

## Criminal Liability for Deepfake Dissemination: Under Indonesia's Cybercrime Framework

B. Wahyu Nurmita Sari<sup>1</sup>, Ali Huristak Hartawlan Hasibuan<sup>2</sup>, Suharto<sup>3</sup>

<sup>1</sup> Universitas Islam Kediri, Jawa Timur, Indonesia. E-mail: [wahyunurmita@student.uniska-kediri.ac.id](mailto:wahyunurmita@student.uniska-kediri.ac.id)

<sup>2</sup> Universitas Islam Kediri, Jawa Timur, Indonesia. E-mail: [alihatibuan@uniska-kediri.ac.id](mailto:alihatibuan@uniska-kediri.ac.id)

<sup>3</sup> Universitas Islam Kediri, Jawa Timur, Indonesia. E-mail: [suharto.fh@uniska-kediri.ac.id](mailto:suharto.fh@uniska-kediri.ac.id)

### ABSTRACT

*The advancement of artificial intelligence (AI) technology, particularly the Generative Adversarial Network (GAN) architecture, has given rise to deepfakes, a serious threat to the digital information ecosystem. Deepfake technology enables the synthesis of a person's face, voice, and body movements into highly convincing fabricated content, thereby posing risks to information integrity, individual privacy, and national security. This study aims to analyze: (1) the legal qualification of deepfake dissemination as a criminal act of electronic information manipulation under Article 35 in conjunction with Article 51 paragraph (1) of Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law; and (2) the forms of criminal liability imposed upon perpetrators of harmful deepfake dissemination based on the 2024 Electronic Information and Transactions Law and Law Number 27 of 2022 concerning Personal Data Protection. This research employs a normative juridical method, drawing on statutory, conceptual, and comparative approaches. The findings indicate that the dissemination of deepfake content may be classified as electronic information manipulation under Article 35 of the 2024 Electronic Information and Transactions Law, carrying penalties of up to 12 years' imprisonment and/or fines of up to IDR 12,000,000,000. Furthermore, the creation of deepfake content involving biometric data without consent constitutes a violation of the Personal Data Protection Law, punishable by up to 6 years' imprisonment and/or fines of up to IDR 6,000,000,000. This study recommends establishing a *lex specialis* regulation explicitly criminalizing the creation and dissemination of harmful deepfake content, accompanied by mandatory labeling of AI-generated content and strengthened digital forensic capabilities.*

**Keywords:** Criminal Liability, Cybercrime, Deepfake, ITE Law, Personal Data Protection.

**Citation:** Sari, B. Wahyu Nurmita, Ali Huristak Hartawlan Hasibuan, and Suharto. 2026. "Criminal Liability in the Dissemination of Deepfake Content as a Cybercrime: A Normative Study Based on the Electronic Information and Transactions Law and the Personal Data Protection Law". *Mulawarman Law Review* 3 (1), 1-4. <https://doi.org/10.30872/mulrev.v3i1.43>.

### INTRODUCTION

The Fourth Industrial Revolution has been characterized by the rapid advancement of artificial intelligence (AI) technology, which has expanded into nearly every aspect of human life. One of the most advanced products of AI development is deepfake technology, a digital media manipulation technique that utilizes deep learning algorithms, par-

ticularly the Generative Adversarial Network (GAN) architecture, to synthesize a person's face, voice, and body movements into video or audio content that appears visually authentic.<sup>1</sup> The term "deepfake" combines the words "deep learning" and "fake," and first emerged on the Reddit platform in 2017, when anonymous accounts began distributing pornographic videos featuring digitally manipulated celebrity faces without consent.<sup>2</sup> The capability of deepfake technology to create highly convincing fabricated content has posed serious threats, ranging from non-consensual intimate imagery (NCII) and financial fraud to political disinformation campaigns and the destruction of individual reputations. Research conducted by Deeptrace Labs (2019) revealed that 96% of deepfake content circulating on the internet consisted of pornographic material, all of which was created without the consent of the manipulated subjects.<sup>3</sup> In Indonesia, sexually explicit deepfake cases targeting female public figures in politics and entertainment have begun to emerge, demonstrating that this phenomenon is no longer merely a hypothetical threat.<sup>4</sup>

