AI Image Generation as a New Form of Crime from the Perspective of Indonesian Criminal Law

Nugraha Ardi Setiawan[1], Inka Dwi Lestari[2], Balqis Niswatul Hanifah[3], and Naisya Ameli Sahara[4]

[1,2,3,4] Faculty of Social Sciences, State University of Malang, Jl. Semarang No. 5, Sumbersari, Lowokwaru, Malang, East Java 65145, Indonesia
Corresponding author:
nugrahaardi.fis@um.ac.id

Abstract. The rapid diffusion of generative artificial intelligence has enabled AI image generation tools to produce photorealistic synthetic images with minimal technical skill, giving rise to new patterns of misuse such as non-consensual sexualized imagery, visual disinformation, and identity-based fraud. This article examines AI image generation as an emerging form of crime within the framework of Indonesian criminal law. Using normative legal research with statutory, conceptual, and comparative approaches, this study analyzes secondary legal materials, including the Criminal Code, the amended Electronic Information and Transaction Law (Law No. 1 of 2024), and comparative regulatory frameworks from South Korea and the People's Republic of China. The findings indicate that Indonesia's existing criminal law framework, built on the assumption of a single, directly acting human perpetrator, is structurally inadequate to address the layered production chain of AI-generated content involving developers, platform providers, and end users. This mismatch produces a functional legal vacuum concerning attribution of criminal liability and digital forensic evidentiary standards. The study concludes that a sui generis regulatory approach combining explicit criminalization of AI-generated non-consensual imagery, tiered liability across the production chain, and strengthened digital forensic evidentiary mechanisms is necessary. These findings carry implications for future revision of Indonesia's electronic information legislation and for the development of AI-specific criminal liability doctrine.

Keywords: *AI image generation, deepfake, criminal liability, Indonesian criminal law, digital forensic evidence.*

1 Introduction

The development of generative artificial intelligence in recent years has fundamentally changed the way humans produce visual content. The emergence of AI image generation models such as Midjourney, DALL·E, and *Stable Diffusion*, along with various derivative applications that are now freely and affordably available, allows anyone to generate photorealistic images simply by entering a text description (prompt), without requiring expertise in photography or graphic design. Technically, the generated images do not originate from a single edited photograph but are synthesized

© The Author(s) 2026
S. Untari et al. (eds.), *Proceedings of the 3rd International Conference on Citizenship Education and Democratic Issues (ICCEDI 2026)*, Advances in Social Science, Education and Humanities Research 1039,
https://doi.org/10.2991/978-2-38476-626-0_16

by artificial neural networks based on statistical patterns derived from billions of visual data points used to train the models. [1] It is this characteristic that fundamentally distinguishes AI image generation from conventional image manipulation: the origin of the results is difficult to trace, they are hard to distinguish from reality even by forensic systems that are not yet state-of-the-art, and they can be produced on a massive scale at a cost approaching zero.

The issue becomes serious when this technical capability is misused. Studies widely cited in the literature show that the majority of synthetic facial content circulating on the internet takes the form of non-consensual pornography targeting women, [2] while other patterns of misuse include visual disinformation in political contexts and the fabrication of evidence for fraud or extortion. In Indonesia, this phenomenon has become increasingly evident through the circulation of deepfake images of public figures and ordinary citizens in degrading contexts whether sexual, political, or defamatory. A recent normative study on the Indonesian context even notes that the absence of an explicit legal definition of "deepfakes" casts doubt on the effectiveness of the state's protection for victims. [3]

Theoretically, the conventional criminal law framework including both the Criminal Code and the Law on Information and Electronic Transactions is built on the classical assumption that the perpetrator of a criminal act is a single human individual who directly creates, alters, or disseminates content. The principle of legality, which requires clear and specific definitions of criminal offenses *lex certa*, becomes problematic when confronted with the multi-layered production chain of AI image generation: model developers who train the system with massive-scale visual data, platform providers who operate the service commercially, and end users who write prompts and distribute the results. The lack of clarity regarding which party can be held criminally liable within this chain creates a functional legal vacuum. [4]

The amendment to the Electronic Information and Transactions Law through Law No. 1 of 2024 has strengthened a number of provisions, including those regarding defamation under Article 27A, [5] but has not yet explicitly classified deepfakes or AI-generated images as separate categories of offenses. In practice, law enforcement still relies on general public decency provisions and the provisions of the Pornography Law, which were actually designed for manually manipulated content, not content that is entirely algorithmically synthesized. [6] This regulatory gap contrasts with several other jurisdictions that have responded to similar phenomena. South Korea, for example, has expanded the scope of its Special Act on Sexual Crimes since the 2020 amendment to include manipulated sexual material, and substantially strengthened it in 2024 by also criminalizing the acts of *viewing* and *possession*, following a deepfake scandal targeting female students at various schools. China, through the Provisions on the Administration of Deep Synthesis of Internet-based Information Services effective since January 2023 requires the labeling of synthetic content as well as identity verification of service providers. The European Union, through Article 50 of the AI Act, mandates transparency and labeling for AI-generated content, including deepfakes, although its approach is administrative in nature rather than purely criminal law.

