The Indonesian Journal of International Clinical Legal Education
Vol. 7 Issue 1 (2025) 37-66
DOI: https://doi.org/10.15294/ijicle.v7i1.25525
Available online since: March 31, 2025

The Indonesian Journal of International Clinical Legal Education
https://journal.unnes.ac.id/sju/index.php/iccle/index

Criminal Law Enforcement on Digital Identity Misuse in AI Era for Commercial Interests in Indonesia

Ameena Syifa Dwiandari ✉
Faculty of Law, Universitas Negeri Semarang, Semarang, Indonesia

Ridwan Arifin
Faculty of Law, Universitas Negeri Semarang, Semarang, Indonesia

✉ Corresponding email: amee_sy_dwiandari@students.unnes.ac.id

Abstract

The rapid development of Artificial Intelligence (AI) technology particularly in the forms of deepfakes and voice cloning has significantly impacted the lives of Indonesians. While AI offers various conveniences and innovations, it also poses serious threats, especially the misuse of digital identities for commercial purposes. This study aims to analyze the adequacy and effectiveness of Indonesia's criminal law, particularly the Indonesian Criminal Code and Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), in addressing AI-based digital identity crimes. Using a normative juridical approach, this research finds that current legal frameworks do not specifically regulate AI-related offenses. As a result, perpetrators often exploit legal and

technological loopholes to avoid prosecution. The consequences of these crimes are far-reaching, including financial losses, reputational damage, and psychological trauma for victims. The study recommends revising the ITE Law, strengthening personal data protection, forming an AI-based digital forensics task force, and fostering cross-sectoral collaboration to combat digital identity crimes without stifling technological innovation.

Keywords
Artificial Intelligence; Identity Misuse; Law Enforcement.

I. Introduction

Technology is something that has become a human need in a series of activities carried out every day. Various forms of physical technology or features have often been applied in parts of human life. The rapid development of technology is also the biggest factor that causes humans to be inseparable from the use of technology. The presence of this technology causes major changes in the lives of mankind from various types of factors. Indonesia is one of the countries that has experienced the influence of these technological developments, both urban and rural communities, technology has had a major influence on people's lives.

The presence of technology in today's digital era allows everyone to access and search for information easily and quickly from simple to complex things, technology can help humans so that this can affect views and lifestyles. Based on data collected by the Indonesian Internet Service Providers Association (APJII) from December 18, 2023 to January 19, 2024, the number of internet users in Indonesia in 2024

has reached 221,563,479 out of a total population of 278,696,200 Indonesians in 2023, which has increased every year.[1]

One of the features that is now widespread among the public is Artificial Intelligence. Artificial intelligence or more commonly known as Artificial Intelligence (AI) is a form of technological power programmed to understand and assist humans by learning algorithms and data in the digital world. AI aims to create systems or machines that can perform tasks that typically require human intelligence, such as learning, reasoning, problem solving, visual perception, and natural language processing.[2] AI consists of several important underlying concepts such as Machine Learning which allows systems to learn from data without explicit programming,[3] Deep Learning which uses artificial neural networks to model complex data such as images, sounds, and text,[4] Natural Language Processing which allows machines to understand, interpret, and generate human language,[5] and Computer Vision to process and analyze visuals such as images or videos.[6]

The real form of AI's presence in everyday life can be seen from things like facial recognition (smartphone unlocking, airport or station security, public surveillance from CCTV cameras, social media automatically detecting faces in Facebook and Instagram applications) and voice (virtual assistants, automatic transcripts, customer service with AI, smart home device control), in-app search engines (Google Search, Google Lens, and search using voice commands), and many

---

1 Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), "APJII: Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang," APJII, accessed 11 May 2025, https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang.

2 Stuart J. Russell dan Peter Norvig, *Artificial Intelligence: A Modern Approach*, edisi ke-4 (Boston: Pearson, 2016), 3.

3 Mitchell, T. M., *Machine Learning*, vol. 1, no. 9 (New York: McGraw-Hill, 1997), 2.

4 Goodfellow, Ian, Yoshua Bengio, Aaron Courville, and Yoshua Bengio. *Deep learning*. Vol. 1, no. 2. (Cambridge: MIT press, 2016.) 76.

5 Dan Jurafsky and James H. Martin, *Speech and Language Processing*, 3rd ed. (Pearson, 2023), 45.

6 Szeliski, Richard. *Computer Vision: Algorithms and Applications* (Springer Nature, 2022), 78.

more. The initial presence of AI in the world of technology received positive feedback from all users, with various types of new features that can facilitate and assist human activities every day, it is hoped that there will be developments that can advance human performance in the future.

However, the use of AI is not only used for positive things. With the rapid advancement of technology, challenges and threats can certainly arise and affect its users. There are many types of crimes using AI that have been rampant in society, not only harming users but also people who receive or view information materially or immaterially. There have been various types of cases regarding misuse in various aspects, what often happens is the spread of hoax news by stealing the identity of a famous figure which is changed by using AI to convince people who do not understand AI. The hoax news that is spread varies from hoaxes about government and politics to hoaxes about the current situation in other countries.

One of the cases of misuse of AI to spread hoax news that is now rampant is by using AI to make famous public figures giving news, giving testimonials and promoting a product or service, without permission from the relevant parties. A number of Indonesian celebrities such as Melaney Ricardo, Najwa Shihab, Raffi Ahmad, Atta Halilintar to famous influencers on social media applications such as Karin Novilda as well as important figures such as the 7th Jokowi Dodo and President Prabowo Subianto, have been victims of digital identity abuse using Deepfake AI technology.