This phenomenon presents significant legal challenges. Although Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 on Electronic Information and Transactions (UU ITE) regulates various forms of cybercrime, it does not explicitly recognize deepfakes as a regulated subject matter. The revision introduced through Law Number 1 of 2024 (UU ITE 2024) is expected to strengthen the existing legal framework. On the other hand, Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) has the potential to serve as an important legal instrument in addressing deepfake cases, which inherently involve victims' biometric data.<sup>5</sup> The vagueness of norms within the existing legislation may create a legal vacuum (*lacuna legis*), thereby complicating the prosecution of individuals responsible for disseminating deepfake content. From the perspective of criminal law theory, the application of the principle of legality (*nullum crimen, nulla poena sine lege*) requires the existence of clear and foreseeable legal norms before an act may be criminalized.<sup>6</sup> This condition makes an in-depth examination of the legal qualification and forms of criminal liability for the dissemination of deepfake content an urgent academic necessity.

---

<sup>1</sup> Ruben Tolosana et al., "Deepfakes and beyond: A Survey of Face Manipulation and Fake Detection," *Information Fusion* 64 (December 2020): 131–48, <https://doi.org/10.1016/j.inffus.2020.06.014>.

<sup>2</sup> Bobby Chesney and Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy*, 107 (2019): 1753–820, <https://doi.org/10.15779/Z38RVOD15J>.

<sup>3</sup> Henry Ajder et al., *The State of Deepfakes: Landscape, Threats, and Impact* (Deeptrace, 2019), 1–27.

<sup>4</sup> Karolus Charlaes Bego et al., "Tindak Pidana Cybercrime: Tantangan Hukum Pidana Dalam Menanggulangi Kejahatan Di Dunia Maya (Desember 2024)," *Jurnal Kolaboratif Sains* 8, no. 1 (2025): 506–11, <https://doi.org/10.56338/jks.v8i1.6740>.

<sup>5</sup> Graham Greenleaf, "Global Data Privacy Laws 2023: 162 National Laws and 20 Bills," SSRN Scholarly Paper no. 4426146 (Social Science Research Network, February 10, 2023), <https://doi.org/10.2139/ssrn.4426146>.

<sup>6</sup> Moeljatno Moeljatno, *Asas-Asas Hukum Pidana*, 8th Ed (Rineka Cipta, 2021).

## METHOD

This study employs a normative legal research method, namely legal research conducted through the examination of library materials or secondary data as the primary sources of analysis.<sup>7</sup> The normative method was selected because the study focuses on legal norms contained in statutory regulations, legal principles, and legal doctrines related to criminal liability for the dissemination of deepfake content. The research applies three approaches. First, the statutory approach, which examines all relevant legislation, particularly the 2024 Electronic Information and Transactions Law (UU ITE 2024) and the Personal Data Protection Law (UU PDP). Second, the conceptual approach, which draws on criminal law doctrines, especially theories of criminal liability, to identify relevant legal concepts and principles. Third, the comparative approach, which compares regulations in several jurisdictions that already possess specific provisions regarding deepfake technology.<sup>8</sup> The legal materials used include primary (statutory regulations and court decisions), secondary (textbooks, accredited scientific journal articles, and research reports), and tertiary (legal dictionaries and encyclopedias). The analysis was conducted qualitatively using legal interpretation methods, particularly grammatical, systematic, and teleological interpretation, to reveal the meaning of relevant legal norms in the context of the deepfake phenomenon.

## DISCUSSION

### Definition and Characteristics of Deepfake Technology as an Instrument of Cybercrime

Deepfake is an artificial intelligence-based content manipulation technology that uses deep learning techniques, particularly the Generative Adversarial Network (GAN) architecture, to produce synthetic images, videos, or audio that are visually and/or audibly indistinguishable from authentic content. GAN operates through two artificial neural networks that operate adversarially: a generator that generates fabricated content and a discriminator that attempts to distinguish fabricated content from genuine material. Through repeated training processes, the manipulated content becomes increasingly realistic.<sup>9</sup> Tolosana et al.<sup>10</sup> classify deepfake techniques into four primary categories: (1) face swapping, namely replacing one person's face with another's; (2) face reenactment, namely manipulating facial expressions or movements; (3) face synthesis, namely creating human faces that do not actually exist; and (4) voice synthesis, namely imitating a person's voice. These four techniques may be combined to create increasingly complex deepfake content. Recent studies even indicate that deepfake technology has developed beyond facial manipulation to include the synthesis of full-body movements.<sup>11</sup>

