of Deepfakes in Indonesia as a Form of State Protection," *USM Law Review* Journal 7, no. 2 (2024): 603-621, https://doi.org/10.26623/julr.v7i2.8995.
[41] Andre Arya Pratama, Fikri Rosyad Fathurrahman, and Rani Lestari, "Criminal Liability Model for Deepfake Al Developers: European Union Inspiration for Indonesia's Legal Framework," *Ius Poenale* 6, no. 1 (2025): 67-76, https://doi.org/10.25041/ip.v6i1.4612.
[42] Regulation (EU) 2024/1689 (Artificial Intelligence Act), arts.

any party who uses an AI system to produce or manipulate images, audio, or videos that constitute a deepfake to reveal that the content has been artificially created or manipulated. This obligation applies regardless of the purpose of the content, whether commercial, entertainment or artistic, with limited exceptions for law enforcement purposes and works of art that are manifestly fictional.[43] Furthermore, through *the Draft Code of Practice on Transparency of AI-Generated Content* published in December 2025, the European Commission is operationalizing Article 50 with a multi-layered approach of a combination of *machine-readable marking*, prominent visual labels, and audio disclaimers tailored to the content format. Sanctions for violations can reach EUR 15 million or 3% of the company's global turnover.[44]

China offers a different but equally instructive regulatory model. Through the *Administrative Provisions on Deep Synthesis of Internet Information Services* (Deep Synthesis Regulation 2022) which came into effect on January 10, 2023, China is the first country in the world to enact comprehensive regulations that specifically target *deep synthesis* technology, a term used in Chinese regulations to refer to what in Indonesia is known as *deepfakes*.[45] This regulation requires *deep synthesis* service providers to: (1) conduct *real-name verification* of all service users; (2) provide clear labels on all content generated through deep synthesis technology; (3) build a content moderation system capable of proactively identifying and blocking harmful content; and (4) obtain explicit consent from the individual whose biometric data is used prior to processing.[46] From the comparison of these two regulatory models, the EU AI Act which is

[43] Regulation (EU) 2024/1689 (Artificial Intelligence Act), art.
[44] Jones Day Insights, "European Commission Publishes Draft Code of Practice on AI Labelling and Transparency," January 2026; Regulation (EU) 2024/1689, Art. 99(4).
[45] Library of Congress, "China: Provisions on Deep Synthesis Technology Enter into Effect," April 26, 2023, https://www.loc.gov/item/global-legal-monitor/2023-04-25/china-provisions-on-deep-synthesis-technology-enter-into-effect/.
[46] AI Regulations, "Provisions on the Administration of Deep Synthesis of Internet-based Information Services," January 6, 2026, https://www.regulations.ai/, art. 14.

oriented towards transparency and protection of human rights, and the Chinese regulation which is oriented towards national security and public order. Indonesia can learn a lesson that there are four essential elements that must be present in the formulation of an effective criminal law: clear normative definitions, labeling obligations, layered accountability, and proportionate sanctions.[47]

The intellectual foundation that must be built first before formulating new criminal norms is the reconstruction of the concept of criminal law subjects in the context of AI. The conventional criminal law doctrine is based on the paradigm that the subject of criminal law is a human being (*persona naturalis*) and a legal entity (*rechtspersoon*), as embraced by the New Criminal Code where it does not provide space for AI as an independent legal subject. AI lacks the awareness, free will, and moral capacity that are prerequisites for criminal liability in the Civil Law legal tradition.[48] For the current Indonesian legal context, the most realistic approach is an *expanded human-based accountability* model, which is to precisely identify human parties and corporations along the deepfake production and distribution chain as subjects who can be held criminally liable.[49]

The recommended multi-level liability *model* includes three complementary layers. **The first layer** is AI developer liability (*developer/producer liability*). Developers who design and market generative AI systems without adequate safeguards, without clear restrictions on use, without abuse detection systems, and without consent mechanisms from biometric data subjects—may be held criminally liable