Technical literature in the field of digital forensic detection indicates that the challenge of proof is not merely a regulatory issue but also stems from the limitations of detection capabilities themselves. A systematic review of hundreds of deepfake detection studies confirms that deep learning-based methods are indeed superior to

other approaches but remain vulnerable to new-generation content creation techniques that evolve faster than detection capabilities can keep up with. [7] This situation reinforces the argument that the weaknesses in Indonesia's criminal law stem not only from criminal definitions that do not yet cover AI-generated images but also from digital forensic evidentiary standards that are not yet prepared to address the unique characteristics of synthetic content.

A synthesis of various previous studies reveals a consistent pattern. Domestic normative research tends to stop at identifying legal gaps without formulating a multi-layered model of criminal liability that covers all actors in the production chain (developer-platform-user), while international technical literature focuses on detection aspects without addressing the dimension of criminal policy. This is *the research gap* that this article aims to fill: there is currently no Indonesian criminal law study that specifically maps AI image generation as a distinct category of crime, while simultaneously linking the analysis of criminal elements to the limitations of digital forensics and current comparative regulatory practices. The novelty of this article lies in the formulation of a criminal law policy model that explicitly distinguishes the levels of liability among technology actors, rather than treating the entire production chain as a single legal entity.

The urgency of this study is all the more evident given that the pace of generative technology adoption far outstrips the pace of regulatory updates, while the social impacts of its misuse ranging from reputational damage and gender-based victimization to the distortion of the public information sphere are rapid and difficult to reverse. Based on the above discussion, this article aims to: (1) analyze forms of misuse of AI image generation as criminal offenses (2) examine the extent to which Indonesia's current criminal law framework is capable of addressing this phenomenon and (3) formulate an ideal direction for criminal law policy to address AI image generation-based crimes in the future.

2 Research Method

The statutory approach was used to examine relevant provisions in the Criminal Code (KUHP), the Information and Electronic Transactions Law (ITE Law), the Pornography Law, the Personal Data Protection Law, and the Copyright Law. Furthermore, the conceptual approach is used to develop a framework for understanding legal concepts that do not yet have clear definitions in legislation, such as the concepts of AI-generated images and deepfakes, by drawing on legal principles and doctrines developed in the literature. [8, p. 133] The comparative approach was used to examine similar regulations in South Korea, China, and the European Union, in order to enrich the reference materials for policy formulation.

The legal materials used consist of primary sources in the form of legislation, secondary sources in the form of academic journals, previous research findings, and policy documents, as well as tertiary sources in the form of legal dictionaries and encyclopedias. [9, pp. 13–14] The analysis was conducted qualitatively using descriptive-analytical techniques, beginning with an examination of the relevant elements of the offense, followed by a comparison with the characteristics of AI-generated images to determine the extent to which existing regulations can address this

phenomenon. The results of this comparison serve as the basis for drawing conclusions regarding the adequacy and weaknesses of current regulations, as well as the foundation for formulating policy recommendations.

3 Results and Discussion

3.1 Forms of Misuse of AI Image Generation as a Criminal Offense

AI image generation enables anyone to produce new, lifelike images using only a brief description a capability driven by technologies such as generative adversarial networks (GANs) and diffusion models. [10] The term “deepfake” itself is more specific it refers to content that superimposes a person's face or voice onto a different scenario, also known as a “face swap.” Slightly different, a synthetic image is an image that is entirely “invented” by an algorithm, without being based on any original photo. Behind the scenes, the process involves a sort of competition between two systems: a generator that attempts to create fake images, and a discriminator that tries to detect the falsity of the images until the final result is nearly indistinguishable from a real photo. [11]

One of the most harmful forms of misuse is deepfake pornography, in which a person's face is superimposed onto sexual content without their consent. In 2025, a student at Udayana University experienced this firsthand. Her face was manipulated by AI, superimposed onto another person's body, and then disseminated via a Telegram bot without her knowledge. [12] This case is difficult to address not only because of the challenges of proving guilt but also because automated bots make it nearly impossible to track the perpetrator's identity, while similar content can be reproduced in a matter of minutes.