In the context of criminal law, four characteristics of deepfake technology are most legally relevant. First, it can manipulate an individual's identity, which constitutes legally

---

<sup>7</sup> Mahmud Marzuki, *Penelitian Hukum: Edisi Revisi* (Prenada Media, 2017).

<sup>8</sup> Marzuki, *Penelitian Hukum*.

<sup>9</sup> Ian Goodfellow et al., *Deep Learning*, Adaptive Computation and Machine Learning Series, ed. Francis Bach (MIT Press, 2016), <https://mitpress.mit.edu/9780262035613/deep-learning/>.

<sup>10</sup> Tolosana et al., "Deepfakes and Beyond."

<sup>11</sup> Yisroel Mirsky and Wenke Lee, "The Creation and Detection of Deepfakes: A Survey," *ACM Computing Surveys* 54, no. 1 (2022): 1–41, <https://doi.org/10.1145/3425780>.

protected biometric data. Second, it has the capacity to deceive public perception on a massive scale, thereby causing serious and difficult-to-repair reputational harm. Third, the ease of replication and distribution through social media platforms, which intensifies the victim's losses. Fourth, the technical challenges involved in detecting and proving the existence of manipulation.<sup>12</sup>

As an instrument of cybercrime, the dissemination of harmful deepfake content corresponds with the elements of cyber offenses under the Convention on Cybercrime (Budapest Convention), ETS No. 185, 2021, namely crimes committed through or against computer systems and internet networks. Although Indonesia has not ratified the Budapest Convention, its principles have served as a reference in the formulation of the Electronic Information and Transactions Law (UU ITE), the national cyber law framework.<sup>13</sup> Furthermore, the threat posed by deepfake technology to democracy and national security has increasingly attracted the attention of academics and international policymakers.<sup>14</sup> Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (UU ITE 2024) represents the most recent legislative reform in Indonesian cyber law. The most relevant provision concerning the deepfake phenomenon is Article 35, which prohibits the manipulation of electronic information and/or electronic documents. Textually, Article 35 provides: "Every Person who intentionally and unlawfully or without authority manipulates, creates, alters, deletes, or destroys Electronic Information and/or Electronic Documents with the intention that such Electronic Information and/or Electronic Documents be regarded as though they were authentic data." This provision may be applied to the dissemination of deepfake content if all elements of the offense are fulfilled.<sup>15</sup>

To classify the dissemination of deepfake content as a criminal offense under Article 35 of the 2024 Electronic Information and Transactions Law, all elements of the offense must be cumulatively satisfied. The analysis of each element is presented as follows. The Element of "Every Person" (Legal Subject) refers to the subject of criminal law, namely a person (*naturlijke persoon*) or legal entity (*rechtspersoon*) that may be held criminally liable. In the context of deepfake technology, perpetrators may be individuals or corporations that use or distribute it for harmful purposes. Corporate criminal liability has been recognized in the Indonesian legal system through various sectoral laws, including the Electronic Information and Transactions Law (UU ITE).<sup>16</sup> In situations where deep-

---

<sup>12</sup> Chesney and Citron, *Deep Fakes*.

<sup>13</sup> Mika Westerlund, "The Emergence of Deepfake Technology: A Review," *Technology Innovation Management Review* 9, no. 11 (2019): 39–52, <https://doi.org/10.22215/timreview/1282>.

<sup>14</sup> Chesney and Citron, *Deep Fakes*; Luciano Floridi et al., "How to Design AI for Social Good: Seven Essential Factors," *Science and Engineering Ethics* 26, no. 3 (2020): 1771–96, <https://doi.org/10.1007/s11948-020-00213-5>.