Deepfake (derived from the words "deep learning" and "fake") is an artificial intelligence (AI) technology used to create fake content to manipulate or replace a person's face, voice, or movements so that they look real..[7] Deepfake uses two main methods in the process of creating these fake videos. Generative Adversarial Networks (GANs) which are two AI models (generator and discriminator) that compete and train each other simultaneously to produce increasingly realistic images or

[7] Citron, Danielle K., and Robert Chesney. "Deepfakes and the new disinformation war." *Foreign Affairs* (2019).

videos, and Autoencoders which analyze and reconstruct facial or voice features from input data.[8]

Various types of fake videos featuring them giving testimonials or promoting certain products, such as skincare products, slimming products, or online gambling services are widely circulated on social media. One of the recent cases is a video of President Prabowo Subianto's face being misused using Deepfake AI technology. The perpetrator created a deepfake video by manipulating the original video of the public figure and changing the narration to information about the opening of social assistance programs by the government. In the video, the public figure provides information about the payment of administrative fees and then promises the disbursement of aid funds, therefore making the public believe in it.[9]

The videos were made without the permission of the relevant parties with the aim of increasing sales of the products and services. This causes losses that can damage the reputation of the relevant figures. Based on examples from these cases, there are several violations that have occurred based on the Indonesian Criminal Code, usually known as Kitab Undang-Undang Hukum Pidana (KUHP), (Articles 263, 378 on Fraud, 310-311 on Defamation) and the Law No. 11 of 2008 on Electronic Information and Transactions, usually known as Undang-Undang Informasi dan Transaksi Teknologi, (Article 27 paragraph (3), Article 28 paragraph (1), Article 35 on Information Manipulation). Therefore, researchers found several irregularities that will be discussed in this research in the form of whether the provisions in the Indonesian Criminal Code and Law No. 11 of 2008 on Electronic Information and

---

8 Goodfellow, Ian J., Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. "Generative adversarial nets." *Advances in neural information processing systems* 27 (2014).

9 "Kasus Penipuan Deepfake AI, Polri Buru Pelaku Pemalsuan Wajah Presiden-Prabowo," Media Indonesia, accessed 14 May 2025, https://mediaindonesia.com/politik-dan-hukum/737308/kasus-penipuan-deepfake-ai-polri-buru-pelaku-pemalsuan-wajah-presiden-prabowo.

Transactions are sufficient to ensnare the perpetrators of AI-based digital identity abuse and How is the criminal liability of the perpetrator (individual/corporation) in the abuse of digital identity involving AI technology.

II. Method

This research uses a normative juridical research method with a qualitative approach to analyze the adequacy of the Indonesian Criminal Code and Law No. 11 of 2008 on Electronic Information and Transactions in ensnaring the perpetrators of Artificial Intelligence (AI)-based digital identity abuse as well as the criminal liability of the perpetrators. This method was chosen because the research focuses on evaluating written legal norms, legal principles, and comparative legislation related to AI-based digital crimes.

The research was conducted through several stages: The first stage identified primary legal materials including the Indonesian Criminal Code (specifically Articles 263 and 378) and the Law No. 11 of 2008 on Electronic Information and Transactions (Articles 26, 27, and 35). The second stage analyzed secondary legal materials in the form of journals, books, and court decisions related to cybercrime and AI. Furthermore, a comparative study was conducted with international legal instruments such as the EU AI Act, as well as evaluation through a statute approach (interpretation of articles) and conceptual approach (analysis of the concept of corporate criminal liability). The analysis technique uses legal interpretation of existing provisions to identify legal gaps and propose regulatory solutions. This research is prescriptive in nature by providing recommendations for criminal law policy in the AI era.

III. The Sufficiency of the Provisions of the Indonesian Criminal Code and Law No. 11 of 2008 on Electronic Information and Transaction in Prosecuting Perpetrators of AI-Based Digital Identity Abuse

AI-based Identity Abuse

The development of artificial intelligence (AI) technology, particularly in the creation of synthetic content such as Deepfake (face or video forgery) and Voice cloning (voice forgery), has triggered a surge in digital identity crime. These technologies, originally designed for entertainment and business purposes, are now being misused for crimes such as fraud, extortion, and the dissemination of hoax information with a level of realism that is difficult to distinguish from the original. It is not only famous personalities who can be targeted, but ordinary people can also become victims of such misuse. Digital identity can be a photo or video that shows our face or voice on social media. Social media is a platform that can be accessed by anyone at any time, therefore we must be careful with the things we spread on social media with the possibility of misuse of our identities that can be accessed.

The development of AI technology has led to a trend of digital identity crimes that are increasingly sophisticated and difficult to detect. One prevalent mode is the use of Deepfake for fraud, where the perpetrator fakes a person's face or voice to trick the victim. An example of a real case that occurred was in Hong Kong (2024), where an employee was deceived by a deepfake video of a superior ordering the transfer of funds worth USD 25 million.[10] Perpetrators usually collect

---

10 "'*Everyone looked real': multinational firm's Hong Kong office loses HK$200 million after scammers stage deepfake video meeting*" South China Morning Post, accessed 15 May 2025, https://www.scmp.com/news/hong-kong/law-and-crime/article/3250851/everyone-looked-real-

victim data from social media, then process it using tools such as DeepFaceLab or FakeApp to create fake footage that looks very authentic. Besides deepfakes, voice cloning is also a serious threat, especially in the case of social engineering. In Arizona, USA (2023), a mother received a call from her "son" asking for a ransom where the voice was cloned using AI from a short audio sample. Technologies such as ElevenLabs or Resemble.AI allow perpetrators to mimic a person's voice with just a 3-second recording, making it easier to use for extortion or fraud. Another emerging mode is Synthetic identity Fraud, where a fully digital identity is created using AI, including a fake face, voice and personal data. These synthetic identities are then used to break into banking verification systems, register online loans, or even create fake official documents such as e-KTP. This trend is exacerbated by easy access to AI tools, anonymity through VPNs and cryptocurrencies, and regulatory backlogs in prosecuting perpetrators.