[47] D.A.Y. Basah, A. Wijaya, and I. Januardy, "Criminalization of Digital Protocol Violations: A Criminal Law Review of the Spread of Deepfakes on Social Media," *Innovative: Journal of Social Science Research*, (2025).
[48] Ahmad Sofian, "Conception of Legal Subjects and Criminal Liability of Artificial Intelligence," 14-16.
[49] N. Cantika et al., "Criminal Liability for the Abuse of Artificial Intelligence (AI) in the Production of Hoax and Deepfake Content on Social Media," *Journal of School Leadership and Management* 10, no. 4 (December 2025): 2590-2599, https://doi.org/10.34125/jkps.v10i4.1435.

based on the principle of *strict liability*. In the *strict liability* paradigm, the element of error does not need to be proven separately if it is proven that the product developed does not meet proper safety standards (*product liability*). This principle is relevant to apply because AI developers are in the best position to assess and control the risks posed by the systems they create.[50] **The second layer** is platform operator liability. Digital platforms, both social media and AI-based applications, that actively provide, facilitate, or neglect to prevent the spread of harmful deepfake content may be subject to corporate criminal liability based on the doctrine of *vicarious liability*. This doctrine, which in Indonesian law is known as corporate liability or substitute liability, stipulates that corporations can be held criminally liable for criminal acts committed by individuals within the scope of their work and for the benefit of the corporation.[51] In the context of *deepfakes*, platforms that receive commercial benefits from *deepfake* AI services without building an effective moderation system can be seen as *principally* responsible for criminal acts committed through their platforms.[52] **The third layer** is *end-user liability*, which is individuals who actively and maliciously create and spread *deepfakes* with the intention of harming, defamatory, or deceptive. This layer is the most direct liability and uses the standard of conventional *dolus malus* as known in Indonesian criminal law.

Based on the comparative analysis and reconstruction of the concept of accountability above, this article formulates several new criminal law norms that are recommended to be included in the Artificial Intelligence Bill (AI Bill) or the next revision of the ITE Law. *First*, it is necessary to formulate

[50] K.A.R. Putri, H.D. Saputro, and A. Amanita, "Legal Accountability for the Use of Artificial Intelligence for Deepfakes According to the Personal Data Protection Law," *Rechtswetenschap: Journal of Law Students* (2025).

[51] Kukuh Dwi Kurniawan and Dwi Ratna Indri Hapsari, "Corporate Criminal Liability According to Vicarious Liability Theory," *Ius Quia Iustum* 29 Legal Journal, no. 2 (2022): 324-346, https://doi.org/10.20885/iustum.vol29.iss2.art5.

[52] Istiqomah, M.S.P. Dinanty, and S.R.A. Saputri, "The Legal Position of Deepfake Al as a Legal Subject and His Criminal Responsibility Based on a Dualistic Theory," *Deposition: Journal of Legal Science Publications* 3, no. 2 (2025): 59-74, https://doi.org/10.59581/deposisi.v3i2.5065.

a definition article that provides a clear and measurable normative definition of key terms such as "*deepfake*", "AI-based synthetic content", "generative AI system", "AI operator", and "biometric data". Without a clear definition, the entire criminal norm built on it would be dogmatically fragile and vulnerable to legal uncertainty.[53] *Second*, it is necessary to formulate *an article on the criminalization of the creation of dangerous deepfakes* whose elements cumulatively include: (a) using AI technology to produce audiovisual content; (b) who manipulates the identity, face or voice of another person; (c) without the lawful consent of the person concerned; and (d) with the intent to harm, defame, deceive, or harm the public interest. *Third*, it is necessary to formulate *an article on the criminalization of the spread of dangerous deepfakes* that expands the formulation of Article 27 of the ITE Law to explicitly include AI-based synthetic content, with the imposition of penalties if the content is disseminated through digital platforms with a wide reach.[54]

The fourth element of the formulation of the new norm is the *article on transparency and labeling obligations*. Referring to the EU AI Act Article 50 model and China's *Deep Synthesis* Regulation, any content produced using generative AI systems must be marked or labeled with clear and detectable labels, either visually labeling or machine-readable watermark). This obligation is imposed on AI system developers and platform operators, while violations against it are categorized as minor criminal offenses with the threat of significant administrative fines.[55] The fifth element is the *corporate/platform liability article* which expressly requires digital platforms to establish an active moderation system, provide a mechanism