Another form is political hoaxes or visual disinformation that depicts events that never actually occurred. Ahead of the 2024 presidential election, for example, a video circulated showing President Joko Widodo speaking fluent Mandarin, even though the original video was in English and recorded in 2015 it was later manipulated using deepfake technology so that his lip movements and voice were adjusted to make it appear as if he were speaking Mandarin. [13] The Ministry of Communication and Information Technology confirmed that the video was the result of AI manipulation. A similar pattern recurred when a video of the late President Soeharto circulated, in which he appeared to be urging the public to vote for a specific political party ahead of the 2024 general election. [14]

Another equally alarming form of fraud involves using the faces of public figures to persuade victims to transfer money. In January 2025, the Cybercrime Directorate of the Indonesian National Police's Criminal Investigation Agency arrested a suspect identified by the initials AMA in Central Lampung, who created deepfake videos featuring the faces and voices of President Prabowo Subianto, Vice President Gibran Rakabuming Raka, and Finance Minister Sri Mulyani, making it appear as though they were offering government social assistance. Victims were asked to transfer between Rp250,000 and Rp1,000,000 under the pretext of administrative fees, with at least 11 victims reported from various regions. An analysis of this case found that this type of scheme thrives precisely because it exploits the public's trust in influential figures whose faces are forged, rather than solely due to the victims' negligence. [15]

These characteristics distinguish AI image generation from conventional image manipulation such as Photoshop. In traditional image manipulation, the altered object still originates from an original photo, so forensic traces such as metadata remain easy to trace. AI-generated images are different they are synthesized from massive statistical and periodic patterns, not from a single specific photo source, making their origin harder to trace. Nevertheless, recent forensic research has found that AI images still leave their own distinct traces, such as the absence of EXIF data and noise patterns that are smoother and more structured than those in original photos. [16]

Detecting such traces, however, is no simple matter. In Indonesia, a number of researchers have attempted to build detection systems based on Convolutional Neural Networks (CNNs) combined with watermarking [17] however, a systematic review of other deep learning studies shows that the quality of deepfakes continues to improve faster than the systems' ability to recognize them. [18] In other words, detection capabilities consistently lag behind advancements in generative technology. Coupled with near-zero production costs and the anonymity of perpetrators, AI image generation has become a criminal tool that is far faster, more widespread, and harder to detect than previous image manipulation technologies. It is this gap between the pace of generative technology's development and the ability to detect it that makes legal regulation crucial. As long as technical detection systems cannot keep up, the only remaining defense to prevent and address its misuse is a robust and responsive criminal law framework. [19]

3.2 **Indonesian Criminal Law Regulations on AI-Generated Images**

One form of misuse of AI image generation is *non-consensual AI-generated sexual content*. This involves the creation of sexually suggestive images or videos using a person's likeness without their consent. Such acts not only violate the victim's privacy but can also be classified as *digital voyeurism*, which is linked to indecency, misuse of personal data, and electronic sexual violence. [20] From the perspective of Indonesian criminal law, the rise of “AI-Generated Images” indicates that the nature of crime has evolved faster than existing regulations. Although certain provisions in the Criminal Code (KUHP), the Law on Information and Electronic Transactions (ITE Law), the Pornography Law, and the Personal Data Protection Law (PDP Law) can still be used to prosecute perpetrators, to date there are no specific regulations classifying the misuse of AI or *deepfakes* as a distinct criminal offense. This situation means that law enforcement still relies on the interpretation of existing regulations, which creates various challenges, particularly regarding the burden of proof and the determination of criminal liability.

To date, Indonesia has not yet enacted regulations specifically addressing the misuse of *Artificial Intelligence* (AI), particularly *AI-generated images* or *deepfakes*. However, this does not mean that perpetrators cannot be held criminally liable. Law enforcement can still be carried out through several existing laws and regulations, such as the Criminal Code (KUHP), the Information and Electronic Transactions Law (ITE Law), the Pornography Law, and the Personal Data Protection Law (PDP Law). However, the application of these provisions remains limited because they address only the consequences of AI misuse, not the AI technology itself. The misuse of AI image generation to produce defamatory or libelous content can be prosecuted under Articles 433, 434, and 435 of the National Criminal Code regarding criminal offenses against