New opportunities for fraud crimes using digital identities have also occurred in Indonesia, especially for commercial purposes. One notable case occurred in 2023, when the National Police Criminal Investigation Unit uncovered an investment fraud syndicate that utilized Deepfake technology. The perpetrators used video footage of celebrities such as Deddy Corbuzier and Nagita Slavina, then manipulated it with the DeepFaceLab application so that it appeared to support fake crypto investments. The content was then disseminated through the WhatsApp application and Facebook Group, ensnaring victims with a total loss of IDR 50 billion. Although the perpetrators can be charged with Article 28 paragraph (1) of the Law No. 11 of 2008 on Electronic Information and Transactions on spreading false news and Article 378 of the Indonesian Criminal Code on fraud, law enforcement faces serious obstacles due to the perpetrators using offshore servers and the absence of a specific article regulating deepfakes for commercial purposes.

In addition to deepfake, voice cloning has also been used to defraud bank customers. In early 2024, a Bank BNI customer fell victim to a scam in which the perpetrator imitated the voice of a bank officer

multinational-firms-hong-kong-office-loses-hk200-million-after-scammers-stage.

using AI technology. With only the original voice recording from a customer service call, the perpetrator managed to trick the victim into providing an OTP code, which resulted in a loss of up to RP 327 million in a matter of hours.[11] This case can actually be charged with Article 263 of the Indonesian Criminal Code on identity forgery and Article 35 of the Law No. 11 of 2008 on Electronic Information and Transactions on illegal access, but the main challenge lies in the difficulty of tracking down perpetrators who use foreign VoIP technology and the absence of regulations requiring verification of voice authenticity in banking transactions.

The issue becomes even more complex when it comes to corporate liability of AI technology providers. The case of US-based Clearview AI, which was sued for collecting facial data without permission for algorithm training, set an important precedent for Indonesia where many local AI startups also use data from the internet without the owner's consent. The weak implementation of the Personal Data Protection Law (PDP Law) makes it difficult for victims to claim compensation, although theoretically they can use Article 1365 of the Civil Code on unlawful acts. To strengthen law enforcement, strategic steps are needed such as the revision of the Law No. 11 of 2008 on Electronic Information and Transactions by including a special article on AI content forgery, collaboration with digital platforms to verify advertisements using deepfake technology, and the establishment of a special task force under the National Police that focuses on digital forensics as well as AI-based. Learning from China, which since the beginning of 2023 has tightened supervision of deepfake technology, new regulations require deep synthesis service providers and users to clearly label fake content and ensure that it can be traced.[12] With a clearer legal framework and synergy between agencies, Indonesia can

---

11 "BNI Ungkap Modus Penipuan Jelang Lebaran, Bagikan Cara Cegah Kerugian," BNI, accessed 15 May 2025, https://www.bni.co.id/id-id/beranda/kabar-bni/berita/articleid/24537.

12 "*China steps up crackdown on 'misleading' AI-generated content, 'troubling phenomena'*," South China Morning Post, accessed 15 May 2025, https://www.scmp.com/news/china/politics/article/3255578/china-steps-crackdown-misleading-ai-generated-content-troubling-phenomena.

more effectively tackle digital identity crime in the AI era while still supporting technological innovation.

The misuse of AI-based digital identities has caused multidimensional adverse impacts, ranging from financial losses, reputational damage, to psychological trauma for victims. In Indonesia, investment fraud cases with deepfakes in 2023 have reached a loss of IDR 50 billion, where the perpetrators manipulate celebrity videos to trick victims. In addition to material losses, the reputational impact is also significant, as deepfake content has damaged the personal and professional lives of many victims, with some cases triggering severe depression and even suicide attempts. Psychologically, victims often experience prolonged cyber trauma due to the difficulty of removing fake content from the internet. Law enforcement challenges are increasingly complex given the development of AI technology that is always faster than regulations. Criminals utilize anonymizer tools such as VPN and blockchain to hide their identities, while generative AI technology such as Stable Diffusion allows the creation of fake identities in just minutes.[13] The case of voice fraud at Bank BNI (2024) shows how difficult it is to track down perpetrators using offshore servers and VoIP Spoofing technology. In addition, the absence of adequate digital forensics in Indonesia to track AI-generated content further exacerbates the problem.

[13] Putra, Muh Abduh Dwi. "Pelacakan Pelaku Kejahatan Siber Pengguna Virtual Private Network (Vpn) Pada Jaringan The Onion Router (Tor) (Studi Kasus Di Badan Siber Dan Sandi Negara)." PhD diss., Universitas Airlangga, 2020.

Analysis of Indonesian Criminal Code Provisions

A. Relevant Articels in the Indonesian Criminal Code

The Indonesian Criminal Code as a legal product of Dutch colonial heritage does not actually anticipate the development of AI-based digital crimes, but some of its articles can be interpreted to ensnare perpetrators through analogical interpretation. Articles 263-266 on forgery of letters or identities are the main legal basis, where forgery of digital identities through AI can be qualified as "making false letters" in analogical interpretation, such as digital identities (social media accounts and online bank profiles) and electronic documents (digital e-KTP manipulated by AI). In the case of e-KTP forgery with AI in 2023, the Attorney General's Office used Article 263 paragraph (1) with the argument that e-KTP is a "letter" in the legal sense. However, problems arose when proving the element of "with the intent to benefit oneself" for AI content that was automatically generated.