<sup>15</sup> Ayunita Nur Rohanawati and Mailinda Eka Yuniza, "Problems with the Institutional Form of the Implementing Agency of Social Security in Indonesia," *Jurnal Hukum Ius Quia Iustum* 31, no. 1 (2024): 128–50, <https://doi.org/10.20885/iustum.vol31.iss1.art6>.

<sup>16</sup> Kristian Kristian, *Sistem Pertanggungjawaban Pidana Korporasi: Tinjauan Teoritis Dan Perbandingan Hukum Di Berbagai Negara* (Refika Aditama, 2016).

fake content is produced by business entities or technology platforms, this doctrine becomes highly relevant and requires further development through Indonesian jurisprudence.

The element of intent (*dolus*) constitutes a decisive subjective element within the offense under Article 35 of the 2024 Electronic Information and Transactions Law (*UU ITE 2024*). In Indonesian criminal law doctrine, intent is interpreted as the will to commit an act while being aware of its consequences.<sup>17</sup> Referring to Van Hamel's doctrine, intent encompasses three forms: *dolus directus* (direct intention toward the consequence), *dolus indirectus* (acceptance of the consequence as certainty), and *dolus eventualis* (acceptance of the consequence as a possible outcome).<sup>18</sup> In the context of deepfake technology, intent is reflected in three aspects: (i) the perpetrator's active decision to use AI technology to manipulate the victim's identity; (ii) the perpetrator's awareness that the created content is false and deceptive; and (iii) the intention to distribute such content so that it is perceived as authentic information. The use of technically sophisticated GAN technology inherently demonstrates deliberate *mens rea* rather than mere negligence (*culpa*).<sup>19</sup> The unlawful nature of Article 35 of the 2024 Electronic Information and Transactions Law must be affirmatively proven. The creation and dissemination of deepfake content that manipulates a person's face, voice, or identity without consent are inherently unlawful because such acts violate the rights to personal integrity, privacy, and control over one's own image, as guaranteed under Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia. The concept of material unlawfulness in Indonesian criminal law also encompasses violations of unwritten legal principles and societal notions of justice, as evidenced by acts involving non-consensual identity manipulation.<sup>20</sup> This element constitutes the core (*actus reus*) of the offense under Article 35. Pursuant to Article 1, paragraph 1 of the 2024 Electronic Information and Transactions Law, "Electronic Information" includes one or a set of electronic data, including writings, sounds, images, photographs, and similar forms that have been processed and possess meaning. Within such a broad scope, video, image, and audio content generated through deepfake technology clearly fall within this category. Manipulation in the context of deepfake technology involves replacing or synthesizing a person's face, voice, or identity using AI algorithms, thereby fundamentally altering the authenticity of the original content.<sup>21</sup>

This purposive element distinguishes harmful deepfakes from the use of similar technologies for artistic or entertainment purposes that are transparently disclosed, such as CGI in films with clear labeling. Harmful deepfake dissemination inherently aims to cause recipients to perceive manipulated content as authentic recordings or information. This purpose may be proven through the context of dissemination, the presentation of the

---

<sup>17</sup> Moeljatno, *Asas-Asas Hukum Pidana*.

<sup>18</sup> Teguh Prasetyo et al., *Hukum Pidana*, Rev. Ed. (Raja Grafindo Persada, 2023).

<sup>19</sup> Mahrus Ali, *Dasar-Dasar Hukum Pidana* (Sinar Grafika, 2022).

<sup>20</sup> Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan* (Prenada Media, 2018).

<sup>21</sup> Sekaring Ayumeida Kusnadi and Dina Wanda Setiawan Putri, "Perlindungan Hak Privasi dalam Penyalahgunaan Teknologi Deepfake di Indonesia," *Jurnal Rechtsvinding: Media Pembinaan Hukum Nasional* 14, no. 2 (2025), <https://doi.org/10.33331/rechtsvinding.v14i2.2135>.