[53] Andre Arya Pratama, Fikri Rosyad Fathurrahman, and Rani Lestari, "Criminal Liability Model for Deepfake Al Developers: European Union Inspiration for Indonesia's Legal Framework," 7.
[54] F.R.M. Wanggai, M.S. Hartono, and N.P.E. Parwati, "Normative Analysis of the Spread of Deepfakes as a Form of Cybercrime in Indonesia," *Assembly: Indonesian Law Journal* 3, no. 1 (February 2026): 122-130, https://doi.org/10.62383/majelis.v3i1.1509.
[55] S.N. Syahirah and B. Prasetyo, "A Juridical Review of the Use of Deepfake Technology for Pornography Through Artificial Intelligence (AI) in Indonesia," *Journal of Legal and Policy Innovation* 6, no. 1 (2025): 191-212.

for reporting harmful *deepfake* content to users, and carry out content removal within the stipulated time frame after receiving the notification. Failure to fulfill this obligation is a criminal act of *corporate negligence*.[56]

In addition to the basic norms above, a comprehensive formulation also requires *a deterrent article* that significantly increases the criminal threat when *deepfakes* are used for the purposes that have the most destructive impact, namely pornography and digital-based sexual violence (*KSBD*), election manipulation and the systematic spread of political disinformation; large-scale financial fraud, and threats to national security and destabilization of state institutions.[57] The threat of criminal aggravation must be at least double the basic threat, following the pattern of aggravation known in the ITE Law and the New Criminal Code.[58] Finally, all of these new norms must be placed within a framework of careful synchronization and harmonization with existing regulations. In the hierarchy of norms, the criminal provisions on deepfakes in the AI Law or the revision of the ITE Law must be treated as *lex specialis* that overrides the general articles in the New Criminal Code on forgery and insult (*lex specialis derogat legi generali*), as well as synergizing with the criminal sanctions of the PDP Law as the first layer of protection against biometric data violations that are a prerequisite for *deepfakes*.[59]

The ideal criminal law policy formulation to answer the threat of AI-based *deepfakes* is not just a matter of adding new articles in the law. It is a paradigmatic reconstruction project that demands a shift in Indonesia's criminal law perspective from a conventional paradigm centered on

[56] P.M. Banfatin, K.K. Medan, and D.F. Fallo, "Criminal Law Regulation in Indonesia on the Abuse of Artificial Intelligence Deepfake Technology in Committing Cybercrime," *Glorification of Justice* 2, no. 1 (2025): 60-73, https://doi.org/10.62383/pk.v2i1.402.

[57] Indah Sri Utari and Bagus Hendradi Kusuma, "Legal Interventions in Combating Gender-Based Violence: Empowering Communities through Legal Advocacy," *Lentera Masyarakat Hukum* 1, no. 4 (2024), https://doi.org/10.65815/wzd6fy42.

[58] SIP Law Firm, "Criminal Law Enforcement on Deepfake Content," August 11, 2025, https://share.google/MIjVwhmzV1eOnjd8a.

[59] M.A. Chairani, K. Yitawati, and A.P. Pradhana, "The Urgency of Legal Arrangements for the Abuse of Deepfake Applications," *Journal of Rechtens* 13, no. 1 (2024): 81-96, https://doi.org/10.56013/rechtens.v13i1.2668.

individual human actors to a paradigm responsive to an AI technology ecosystem that is multilayered, autonomous, and cross-border. The resulting regulation must be able to answer the fundamental question: who is responsible when a man-made system produces evil? The answer, as formulated, lies in a multi-layered accountability model that reaches developers, platforms, and users with *safeguards* in the form of transparency obligations, technical standards, and proportionate criminal sanctions. Only then can Indonesia's criminal law fulfill its most basic function, which is to provide legal certainty, justice for victims, and protection of the community from the destructive effects of artificial intelligence-based crimes.[60]

Conclusion

This research yielded two main conclusions. *First*, Indonesia's positive criminal laws, namely the ITE Law, the New Criminal Code, and the PDP Law, have not been able to adequately reach criminal liability for the creation and dissemination *of AI-based deepfake* videos. All three contain normative gaps (*lex lacuna*) that cannot be overcome through interpretation alone, no legal definition of *deepfakes*, no regulation targeting the entire production chain from developers to end users, and the application of *mens rea* principles is hampered by the autonomy of AI systems that work without traceable human will. *Second*, the formulation of an ideal criminal law policy must rest on three pillars: (1) a layered accountability model that reaches AI developers based on the principle of *strict liability*, platform operators based on the doctrine *of vicarious liability*, and end users based on *dolus malus*; (2) the formulation of new criminal norms that explicitly regulate the definition of *deepfakes*,