Articles 310-321 on defamation are relevant for deepfake cases that damage reputation, especially Article 310 is relevant for non-consensual deepfake cases and fake voice recordings that can damage reputation. In the Jakarta District Court Decision, a sentence of 1 year and 6 months was imposed under Article 310 for a deepfake harassment case against an artist. However, obstacles arise because the victim must prove the intention to defame the perpetrator, because the perpetrator can argue that he did not know the impact of the misuse of the content he created. Meanwhile, Article 378 on fraud can be the main weapon for deepfake-based investment fraud and voice cloning for social engineering. This article has been applied in the PT AI Profit 2024 investment fraud case, the prosecutor combined Article 378 with Article 55 participation, because the perpetrator used AI tools made by third parties.

B. Substantive Weakness of the Indonesian Criminal Code

The Indonesian Criminal Code as a legal product born long before the digital era has several fundamental weaknesses in dealing with the complexity of AI-based digital identity crimes. The

construction of articles in the Indonesian Criminal Code is still analog in nature and does not accommodate the special characteristics of digital crimes. Articles such as 263 on forgery of letters or article 310 on defamation are formulated for traditional physical contexts, so their application to digital cases requires very broad and often multiple interpretations. For example, in deepfake cases, it is difficult to determine whether a fake video recording can qualify as a "fake letter" under Article 263, as the elements of the article are not designed to capture sophisticated digital modus operandi.

The Indonesian Criminal Code does not specifically regulate the responsibilities of related parties in the AI technology ecosystem. Unlike some countries that already have special provisions on the accountability of digital platforms and AI developers, the Indonesian Criminal Code does not touch this aspect at all. In fact, many cases of digital identity abuse actually utilize AI tools developed by third parties. Without a clear regulation on the due diligence that AI developers must do, it will be difficult to ensnare perpetrators who use the platform for crimes.

Also, the evidentiary system in the Indonesian Criminal Code, which is still conventional, does not match the characteristics of digital evidence in AI cases. Elements such as "malicious intent" or "willfulness:" which are the main requirements in many articles of the Indonesian Criminal Code are very difficult to prove for content generated by AI systems. In addition, the electronic evidence mechanism stipulated in the Law No. 11 of 2008 on Electronic Information and Transactions has not been well integrated into the Indonesian Criminal Code's evidence system, creating gaps in law enforcement. The relatively light criminal penalties in the Indonesian Criminal Code (e.g., a maximum of 6 years for forgery) are also disproportionate to the massive impact that AI-based identity crimes can have.

Analysis of Law No. 11 of 2008 on Electronic Information and Transactions Provisions (Law No.11/2008 jo. Law No.19/2016)

A. Applicable Articles

The Electronic Information and Transaction Law (UU ITE) has several provisions that form the basis of law enforcement against AI-based digital identity abuse, namely: Article 27 paragraph (3) on defamation, a mainstay in dealing with deepfake cases that harm reputation. This article has been used in various cases. However, its application is often criticized due to the many interpretations of the term "defame" in the digital space. Article 28 paragraph (1) on the dissemination of false news is relevant for AI content manipulation cases that mislead the public. An example of the application of this article is in the case of President Joko Widodo's deepfake hoax in 2023, where the perpetrator was charged with this article, but faced difficulties in proving the element of "knowing the lie" in AI-generated content. Articles 35-36 on data falsification and illegal access are important legal grounds for cases of creating fake digital identities. Article 35 in particular has been used in the case of breaking into a bank's bimetric verification system using synthetic identity in 2024.

B. Weakness of the Law No. 11 of 2008 on Electronic Information and Transactions

Although the Law No. 11 of 2008 on Electronic Information and Transactions is more progressive than the Indonesian Criminal Code, there are still some weaknesses that exist in the Law No. 11 of 2008 on Electronic Information and Transactions, namely:

1. There is no explicit regulation of AI-based content manipulation. The Law No. 11 of 2008 on Electronic Information and Transactions does not recognize key terms such as "deepfake", "synthetic media", or "AI-generated content" that characterize

AI-based crimes.[14] Compare this to California's AB-730 which specifically regulates "deepfake" in the context of elections.

2. Limited jurisdiction in dealing with cross-border offenders. In the 2023 deepfake investment fraud case involving a Singapore server and perpetrators in Malaysia, Indonesian law enforcement had difficulty extraditing due to international cooperation barriers.
3. Lack of provisions on the liability of AI service provider platforms. Unlike the EU Digital Service Act, which requires platforms to conduct a risk assessment of their AI technology, the Law No. 11 of 2008 on Electronic Information and Transactions does not provide for this obligation at all.[15]

Comparison with Other Countries' Regulations

A. AI-Related Regulations in Other Countries

In facing the challenge of AI-based identity abuse, some countries have taken progressive steps by developing specific and comprehensive legal frameworks. For example, the European Union, through the AI Act (2024), has set strict standards that classify AI systems based on their risk level, ranging from minimal to unacceptable risk.[16] This regulation not only requires transparency for generative AI systems, but also explicitly prohibits the use of AI to manipulate identities without consent (Article 52).[17] Meanwhile, the United States has taken a sectoral approach with a series of laws that target specific aspects of AI abuse. The Deepfake Accountability Act (2023) requires watermarking of synthetic content to prevent the misleading spread of deepfakes.[18] In Asia, Singapore has pioneered an AI governance framework through the AI Governance Framework, which emphasizes the principles of accountability and

---

14 California Legislative Information, "AB-730 Elections: Deceptive Audio or Visual Media," 2019.

15 European Commission, Digital Services Act (Brussels, 2022).

16 European Parliament and of The Council, Regulation on Artificial Intelligence (AI Act) 2024/1689 (2024).

17 Ibid., Article 52.

18 U.S. Congress, H.R.5586 Deepfake Accountability Act of 2023 (2023).

transparency, and requires audits for high-risk AI systems.[19] This approach not only protects consumers but also encourages responsible innovation.