content without clarification that it is fictional, and the choice of distribution platforms.<sup>22</sup> The doctrine of purposive interpretation supports a teleological understanding of this element in accordance with legislative intent.<sup>23</sup> Based on the analysis above, the dissemination of deepfake content designed to deceive and harm others may constitute the criminal offense of electronic information manipulation under Article 35 of the 2024 Electronic Information and Transactions Law. The criminal sanctions are regulated under Article 51 paragraph (1), namely imprisonment for up to 12 years and/or fines of up to IDR 12,000,000,000. In addition to Article 35, several other provisions of the 2024 Electronic Information and Transactions Law may be cumulatively applied under the principle of *concursum idealis* (Article 63 of the Criminal Code), including Article 27 paragraph (1) regarding content violating decency norms (relevant to deepfake pornography), Article 27 paragraph (3) regarding electronic defamation, and Article 28 paragraph (1) regarding the dissemination of harmful false information.<sup>24</sup>

Criminal liability constitutes the juridical consequence arising from the fulfillment of the elements of a criminal offense by a person who possesses legal capacity for responsibility. (Roeslan, 1983) defines criminal liability as the continuation of objective blame attached to a criminal act subjectively toward a person who fulfills the requirements for punishment. Within criminal law doctrine, there are three requirements for criminal liability: (a) the capacity for responsibility (*toerekeningsvatbaarheid*); (b) fault (*schuld*), whether in the form of intent (*dolus*) or negligence (*culpa*); and (c) the absence of grounds for excuse (*schulduitsluitingsgrond*).<sup>25</sup>

The framework of criminal liability under the 2024 Electronic Information and Transactions Law refers to the doctrine of participation (*deelneming*) under the Criminal Code, which distinguishes between direct perpetrators (*pleger*), indirect perpetrators (*doenpleger*), co-perpetrators (*medepleger*), and instigators (*uitlokker*). Within the ecosystem of deepfake dissemination, the chain of liability may involve various parties.<sup>26</sup>

First, creators of deepfake content who directly utilize AI algorithms to manipulate electronic information may be categorized as *pleger* under Article 35 of the 2024 Electronic Information and Transactions Law. Second, parties who commission the creation of deepfake content may be classified as *doenpleger* or *uitlokker*. Third, individuals who disseminate existing deepfake content without involvement in its production process may be categorized as *medepleger* or accomplices (*medeplichtige*). Fourth, the liability of social media platforms as service providers is also a significant issue; if a platform knowingly permits harmful deepfake content to circulate after receiving notification, it may be held liable under Article 21 of the 2024 Electronic Information and Transactions Law.<sup>27</sup>

---

<sup>22</sup> Muslim Nugraha et al., "Analisis Unsur Perbuatan Melanggar Hukum Atas Penggunaan Artificial Intelligence Dalam Kasus Konten Deepfake," *Legal System Journal* 2, no. 1 (2025): 23–36, <https://doi.org/10.70656/ljsj.v2i1.392>.

<sup>23</sup> Marzuki, *Penelitian Hukum*.

<sup>24</sup> Andi Hamzah, *KUHP & KUHPA*, Edisi Revisi (Rineka Cipta, 2014).

<sup>25</sup> Ali, *Dasar-Dasar Hukum Pidana*; Prasetyo et al., *Hukum Pidana*.

<sup>26</sup> E. Setiadi, *Hukum Pidana: Teori Dan Praktik* (Refika Aditama, 2021).

<sup>27</sup> Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan*.



Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) provides a distinct yet complementary layer of protection alongside the 2024 Electronic Information and Transactions Law in addressing deepfake cases. The relevance of the Personal Data Protection Law lies in the fact that deepfake technology inherently involves the collection, processing, and use of a person's biometric data (facial features and voice) without consent, which constitutes "specific personal data" as referred to in Article 4 paragraph (2) letter b of the Personal Data Protection Law.<sup>28</sup>