[60] M.A. Chairani, K. Yitawati, and A.P. Pradhana, "The Urgency of Legal Arrangements for the Abuse of Deepfake Applications," 93.

criminalization of creation and dissemination, labeling obligations, corporate liability, and burdening for the context of pornography, election manipulation, and national security threats; and (3) harmonization of new regulations as *lex specialis* that synergize with the PDP Law and the New Criminal Code as *lex generalis of* criminalization.

Based on this conclusion, this study recommends that the House of Representatives and the Government immediately prioritize the formation of the Artificial Intelligence Bill or include *deepfake* articles in the next revision of the ITE Law as a transitional step. On the institutional side, the Police, Prosecutor's Office, and the Supreme Court need to build adequate digital forensic capacity to handle AI-based evidence at trial, while digital platforms and AI developers are recommended to proactively implement synthetic content labeling and active moderation without waiting for formal regulatory obligations. Ultimately, *the threat of deepfakes* is a matter of information sovereignty and the protection of human dignity that requires the criminal law to be proactive in its presence. The momentum of the full implementation of the New Criminal Code in 2026 must be used as a starting point to build an adaptive and fair AI regulatory ecosystem for all citizens.

References

Ali Masyhar and Indah Sri Utari, "Policing and Human Rights: Analyzing Excessive Use of Force in Indonesian Law Enforcement," *Contemporary Issues on Indonesian Human Rights Law and Policy* 2, no. 2 (2025), https://doi.org/10.65815/6zp8et83.

Andre Arya Pratama, Fikri Rosyad Fathurrahman, and Rani Lestari, "Criminal Liability Model for Deepfake Al Developers: European Union Inspiration for Indonesia's Legal Framework," *Ius Poenale* 6, no. 1 (2025): 67-76, https://doi.org/10.25041/ip.v6i1.4612.

Ahmad Sofian, "The Conception of Legal Subjects and Criminal Responsibility of Artificial Intelligence," *Halu Oleo Law Review* 9, no. 1 (March 2025), https://doi.org/10.33561/holrev.v9i1.129.

AI Asia Pacific Institute, "Unmasking the Era of Misinformation: Navigating the Threat of Deepfakes," February 15, 2024, https://aiasiapacific.org/2024/02/15/unmasking-the-era-of-misinformation-navigating-the-threat-of-deepfakes/.

Arash Heidari et al., "Deepfake detection using deep learning methods: A systematic and comprehensive review," in *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 14, no. 2, preprint, John Wiley and Sons Inc, March 1, 2024, https://doi.org/10.1002/widm.1520.

Directed by Amanda Uly Sijabat and Diana Lukitasari, "Deepfake Pornographic Image and Video Content as a Form of Defamation Crime," *Recidive: Journal of Criminal Law and Crime Prevention* 13, no. 2 (July 2024): 179-194, https://doi.org/10.20961/recidive.v13i2.86771.

C.T. Noerman and A.L. Ibrahim, "Criminalization of Deepfakes in Indonesia as a Form of State Protection," *USM Law Review* 7 Journal, no. 2 (2024): 603-621, https://doi.org/10.26623/julr.v7i2.8995.

Cyberspace Administration of China (CAC), Ministry of Industry and Information Technology (MIT), and Ministry of Public Security (MPS), Provisions on the Administration of Deep Synthesis of Internet Information Services（深度合成互联网信息服务管理规定）, November 25, 2022, effective January 10, 2023.

D.A.Y. Basah, A. Wijaya, and I. Januardy, "Criminalization of Digital Protocol Violations: A Criminal Law Review of the Spread of Deepfakes on Social Media," *Innovative: Journal of Social Science Research*, (2025).

Dara Sawitri, "Artificial Intelligence for a Digital Technology Smart Society in the Era of Society 5.0," *Journal of Artificial Intelligence and*

Software Engineering (J-AISE) 5, no. 1 (March 2025): 135, https://doi.org/10.30811/jaise.v5i1.6441.