honor or dignity. If AI-generated images are used to produce pornographic images or videos without the victim's consent, Law No. 44 of 2008 on Pornography may also be applied. In this case, it is not the AI technology itself that is criminalized, but rather the acts of creating, producing, or disseminating pornographic content. Article 65 of Law No. 27 of 2022 on Personal Data Protection may also be applied in cases of misuse, as it provides a strong legal basis establishing that facial features, biometric data, voice, and other characteristics constitute personal data protected by law. Furthermore, Law No. 1 of 2024 on the Second Amendment to the ITE Law serves as the most robust instrument for addressing the unlawful use of AI in the digital space. Specifically, under Article 27A, any person who intentionally attacks the honor or reputation of another person through an electronic system is subject to criminal penalties. In the context of AI-generated images, this element is satisfied if an AI-generated image is uploaded or disseminated via electronic media, thereby damaging the victim's reputation. However, although the provisions of the ITE Law can be applied to *deepfake* cases, the regulations remain general in nature because deepfakes have not yet been classified as a distinct criminal offense. [20]

The misuse of *AI-generated images* involves several actors: *developers*, platform providers, and *users*. However, based on evolving concepts of criminal liability, users are the parties most easily held accountable because they directly use, generate, and disseminate AI-based content that meets the elements of a criminal offense. Conversely, liability for *developers* and platform providers remains a subject of debate because there are no regulations that explicitly define the limits of their liability for the misuse of AI technology. This is especially true when AI misuse occurs via bots, where it is extremely difficult to trace the creator, making it necessary to investigate *the developers* and platform providers instead. These developments highlight the need to reformulate the concept of criminal liability to accommodate the characteristics of crimes involving *deepfakes* and artificial intelligence. [21]

Although the misuse of *AI-generated images* can be prosecuted under the Criminal Code (KUHP), the Information and Electronic Transactions Law (ITE Law), the Pornography Law, and the Personal Data Protection Law, these regulations do not yet specifically classify *deepfakes* or the misuse of AI technology as distinct criminal offenses. As a result, law enforcement still relies on the interpretation of existing provisions, which has the potential to create legal uncertainty, particularly in determining the elements of the offense and the liability of the parties involved. [22] Proving cases of AI misuse also poses significant challenges because law enforcement officials must demonstrate that the circulating content is the result of AI manipulation and identify the perpetrators who created and disseminated it. In the author's view, these conditions highlight the need for specific regulations on AI that not only criminalize the misuse *of deepfakes* but also clarify the responsibilities of *developers*, platform providers, and users, accompanied by the strengthening of digital forensic capabilities to support effective law enforcement.

3.3 Formulation of Criminal Law Policies Against Crimes Involving AI-Generated Images

Regulatory developments in various countries indicate that legal policies regarding the misuse *of AI-generated images* are beginning to shift from a purely repressive approach

to one that is also preventive in nature. The European Union, through the EU AI Act, emphasizes transparency requirements for synthetic content so that the public can distinguish between authentic content and AI-generated content. Meanwhile, China requires *deep synthesis* service providers to label AI-generated content and verify user identities. South Korea has even taken a more progressive step by expanding the criminalization of sexually explicit *deepfakes* as a form of protection for victims. These developments indicate that modern regulations do not only focus on punishing perpetrators but also position technology providers as part of the system for preventing the misuse of AI.

Unlike those countries, Indonesia's positive law still relies on general provisions in the Criminal Code, the ITE Law, the Pornography Law, and the Personal Data Protection Law. Although these regulations can still be used to prosecute perpetrators, there are no specific provisions that classify the misuse *of AI-generated images* or *deepfakes* as separate criminal offenses. As a result, law enforcement still depends on the interpretation of existing norms, which often leads to legal uncertainty particularly in determining the elements of a crime and the parties who should be held criminally liable. [23] This situation highlights the need for an update to criminal law policy that is more adaptive to developments in digital technology.

The formulation of criminal law policy in Indonesia needs to focus on three main aspects. First, the establishment of specific provisions regarding the misuse *of AI-generated images* that include definitions, scope, and forms of prohibited acts, such as the creation or dissemination *of deepfakes* that harm a person's dignity, privacy, or right to personal data. Such regulations will provide legal certainty while fulfilling the principle of *lex certa*, so that law enforcement officials no longer have to rely on interpretations of general provisions. [24]

Second, a system of "*layered criminal* liability" is needed to distinguish the responsibilities of *developers*, platform providers, and users. Users remain the primary parties responsible if they intentionally use AI to commit criminal acts. However, platform providers and *developers* must also be subject to specific legal obligations, such as providing *reporting* mechanisms, implementing "*notice and takedown*" procedures for infringing content, and applying *watermarks* or other identifiers to synthetic content. In this way, the legal system not only punishes the direct perpetrators but also encourages technology providers to implement preventive measures from the outset.