Article 1, paragraph 1 of the Personal Data Protection Law defines personal data as data concerning an identified or identifiable individual, either directly or indirectly, through electronic or non-electronic systems. A person's facial and voice data used to create deepfake content clearly falls within this definition, particularly as biometric data subject to stricter protection. Furthermore, Article 20 of the Personal Data Protection Law requires a lawful basis for data processing, including explicit consent from the data subject; therefore, creating deepfake content using a person's face or voice without their consent clearly violates this provision.<sup>29</sup> The criminal provisions of the Personal Data Protection Law relevant to deepfake technology include two principal articles. Article 65 regulates criminal sanctions for parties who unlawfully or without authority process personal data, punishable by imprisonment of up to 5 years and/or fines of up to IDR 5,000,000,000. Article 66 regulates sanctions against parties who create or falsify personal data for personal or third-party benefit, punishable by imprisonment of up to 6 years and/or fines of up to IDR 6,000,000,000. In addition, Article 70 of the Personal Data Protection Law governs corporate liability, under which fines imposed on corporations may be increased up to ten times the maximum fines applicable to individuals, thereby constituting highly significant sanctions for technology companies involved in the development or commercialization of harmful deepfake content.<sup>30</sup>

### **Comparative Regulation of Deepfake Technology Across Various Jurisdictions**

A comparative review of deepfake regulations across jurisdictions is important for identifying best practices that can be adapted to the Indonesian context. The United States has adopted a sectoral approach through several specific regulations, including the *DEEPFAKES Accountability Act* (2019), which requires watermarking on deepfake content; the *Malicious Deep Fake Prohibition Act* (2018), which criminalizes deepfakes used for fraudulent purposes; and state-level regulations such as California AB-602 prohibiting deepfake pornography and AB-730 regulating deepfakes in electoral contexts.<sup>31</sup> This approach specifically targets deepfake use within domains considered most harmful.

---

<sup>28</sup> Greenleaf, "Global Data Privacy Laws 2023."

<sup>29</sup> Kurdi Kurdi and Joko Cahyono, "Perlindungan Data Pribadi di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022," *JUNCTO: Jurnal Ilmiah Hukum* 6, no. 2 (2024): 330–39, <https://doi.org/10.31289/juncto.v6i2.5443>.

<sup>30</sup> Nugraha et al., "Analisis Unsur Perbuatan Melanggar Hukum Atas Penggunaan Artificial Intelligence Dalam Kasus Konten Deepfake."

<sup>31</sup> Chesney and Citron, *Deep Fakes*.

China has adopted a more comprehensive and ex ante approach through the *Provisions on the Management of Deep Synthesis Internet Information Services* issued by the Cyberspace Administration of China (CAC) in November 2022. This regulation requires providers of deep synthesis services to label AI-generated content, prohibits the use of deepfake technology to create content that disrupts social order, and requires user identity verification.<sup>32</sup>

The European Union regulates deepfake technology within a broader framework through the *AI Act* (2024) and the *Digital Services Act* (DSA). The AI Act classifies AI systems generating synthetic content as systems that must comply with high transparency standards, including mandatory watermarking of AI-generated content. The DSA obliges platforms to take action against harmful and misleading deepfake content.<sup>33</sup> The European Union's approach is considered the most comprehensive because it combines preventive measures, platform regulation, and user protection. This comparative regulatory analysis demonstrates that Indonesia requires a more specific legislative approach. Although the 2024 Electronic Information and Transactions Law (UU ITE 2024) and the Personal Data Protection Law (UU PDP) provide an adequate legal basis for prosecution, neither was specifically designed to address the technological complexity and social impacts of deepfake technology. Therefore, a *lex specialis* regulation, or at minimum a government regulation explicitly defining deepfake technology, requiring labeling of AI-generated content, and regulating reporting and removal mechanisms for harmful content, is necessary.<sup>34</sup>

One of the greatest challenges in enforcing the law against deepfake-related cases concerns evidentiary issues. The evidentiary system within Indonesian criminal procedure law, which adopts the principle of minimum proof (Article 183 of the Criminal Procedure Code), requires at least two valid forms of evidence and judicial conviction before criminal sanctions may be imposed.<sup>35</sup> In the context of deepfake technology, several significant evidentiary problems arise. The first challenge concerns verifying the authenticity of digital content. Proving that certain content constitutes a deepfake rather than an authentic recording requires advanced expertise in digital forensics. Recent research demonstrates a significant detection-generation gap, in which deepfake detection capabilities lag behind generation technologies.<sup>36</sup> In Indonesia, the current capacity of digital forensic institutions has not yet fully enabled reliable deepfake detection, thereby requiring immediate strengthening. The second challenge concerns identifying perpetra-

---

<sup>32</sup> "The Convention on Cybercrime (Budapest Convention, ETS No. 185) and Its Protocols," Cybercrime, accessed May 13, 2026, <https://www.coe.int/en/web/cybercrime/the-budapest-convention>.