B. Analysis of Regulatory Needs in Indonesia

Based on the experiences of these countries, Indonesia needs to immediately make regulatory adjustments to address the legal gap in handling AI-based digital identity abuse. The first thing that needs to be done is to make the revision of the Law No. 11 of 2008 on Electronic Information and Transactions an urgent step to include explicit definitions of content using AI and "digital manipulation", as well as requiring the labeling of AI-generated content as stipulated in the EU AI Act. Without clear definitions, law enforcement will continue to face interpretation issues, especially in distinguishing between genuine and AI-engineered content. Then, Indonesia needs specific regulations governing the responsibilities of AI platform providers and setting standards for digital identity verification. This regulation should include a due diligence mechanism for AI developers to prevent misuse of their technology, as required under the EU Digital Services Act. In addition, the legal framework should strengthen collaboration with private parties, including digital platforms and AI service providers, to proactively mitigate risks.

And finally, the establishment of specialized institutions such as the AI Regulatory Sandbox (following the Singapore model) and a team of digital forensic experts focused on AI content analysis can strengthen law enforcement capacity.[20] These institutions would not only serve as clearing houses for AI-related cases, but could also develop guidelines and technical standards for the identification and

---

19 Personal Data Protection Commission (PDPC) Singapore, Model AI Governance Framework, 2nd ed. (Singapore: IMDA, 2023).

20 Bakara, Amanda Rich Margareth. "Kerjasama Badan Siber Dan Sandi Negara (Bssn) dan Departement of Foreign Affairs And Trade (DFAT) dalam Meningkatkan Keamanan Siber Indonesia melalui Program Share Information and Best Practice Tahun (2019-2022)." PhD diss., Universitas Pembangunan Nasional Veteran Jakarta, 2024.

substantiation of deepfakes and other digital manipulations. With these steps, Indonesia can build a legal system that is more adaptive to the development of AI technology, while ensuring maximum protection for the public from digital identity abuse.

IV. Criminal Liability of Perpetrators (Individual/Corporation) in Misuse of Digital Identity with AI-Based Crime

AI-based identity crimes have become a serious threat in the digital age. The development of AI technology allows criminals to manipulate digital identities with a high level of sophistication. These crimes not only harm victims financially but also threaten privacy and cybersecurity. Unlike conventional crimes, AI-based crimes have a higher level of evidentiary difficulty due to their cross-jurisdictional nature, use of sophisticated technology, and lack of traceable digital footprints. The modus operandi also continues to evolve, utilizing AI algorithms to avoid detection by law enforcement authorities.

The difference between conventional crime and AI-based crime can be seen in the method, difficulty of proof, and impact. Conventional crimes, such as theft and outright fraud, generally involve physical interaction and can leave traces that are relatively easy to trace, such as fingerprints or eyewitnesses. Meanwhile, AI-based crimes utilize advanced technologies such as deepfake, voice cloning, or generative adversarial networks (GANs) to forge digital identities with a high degree of realism. In addition, AI crimes can be automated on a large scale, such as phishing attacks programmed through chatbots, so the impact is more massive and difficult to anticipate. The main challenge in law enforcement against AI crimes lies in the difficulty of proof, as digital evidence can be easily manipulated or deleted, while regulations

and digital forensic capacity in Indonesia still lag behind technological developments.[21]

Under Indonesian positive law, criminal liability for AI-based digital identity abuse crimes can be imposed on both individuals and corporations. For individuals, Article 263 of the Indonesian Criminal Code on forgery and Article 378 on fraud can be applied if the perpetrator intentionally manipulates digital identities for commercial purposes or harms other parties. Meanwhile, the Law No. 11 of 2008 on Electronic Information and Transactions specifically regulates cybercrime, including digital identity forgery (Article 32) and illegal access to electronic systems (Article 30). Corporations can also be held criminally liable under Article 46 of the Law No. 11 of 2008 on Electronic Information and Transactions if the crime is committed on behalf of the corporation or for the benefit of the corporation. However, the main challenge is the lack of regulatory clarity regarding the responsibility of AI development or digital platforms that may indirectly facilitate such crimes. In addition, the Personal Data Protection Bill, if enacted, could strengthen the legal framework by prescribing specific sanctions for privacy violations and data misuse. Nonetheless, the effectiveness of law enforcement still depends on the capacity of law enforcement officials in understanding AI technology as well as collaboration with related parties such as digital service providers and forensic experts.

AI-based digital identity abuse by individuals is often done through the creation of fake accounts that mimic a person's real identity.[22] Deepfake technology and voice cloning, in the case of that has occurred in 2023, a perpetrator used AI to trick customers and drain their accounts. Meanwhile, AI service providers can be held liable if their systems are used for digital identity crimes. Negligence such as the

---

21 Aini, Nurul, and Fauziah Lubis. "Tantangan Pembuktian Dalam Kasus Kejahatan Siber." *Judge: Jurnal Hukum* 5, no. 02 (2024): 55-63.

22 Denta Putra Azhar and Ahmad Mahyani, "Pertanggungjawaban Pidana Korporasi Sebagai Pelaku Tindak Pidana Penyebaran Data Pribadi," *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance* 3, no. 1 (2023): 540–58.

absence of user identity verification or lack of oversight on the use of generative AI can worsen the situation.