Deva Wayan Zenitia, "Legal Implications for the Misuse of Deepfake Technology for Extortion in the Legal Perspective of Information Technology in Indonesia," *Assembly: Indonesian Law* Journal 3, no. 1(2026): 102-114, https://doi.org/10.62383/majelis.v3i1.1504.

DSAP Law Firm, "Artificial Intelligence and Criminal Responsibility: Reconstruction of Legal Subjects and Criminal Mechanisms in the National Criminal Code Paradigm," January 29, 2026, https://dsaplawfirm.com/.

European Parliament and Council, Regulation (EU) 2024/1689 of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), Official Journal of the European Union L 2024/1689, July 12, 2024, art. 50.

Faathurrahman and Priowirjanto, "Accountability Arrangements for Perpetrators of Deepfake Abuse," 1163.

F.R.M. Wanggai, M.S. Hartono, and N.P.E. Parwati, "Normative Analysis of the Spread of Deepfakes as a Form of Cybercrime in Indonesia," *Assembly: Indonesian Law Journal* 3, no. 1 (February 2026): 122-130, https://doi.org/10.62383/majelis.v3i1.1509.

Hartono, "Normative Analysis of the Abuse of Deepfake Technology in Digital Political Campaigns as a Cyber Criminal Act based on Article 28 paragraph (2) of the ITE Law," *Muqoddimah Journal: Journal of Social, Political, and Humanities Sciences* 10, no. 1 (2026): 591-601, https://doi.org/10.31604/jim.v10i1.2026.591-601.

Hukumonline, "What is Deepfake Porn and Criminal Snares for the Perpetrators," January 19, 2024, https://share.google/ptiF4ekrPt4VlYLM9.

Indah Rohmawati, Amir Junaidi, and Ariy Khaerudin, "The Urgency of Deeptake Abuse Regulation as Online-Based Sexual Violence," *Innovative: Journal of Social Science Research* 4, no. 6 (2024): 1779-1794, https://doi.org/10.31004/innovative.v4i6.16559.

Indah Sri Utari and Bagus Hendradi Kusuma, "Legal Interventions in Combating Gender-Based Violence: Empowering Communities through Legal Advocacy," *Lentera Masyarakat Hukum* 1, no. 4 (2024), https://doi.org/10.65815/wzd6fy42.

Istiqomah, M.S.P. Dinanty, and S.R.A. Saputri, "The Legal Position of Deepfake Al as a Legal Subject and His Criminal Liability Based on a Dualistic Theory," *Deposition: Journal of Legal Science* Publications 3, no. 2 (2025): 59-74, https://doi.org/10.59581/deposisi.v3i2.5065.

Itok Kurniawan, "Analysis of Artificial Intelligence as a Subject of Criminal Law," *Mutiara: Indonesian Multidisciplinary Scientific Journal* 1, no. 1 (July 2023): 35-44, https://doi.org/10.61404/jimi.vli1.4.

Jones Day Insights, "European Commission Publishes Draft Code of Practice on Al Labelling and Transparency," January 2026; Regulation (EU) 2024/1689, Art. 99(4).

K.A.R. Putri, H.D. Saputro, and A. Amanita, "Legal Accountability for the Use of Artificial Intelligence for Deepfakes According to the Personal Data Protection Law," *Rechtswetenschap: Journal of Law Students* (2025).

Kukuh Dwi Kurniawan and Dwi Ratna Indri Hapsari, "Corporate Criminal Liability According to Vicarious Liability Theory," *Ius Quia Iustum 29 Legal Journal* , no. 2 (2022): 324-346, https://doi.org/10.20885/iustum.vol29.iss2.art5.

Laili Rahmawati, "Legal Policy in the Regulation of Artificial Intelligence in Indonesia," *Journal of Law and Development* 54, no. 1 (2024).

Library of Congress, "China: Provisions on Deep Synthesis Technology Enter into Effect," April 26, 2023,

https://www.loc.gov/item/global-legal-monitor/2023-04-25/china-provisions-on-deep-synthesis-technology-enter-into-effect/.