<sup>33</sup> Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA Relevance) (2024), <http://data.europa.eu/eli/reg/2024/1689/oj>.

<sup>34</sup> Bego et al., "Tindak Pidana Cybercrime"; Kusnadi and Putri, "Perlindungan Hak Privasi dalam Penyalahgunaan Teknologi Deepfake di Indonesia."

<sup>35</sup> Hamzah, *KUHP & KUHP*.

<sup>36</sup> Mirsky and Lee, "The Creation and Detection of Deepfakes."



tors. Deepfake perpetrators frequently operate anonymously, using VPNs or cyberinfrastructure located across multiple jurisdictions. Digital tracing, therefore, requires cross-platform and cross-border cooperation, which is often hindered by differences in legal regimes and inefficient mutual legal assistance (MLA) mechanisms.<sup>37</sup>

The third challenge concerns proving the element of intent. Although the existence of deepfake content may be technically identified, proving that the perpetrator knew the content was fabricated and intentionally distributed it to be perceived as authentic requires comprehensive digital evidence, including file metadata, digital communication records, and patterns of content distribution.<sup>38</sup> To address these challenges, several strategic measures are necessary. First, enhancing law enforcement agencies' digital forensic capabilities for deepfake detection. Second, developing specialized digital forensic standards for deepfake-related cases. Third, strengthening international cooperation through extradition agreements and mutual legal assistance mechanisms. Fourth, establishing specialized cybercrime units with technical expertise in AI forensics. These recommendations align with the direction of national policy outlined in the National Cybersecurity Strategy and may serve as a reference for reforming criminal procedural law to address the challenges posed by next-generation digital crimes.

## CONCLUSION

The dissemination of harmful deepfake content may constitute the offense of electronic information and/or electronic document manipulation under Article 35 of the 2024 Electronic Information and Transactions Law (UU ITE 2024), punishable under Article 51(1), provided all legal elements of the offense are satisfied. Depending on the context, perpetrators may also be charged under Article 27 concerning immoral content or defamation. Second, criminal liability extends to both the 2024 Electronic Information and Transactions Law and the Personal Data Protection Law (UU PDP), particularly where unauthorized use of biometric personal data is involved, including potential corporate liability. However, the current legal framework remains inadequate to comprehensively address deepfake-related crimes. Therefore, this study recommends the adoption of specific regulations governing deepfake technology, strengthening digital forensic capabilities, enhancing international cooperation, and improving reporting and content removal mechanisms for AI-generated harmful content.

---

<sup>37</sup> Westerlund, "The Emergence of Deepfake Technology."

<sup>38</sup> Bego et al., "Tindak Pidana Cybercrime."