Individual Criminal Liability

In the context of AI-based digital identity abuse, criminal liability of individual perpetrators in Indonesia can be traced through two main instruments, namely the Indonesian Criminal Code (KUHP) and the Electronic Information and Transaction Law (Law No. 11 of 2008 on Electronic Information and Transactions). The Indonesian Criminal Code, as a general criminal law, provides a number of articles that are relevant to ensnare perpetrators of digital identity crimes. Article 263 of the Indonesian Criminal Code on mail forgery can be analogized to cases of digital identity forgery through AI technology, given that the modus operandi often involves creating fake documents or electronic data that resemble real identities. In addition, Articles 310-311 of the Indonesian Criminal Code on defamation and insult can also be applied if the misuse of digital identity can aim to damage the reputation or dignity of the victim. Article 378 of the Indonesian Criminal Code on fraud can also be an appropriate legal basis when perpetrators use AI-based fake identities to obtain material benefits unlawfully.

The Law No. 11 of 2008 on Electronic Information and Transactions can provide a more specific legal framework in regulating crimes in the digital realm. Article 27 paragraph (3) of the Law No. 11 of 2008 on Electronic Information and Transactions threatens punishment for anyone who intentionally distributes or transmits electronic content that violates decency or contains identity forgery. Article 28 paragraph (1) is also relevant in this context, especially when a fake digital identity is used to spread hatred or hoaxes that can cause hostility between individuals or groups. Then, Articles 35-36 regulate losses arising from misuse of electronic data and systems, including the use of AI to manipulate identities for the purpose of fraud or other unlawful acts. Therefore, the combination of the Indonesian Criminal Code and the Law No. 11 of 2008 on Electronic Information and Transactions can provide a comprehensive legal basis to ensnare individual perpetrators who misuse AI-based digital identities.

Despite the availability of legal instruments, law enforcement against AI-based digital identity abuse faces a number of significant challenges, especially in terms of proof. One of the main challenges is the difficulty in tracing the perpetrators due to the anonymity provided by the technology. Digital criminals often use encryption techniques, virtual private networks (VPNs), or even dark web platforms to hide their true identities. This is exacerbated by AI's ability to generate highly convincing fake identities, making it difficult for law enforcement agencies to trace the source of the crime. Moreover, the fact that many AI services are based outside Indonesian jurisdiction also adds to the complexity of handling cases, given the need for international cooperation in the investigation process.

Another important challenge is proving the element of guilt (mens rea) in AI crimes. In criminal law, the element of intent (dolus) or negligence (culpa) is the determining factor for criminal liability. However, in the context of AI, a fundamental question arises: did the perpetrator have malicious intent or simply use AI without realizing the legal impact? For example, someone who uses deepfake technology to create parody content may not intend to commit fraud or defamation. On the other hand, the rapid development of AI has also led to the phenomenon of "crimes without direct perpetrators", where AI systems can act autonomously based on programmed algorithms. This creates a legal dilemma as it is difficult to determine who should be held liable, whether the AI developer, the user, or the algorithm itself.

Corporate Criminal Liability

Corporate criminal liability in the context of AI-based digital identity misuse in Indonesia is primarily regulated in Article 40 of the Law No. 11 of 2008 on Electronic Information and Transactions. This article states that corporations can be held criminally liable for acts committed by their management or employees, both within the scope of work and for the benefit of the corporation. In addition, Law Number 11 of 2020 on Job Creation expands the scope of corporate liability by covering not

only direct acts, but also negligence in prevention ensnaring tech companies that fail to implement adequate preventive measures against the misuse of their platforms.

The two main categories of corporations that can be criminally liable in cases of AI-based digital identity abuse are AI platform providers that do not verify users (lack of due diligence), allowing individual actors to create fake accounts or spread deepfake content.[23] This kind of negligence can be considered a license to commit crimes, especially if the platform does not have an effective reporting or moderation mechanism. Also, companies that actively facilitate the creation of unmonitored deepfake content, such as generative AI service providers that do not restrict the use of their technology for illegal purposes.[24] In this case, while the company may not be directly involved in the crime, they could be deemed to be contributing to the misuse of technology if nothing is done to prevent it.

Several global cases have tested the limits of corporate liability in the context of AI misuse. One example is the lawsuit against Meta (Facebook) for failing to moderate deepfake content used for fraud. Courts in several countries have considered whether social media platforms like Meta can be penalized for negligence in preventing the spread of identity palsies, especially when their algorithms indirectly promote harmful content. Another case involves OpenAI, where critics have questioned the liability of AI developers when their technology is used to create fake identities or malicious content. Regulatory discussions in this regard have focused on the extent to which tech companies should be liable for misuse of their products, including whether a duty of "proactive oversight" should be legally imposed.

Law enforcement against corporations in AI misuse cases faces complex challenges, including the difficulty of proving negligence and

---

23 Putra, Akbar Rajendra, and Gialdah Tapiansari Batubara. "Analisis Dampak Penggunaan AI Terhadap Tindak Pidana Penipuan Online Bagi Masyarakat Di Indonesia." *Jurnal Ilmiah Multidisiplin Terpadu* 8, no. 6 (2024).

24 Citaristi, Ileana. "Organisation For Economic Co-Operation And Development—OECD." In *The Europa Directory of International Organizations 2022*, pp. 694-701. Routledge, 2022.

conflicts of jurisdiction when companies operate globally. However, recent developments in various countries, such as the EU with its AI Act, suggest that it is necessary to impose stricter legal obligations on AI service providers. In Indonesia, similar steps can be taken by strengthening the due diligence aspect in the Law No. 11 of 2008 on Electronic Information and Transactions or creating specific regulations governing the liability of AI developers. International cooperation is needed to ensure that multinational corporations cannot avoid legal liability simply because of differences in regulations between countries.