Third, updates to criminal law must be accompanied by the strengthening of the digital evidence system. Given that *AI-generated images* are difficult to distinguish from authentic content, there is a need to expand the use of electronic evidence, such as *metadata*, *prompts*, activity *logs*, and the results of digital forensic examinations. [25] In addition to regulatory updates, enhancing the capacity of law enforcement officials in the field of digital forensics is also an urgent necessity so that the evidentiary process can keep pace with the increasingly complex developments in AI technology.

Thus, formulating criminal law policies regarding crimes based on *AI-generated images* requires more than simply expanding criminalization it must also establish a comprehensive regulatory framework by defining the responsibilities of all actors within the AI ecosystem, strengthening digital evidence mechanisms, and implementing preventive measures. This approach is expected to provide legal certainty

while enhancing the effectiveness of protecting the public from the misuse of artificial intelligence technology.

4 Conclusions and Suggestions

The misuse *of AI-generated images* has evolved into a new form of cybercrime that has the potential to violate the rights to dignity, privacy, decency, and personal data protection. This phenomenon demonstrates that although Indonesia's positive law through the Criminal Code (KUHP), Law No. 1 of 2024 on the Second Amendment to the Law on Information and Electronic Transactions, Law No. 44 of 2008 on Pornography, and Law No. 27 of 2022 on Personal Data Protection can still be used to prosecute perpetrators, these regulations do not explicitly classify *AI-generated images* or *deepfakes* as distinct criminal offenses. As a result, the application of the law still depends on the interpretation of existing provisions, while criminal liability is more easily attributed to users than to *developers* or platform providers who play a role in the AI technology ecosystem.

Drawing on regulatory developments in various countries, such as the European Union, China, and South Korea, Indonesia needs to update its criminal law policies to better adapt to advancements in artificial intelligence technology. These updates should not only involve the establishment of specific regulations regarding the misuse of *AI-generated images* but also the implementation of a "*layered criminal* liability" framework that proportionally assigns responsibility to *developers*, platform providers, and users. Furthermore, strengthening the evidentiary system through the use of digital evidence and enhancing digital forensic capabilities are crucial steps to support the effective enforcement of laws against AI-based crimes.

The government and lawmakers need to immediately formulate regulations that specifically address the misuse of *AI-generated images* as a new form of cybercrime, while maintaining a balance between the protection of public rights, legal certainty, and technological innovation. Furthermore, enhancing the capacity of law enforcement officials in the field of digital forensics and strengthening cooperation with digital platform providers are strategic steps to ensure that law enforcement can keep pace with the increasingly complex developments in artificial intelligence technology.

References

1. Nguyen, T.T., Nguyen, Q.V.H., Nguyen, D.T., Nguyen, D.T., Huynh-The, T., Nahavandi, S., Nguyen, T.T., Pham, Q.-V., Nguyen, C.M.: Deep learning for deepfakes creation and detection: a survey. Computer Vision and Image Understanding **223**, 103525 (2022)
2. Bohacek, M., Farid, H.: Protecting world leaders against deep fakes using facial, gestural, and vocal mannerisms. Proceedings of the National Academy of Sciences **119**(48), e2216035119 (2022)
3. Noerman, C.T., Ibrahim, A.L.: Kriminalisasi Deepfake di Indonesia sebagai Bentuk Pelindungan Negara. Jurnal USM Law Review **7**(2), 603–621 (2024)
4. Satrul, H.S., Hasanah, N.H.: Reconstruction of criminal liability for deepfake misuse in defamatory defenses in Indonesia. **4**(1), 353–358 (2026)