M.A. Chairani, K. Yitawati, and A.P. Pradhana, "The Urgency of Legal Arrangements for the Abuse of Deepfake Applications," *Journal of Rechtens* 13, no. 1 (2024): 81-96, https://doi.org/10.56013/rechtens.v13i1.2668.

M.A. Chairani, K. Yitawati, and A.P. Pradhana, "The Urgency of Legal Arrangements for the Abuse of Deepfake Applications," 93.

Muhaimin, Legal Research Methods (Mataram: Mataram University Press, 2020), 59-60.

Muhammad Fagih Faathurrahman and Enni Soerjati Priowirjanto, "Accountability Arrangements for Perpetrators of Deepfakes Abuse in Artificial Intelligence Technology on Pornographic Content Based on Indonesian Positive Law," *Indonesian Journal of Social Technology* 3, no. 11 (November 2022): 1157-1158.

N. Cantika et al., "Criminal Liability for the Misuse of Artificial Intelligence (AI) in the Production of Hoax and Deepfake Content on Social Media," *Journal of School Leadership and Management* 10, no. 4 (December 2025): 2590-2599, https://doi.org/10.34125/jkps.v10i4.1435.

N. Syam et al., "Reconstructing the Legal Accountability Paradigm for the Absence of Mens Rea in the Era of Artificial Intelligence," *DEDICATION: Journal of Social, Law, and Cultural Studies* (December 2025).

N.P.M. Putri, M.S. Hartono, and I.D.G.H. Yudiawan, "Analysis of Reformulation of Criminal Liability of Deepfake Technology Users in Artificial Intelligence-Based Defamation Crimes," *Pacta Sunt Servanda* Journal 5, no. 2 (2024), https://doi.org/10.23887/jpss.v512.5807.

Nur Solikin, Introduction to Legal Research Methodology (Pasuruan: CV. Qiara Media Publisher, 2021), 39.

Article 27 paragraph (1) jo. Article 45 paragraph (1) of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions.

Article 35 jo. Article 51 paragraph (1) of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions.

Article 407 of Law Number 1 of 2023 concerning the Criminal Code.

Article 65 paragraph (1) and Article 67 paragraph (1) of Law Number 27 of 2022 concerning Personal Data Protection.

Article 68 of Law Number 27 of 2022 concerning Personal Data Protection.

P.M. Banfatin, K.K. Medan, and D.F. Fallo, "Criminal Law Regulation in Indonesia on the Abuse of Artificial Intelligence Deepfake Technology in Committing Cybercrime," *Pejuraan Keadilan* 2, no. 1 (2025): 60-73, https://doi.org/10.62383/pk.v2i1.402.

R.S. Arvitto, "Legal Implications of Deepfakes: A Study of the ITE Law and the PDP Law," *Scientific Journal of Law and Human Rights* 4, no. 2 (2025): 77, https://doi.org/10.35912/jihham.v4i2.3937.

Regulation (EU) 2024/1689 (Artificial Intelligence Act), arts.

AI Regulations, "Provisions on the Administration of Deep Synthesis of Internet-based Information Services," January 6, 2026, https://www.regulations.ai/, art. 14.

Sensity AI, State of Deepfakes 2024 (annual report).

SIP Law Firm, "Criminal Law Enforcement on Deepfake Content," August 11, 2025, https://share.google/MIjVwhmzV1eOnjd8a.

S.N. Syahirah and B. Prasetyo, "A Juridical Review of the Use of Deepfake Technology for Pornography Through Artificial Intelligence (AI) in Indonesia," *Journal of Legal and Policy Innovation* 6, no. 1 (2025): 191-212.

S.W. Nurdin and I.F. Nugraha, "Deepfake Threats and Al-Based Disinformation: Implications for Cybersecurity and Indonesian National Stability," *JIMR: Journal of International Multidisciplinary Research* 4, no. 1 (June 2025): 73-92, https://doi.org/10.62668/jimr.v4i01.1551.

Law Number 11 of 2008 concerning Information and Electronic Transactions as last amended by Law Number 1 of 2024, Statute Book of the Republic of Indonesia of 2024.

Law Number 27 of 2022 concerning Personal Data Protection, Statute Book of the Republic of Indonesia of 2022.