The debate on digital platform immunity with legal liability has become a crucial issue in international regulation of AI-based digital identity abuse. In the United States, Section 230 of the Communications Decency Act (1996) provides legal protection for technology platforms on the principle that they are not responsible for user-generated content.[25] However, this immunity is often criticized for facilitating the spread of harmful content, including deepfakes and digital fraud. In contrast, the EU through its Digital Services Act (DSA, 2022) and AI Act (2024) enforces proactivity and algorithmic transparency, particularly for high-risk AI systems.[26] These different approaches show variations in balancing freedom of expression and public protection from the negative impacts of technology.

In Asia, some countries have adopted a hybrid model. China, for example, through its Cybersecurity Law (2017) and Regulation on Recommendation Algorithms (2022), requires platforms to verify user identities and take responsibility for illegal content that is not immediately removed.[27] Meanwhile, Singapore's Protection from Online Falsehoods and Manipulation Act (POFMA, 2019) gives the government broad authority to order the removal of false content, including those created with AI, without completely removing platform

---

25 *47 U.S. Code § 230* (Communications Decency Act, 1996).

26 European Parliament and of the Council, *Digital Services Act (Regulation (EU) 2022/2065)* (Brussels: EU Parliament, 2022).

27 Cyberspace Administration of China, Algorithmic Recommendation Management Provisions (Beijing: CAC, 2022).

immunity.[28] For the Indonesian context, lessons from international law can be used to strengthen the Law No. 11 of 2008 on Electronic Information and Transactions, particularly by considering restrictions on platform immunity if proven negligent in preventing AI abuse, due diligence obligations such as user identity verification and algorithm audits, and proportional sanctions for corporations that intentionally or negligently facilitate digital identity crimes.

Corporate criminal liability plays an important role given that AI is often developed, operated, and utilized by corporate entities. However, Indonesian criminal law currently does not explicitly regulate corporate liability for AI malfunctions or misuse, creating a significant legal vacuum. In practice, corporate criminal liability can be adopted based on liability for AI system malfunctions that cause harm, liability for ethical negligence in the development and use of AI, and liability for inherent risks of AI technology that have not been fully anticipated.[29] This explains that if AI used by a company causes losses or criminal offenses, the corporation as a legal entity can be held liable, especially if there is evidence of negligence in the supervision, management, or application of the technology.

Moreover, in the Indonesian legal system which still refers to the principle of fault (mens rea), challenges arise in determining who should be responsible for the actions of autonomous AI. Since AI is not recognized as a legal subject, criminal responsibility must be transferred to the human or corporation that controls or utilizes the AI. Doctrines such as vicarious liability and identification doctrine become relevant to ensnare corporations for acts committed using AI within their operational scope.[30] Therefore, the establishment of clear regulations

---

28 Singapore Statutes Online, Protection from Online Falsehoods and Manipulation Act (POFMA) (2019).

29 Lukitasari, Diana. "Adopsi Model Pertanggungjawaban Pidana Korporasi Terhadap Malfungsi Penggunaan Artificial Intelligence Di Indonesia." PhD diss., UNS (Sebelas Maret University), 2023.

30 Rahman, Rofi Aulia, and Rizki Habibulah. "The criminal liability of artificial intelligence: is it plausible to Hitherto Indonesian criminal system?." *Legality: Jurnal Ilmiah Hukum* 27, no. 2 (2019): 147-160.

regarding corporate criminal liability in the use of AI is urgent in order to close the legal loopholes and provide legal certainty in the face of rapid technological development.

Proof Process and Constraints

The evidentiary process requires a specialized approach given the complexity of the technologies involved. Commonly used digital evidence tools include system logs, metadata, and algorithm recordings that can trace the origins of fake content. System logs from digital platforms can show the activity of users who created or modified deepfake content, while metadata on digital files often contain information about the time of creation and the devices used. Recordings of AI algorithms, if accessible, can be crucial evidence to prove whether content was generated by a particular system and whether there was intentional use of it for unlawful purposes. However, the availability of this evidence often depends on the cooperation of the technology company in question, which is not always easy to obtain, especially if the platform is based outside of Indonesian jurisdiction.

Although Article 5 of the Law No. 11 of 2008 on Electronic Information and Transactions recognizes electronic evidence as a valid tool in legal proceedings, its implementation still faces a number of challenges. Not all law enforcement officials understand how to adequately collect and analyze digital evidence, potentially reducing its evidentiary value in court, as well as the vulnerability of electronic evidence to data forgery or corruption, which can compromise its integrity during investigations. Furthermore, many digital service providers do not keep system logs or metadata for long enough, so important evidence is often lost before the case reaches court. This condition is exacerbated by the absence of specific regulations that require technology companies to store data related to transactions or user activities within a certain period.

In addition, there is uncertainty in determining the legal subject responsible for AI-based crimes, considering that AI systems can operate autonomously and the algorithms used may not be directly controlled

by human perpetrators. This condition creates legal uncertainty that opens a gap for perpetrators to avoid legal liability. The limited technical capacity of law enforcement agencies also exacerbates this situation, due to the lack of adequate digital forensic tools to identify AI manipulation. Overall, this legal vacuum points to the need for more adaptive and progressive regulatory reforms, including clear definitions of AI-based crimes, legal liability mechanisms, and increased technical capacity of law enforcement agencies to effectively address the complexity of crimes in the digital age.[31]

The importance of updating the Indonesian Criminal Code and Law No. 11 of 2008 on Electronic Information and Transactions is urgent to respond to the development of AI-based crimes. Amendments to the Indonesian Criminal Code should include a special chapter on digital technology and artificial intelligence crimes that could include legal definitions of deepfake, synthetic identity, and AI-generated content, specific elements to prove malicious intent in AI-based crimes, and aggravated penalties for commercial perpetrators of digital identity abuse. Then, for the Law No. 11 of 2008 on Electronic Information and Transactions, revisions should focus on mandatory content labelling for all AI-generated media (similar to the provisions of the EU AI Act), platform responsibility in preventing misuse of AI tools, and accelerated notice and takedown mechanisms for manipulative content.