5. Purwono, A., Zamroni, M.Z., Santoso, H.A., Miarsa, F.R.D.: Implications and considerations of the new Electronic Information and Transaction Law. ANAYASA: Journal of Legal Studies **1**(2), 178–195 (2024)
6. Octarina, N.F., Hasan, M.: The urgency of regulating access to pornography content in Law No. 44 of 2008 concerning Pornography. International Journal of Science and Society **5**(1), 141–153 (2023)
7. Rana, M.S., Nobi, M.N., Murali, B., Sung, A.H.: Deepfake detection: a systematic literature review. IEEE Access **10**, 25494–25513 (2022)
8. Marzuki, P.M.: Penelitian Hukum. Kencana (2025)
9. Soekanto, S., Mamudji, S.: Penelitian Hukum Normatif: Suatu Tinjauan Singkat, 11th edn. Rajawali Pers (2009)
10. Syaifudin, S.: Generative Adversarial Networks (GAN) dalam Fotografi: Menciptakan Imaji dari Nol. Specta **8**(2), 169–180 (2024)
11. Mu, J., Adrezo, M., Haikal, A.N.: Identifikasi Wajah Asli dan Buatan Deepfake Menggunakan Metode Convolutional Neural Network. Teknika **13**(1), 45–50 (2024)
12. detikNews: Unud Buka Suara soal Mahasiswa Diduga Edit Foto Mahasiswi Jadi Tak Senonoh, https://news.detik.com/berita/d-7885705/unud-buka-suara-soal-mahasiswa-diduga-edit-foto-mahasiswi-jadi-tak-senonoh, last accessed 2025/04/25
13. detikNews: Beredar Video Jokowi Fasih Mandarin, Kominfo: Editan AI Menyesatkan!, https://news.detik.com/berita/d-7003320/beredar-video-jokowi-fasih-mandarin-kominfo-editan-ai-menyesatkan (2023)
14. Kompas.com: Video AI Soeharto Kampanye untuk Golkar, https://www.kompas.com/cekfakta/read/2024/01/18/164800982/-klarifikasi-video-ai-soeharto-kampanye-untuk-golkar- (2024)
15. Kristiyenda, Y.S., Faradila, J., Basanova, C.: Pencegahan Kejahatan Deepfake: Studi Kasus terhadap Modus Penipuan Deepfake Prabowo Subianto dalam Tawaran Bantuan Uang. Aladalah: Jurnal Politik, Sosial, Hukum dan Humaniora **3**(2), 149–164 (2025)
16. Ferdiansyah, F., Deazwara, M.R.A., Billanivo, R.R., Ardiansyah, M., Ilham, I.: Forensic analysis of AI-generated image alterations using metadata evaluation, ELA, and noise pattern analysis. Journal of Information Systems and Informatics **7**(4), 4014–4035 (2025)
17. Jiwani, F.A., Poetro, B.S.W.: Sistem Deteksi Gambar Deepfake Menggunakan CNN DenseNet-121 dengan Watermarking Least Significant Bit (LSB). Jurnal Rekayasa Sistem Informasi dan Teknologi **2**(3), 1157–1170 (2025)
18. Arif Fernandes, Y., Fatma, Y.: Metode Deep Learning dalam Teknologi Deepfake: Systematic Literature Review. JATI (Jurnal Mahasiswa Teknik Informatika) **9**(2), 3403–3410 (2025)
19. BR, W.: Tantangan Penegakan Hukum terhadap Kejahatan Berbasis Teknologi AI. **5**(1), 3436–3450 (2025)
20. Devy Fitri Syahrani, Primananda, M.A., Paramesti, N.Z., Zalifah, Y.K., Nugroho, A.A.: Analisis Yuridis Terhadap Non-Consensual AI-Generated Sexual Content Sebagai Digital Voyeurism dalam Hukum Pidana Indonesia. **4**(1) (2025)
21. Wafi, M.S., Wisnubroto, A., Prayudi, Y.: Artificial intelligence-based deepfake crimes: a conception of culpability principle as a criminal liability reform. Reformasi Hukum **29**(2), 168–183 (2025)
22. Nurul Aulia Fitriani, Endik Wahyudi: 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), 157–169 (2026)
23. Putri, N.P.M., Hartono, M.S., Yudiawan, I.D.G.H.: Analisis Reformulasi Pertanggungjawaban Pidana Pengguna Teknologi Deepfake dalam Tindak Pidana

Pencemaran Nama Baik Berbasis Artificial Intelligence. Jurnal Pacta Sunt Servanda **5**(2), 120–129 (2024)
24. Novrianto, M.: Kebijakan Hukum Pidana terhadap Cyber Crime Berbasis Artificial Intelligence di Indonesia. Jurnal Kepastian Hukum & Keadilan **7**(2) (2025)
25. Kwangtama Tekayadi, S., Efendi, S., Rosikhu, M.: Konstruksi Hukum Pidana terhadap Kejahatan Deepfake dalam Perspektif Manipulasi Bukti Digital. Justice Voice **5**(1), 47–59 (2026)

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