## REFERENCES

- Ajder, Henry, Giorgio Patrini, Francesco Cavalli, and Laurence Cullen. *The State of Deep-fakes: Landscape, Threats, and Impact*. Deeptrace, 2019.
- Ali, Mahrus. *Dasar-Dasar Hukum Pidana*. Sinar Grafika, 2022.
- Arief, Barda Nawawi. *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan*. Prenada Media, 2018.
- Bego, Karolus Charlaes, Fajar Rahmat Aziz, Riadi Asra Rahmad, Sunarto, and Heri Budianto. "Tindak Pidana Cybercrime: Tantangan Hukum Pidana Dalam Menanggulangi Kejahatan Di Dunia Maya (Desember 2024)." *Jurnal Kolaboratif Sains* 8, no. 1 (2025): 506–11. <https://doi.org/10.56338/jks.v8i1.6740>.
- Chesney, Bobby, and Danielle Citron. *Deep Fakes: A Looming Challenge for Privacy*. 107 (2019): 1753–820. <https://doi.org/10.15779/Z38RV0D15J>.
- Cybercrime. "The Convention on Cybercrime (Budapest Convention, ETS No. 185) and Its Protocols." Accessed May 13, 2026. <https://www.coe.int/en/web/cyber-crime/the-budapest-convention>.
- Floridi, Luciano, Josh Cowls, Thomas C. King, and Mariarosaria Taddeo. "How to Design AI for Social Good: Seven Essential Factors." *Science and Engineering Ethics* 26, no. 3 (2020): 1771–96. <https://doi.org/10.1007/s11948-020-00213-5>.
- Goodfellow, Ian, Yoshua Bengio, and Aaron Courville. *Deep Learning*. Adaptive Computation and Machine Learning Series, edited by Francis Bach. MIT Press, 2016. <https://mitpress.mit.edu/9780262035613/deep-learning/>.
- Greenleaf, Graham. "Global Data Privacy Laws 2023: 162 National Laws and 20 Bills." SSRN Scholarly Paper No. 4426146. Social Science Research Network, February 10, 2023. <https://doi.org/10.2139/ssrn.4426146>.
- Hamzah, Andi. *KUHP & KUHPA*. Edisi Revisi. Rineka Cipta, 2014.
- Kristian, Kristian. *Sistem Pertanggungjawaban Pidana Korporasi: Tinjauan Teoritis Dan Perbandingan Hukum Di Berbagai Negara*. Refika Aditama, 2016.
- Kurdi, Kurdi, and Joko Cahyono. "Perlindungan Data Pribadi di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022." *JUNCTO: Jurnal Ilmiah Hukum* 6, no. 2 (2024): 330–39. <https://doi.org/10.31289/juncto.v6i2.5443>.
- Kusnadi, Sekaring Ayumeida, and Dina Wanda Setiawan Putri. "Perlindungan Hak Privasi dalam Penyalahgunaan Teknologi Deepfake di Indonesia." *Jurnal Rechtsvinding: Media Pembinaan Hukum Nasional* 14, no. 2 (2025). <https://doi.org/10.33331/rechtsvinding.v14i2.2135>.
- Marzuki, Mahmud. *Penelitian Hukum: Edisi Revisi*. Prenada Media, 2017.
- Mirsky, Yisroel, and Wenke Lee. "The Creation and Detection of Deepfakes: A Survey." *ACM Computing Surveys* 54, no. 1 (2022): 1–41. <https://doi.org/10.1145/3425780>.
- Moeljatno, Moeljatno. *Asas-Asas Hukum Pidana*. 8th Ed. Rineka Cipta, 2021.

- Nugraha, Muslim, Amanda Sela Sadina, Viraliza Ramadonna, and Keysyah Aulia Hidayat. "Analisis Unsur Perbuatan Melanggar Hukum Atas Penggunaan Artificial Intelligence Dalam Kasus Konten Deepfake." *Legal System Journal* 2, no. 1 (2025): 23–36. <https://doi.org/10.70656/ljsj.v2i1.392>.
- Prasetyo, Teguh, Yuni Priskila Ginting, and Rizky Karo Karo. *Hukum Pidana*. Rev. Ed. Raja Grafindo Persada, 2023.
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA Relevance) (2024). <http://data.europa.eu/eli/reg/2024/1689/oj>.
- Rohanawati, Ayunita Nur, and Mailinda Eka Yuniza. "Problems with the Institutional Form of the Implementing Agency of Social Security in Indonesia." *Jurnal Hukum Ius Quia Iustum* 31, no. 1 (2024): 128–50. <https://doi.org/10.20885/iustum.vol31.iss1.art6>.
- Setiadi, E. *Hukum Pidana: Teori Dan Praktik*. Refika Aditama, 2021.
- Tolosana, Ruben, Ruben Vera-Rodriguez, Julian Fierrez, Aythami Morales, and Javier Ortega-Garcia. "Deepfakes and beyond: A Survey of Face Manipulation and Fake Detection." *Information Fusion* 64 (December 2020): 131–48. <https://doi.org/10.1016/j.inffus.2020.06.014>.
- Westerlund, Mika. "The Emergence of Deepfake Technology: A Review." *Technology Innovation Management Review* 9, no. 11 (2019): 39–52. <https://doi.org/10.22215/timreview/1282>.