The establishment of a special unit for AI cybercrime is also one of the important things to do in an effort to prevent the misuse of AI. The formation of this special unit must have specifications with a team of experts trained in digital footprint analysis to track AI content, a rapid responses unit for handling priority cases such as elections, and collaboration with the AI Security Operations Center at BSSN. Then, in direct prevention efforts from the community, public education programs on the rampant spread of deepfake content can be

---

31 Nuhi, Muhammad Hanan, Logan Al Ghozi, Syakira Nazla, and Davina Syakirah. "Pembaharuan Hukum Penanganan Tindak Pidana Pemalsuan Identitas Akibat Penyalahgunaan Artificial Intelligence Di Indonesia." *Jurnal Batavia* 1, no. 02 (2024): 80-88.

implemented in a structured manner to increase understanding of the vulnerability of hoax news spread on social media.

V. Conclusion

From the above discussion, it can be concluded that the development of artificial intelligence (AI) technology, especially deepfake and voice cloning, has had a significant impact in Indonesia, both positive and negative. On the one hand, AI facilitates various aspects of life, but on the other hand, this technology is misused for digital identity crimes such as fraud, forgery, and spreading hoaxes. Cases such as faking the faces of public figures for commercial purposes or scamming bank customers' votes show how serious this threat is. Although the Indonesian Criminal Code and Law No. 11 of 2008 on Electronic Information and Transactions have articles that can be used to ensnare perpetrators, such as Article 263 of the Indonesian Criminal Code on forgery and Articles 27-28 of the Law No. 11 of 2008 on Electronic Information and Transactions on the dissemination of illegal content, these regulations are not comprehensive enough to deal with the complexity of AI-based crimes. Key challenges include difficulty of proof, regulatory lag, and lack of digital forensic capacity. Therefore, there is a need to revise the law to include an explicit definition of AI crimes, strengthen the corporate liability of AI service providers, and increase international collaboration and public education. With these measures, Indonesia can more effectively tackle AI-based digital identity abuse while still supporting technological innovation.

VI. References

"'*Everyone looked real': multinational firm's Hong Kong office loses HK$200 million after scammers stage deepfake video meeting*" South China Morning Post, accessed 15 May 2025,

https://www.scmp.com/news/hong-kong/law-and-crime/article/3250851/everyone-looked-real-multinational-firms-hong-kong-office-loses-hk200-million-after-scammers-stage.

"BNI Ungkap Modus Penipuan Jelang Lebaran, Bagikan Cara Cegah Kerugian," BNI, accessed 15 May 2025, https://www.bni.co.id/id-id/beranda/kabar-bni/berita/articleid/24537.

"*China steps up crackdown on 'misleading' AI-generated content, 'troubling phenomena'*," South China Morning Post, accessed 15 May 2025, https://www.scmp.com/news/china/politics/article/3255578/china-steps-crackdown-misleading-ai-generated-content-troubling-phenomena.

"Kasus Penipuan Deepfake AI, Polri Buru Pelaku Pemalsuan Wajah Presiden-Prabowo," Media Indonesia, accessed 14 May 2025, https://mediaindonesia.com/politik-dan-hukum/737308/kasus-penipuan-deepfake-ai-polri-buru-pelaku-pemalsuan-wajah-presiden-prabowo.

47 U.S. Code § 230 (Communications Decency Act, 1996).

Aini, Nurul, and Fauziah Lubis. "Tantangan Pembuktian Dalam Kasus Kejahatan Siber." *Judge: Jurnal Hukum* 5, no. 02 (2024): 55-63.

Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), "APJII: Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang," APJII, accessed 11 May 2025, https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang.

Bakara, Amanda Rich Margareth. "Kerjasama Badan Siber Dan Sandi Negara (Bssn) dan Departement of Foreign Affairs And Trade (DFAT) dalam Meningkatkan Keamanan Siber Indonesia melalui Program Share Information and Best Practice Tahun (2019-2022)." PhD diss., Universitas Pembangunan Nasional Veteran Jakarta, 2024.

California Legislative Information, "AB-730 Elections: Deceptive Audio or Visual Media," 2019.

Citaristi, Ileana. "Organisation For Economic Co-Operation And Development—OECD." In *The Europa Directory of International Organizations 2022*, pp. 694-701. Routledge, 2022.

Citron, Danielle K., and Robert Chesney. "Deepfakes and the new disinformation war." *Foreign Affairs* (2019).

Cyberspace Administration of China, Algorithmic Recommendation Management Provisions (Beijing: CAC, 2022).

Dan Jurafsky and James H. Martin, *Speech and Language Processing*, 3rd ed. (Pearson, 2023), 45.

Denta Putra Azhar and Ahmad Mahyani, "Pertanggungjawaban Pidana Korporasi Sebagai Pelaku Tindak Pidana Penyebaran Data Pribadi," *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance* 3, no. 1 (2023): 540–58.

European Commission, Digital Services Act (Brussels, 2022).

European Parliament and of the Council, *Digital Services Act (Regulation (EU) 2022/2065)* (Brussels: EU Parliament, 2022).

European Parliament and of The Council, Regulation on Artificial Intelligence (AI Act) 2024/1689 (2024).

Goodfellow, Ian J., Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. "Generative adversarial nets." *Advances in neural information processing systems* 27 (2014).

Goodfellow, Ian, Yoshua Bengio, Aaron Courville, and Yoshua Bengio. *Deep learning*. Vol. 1, no. 2. (Cambridge: MIT press, 2016.) 76.

Lukitasari, Diana. "Adopsi Model Pertanggungjawaban Pidana Korporasi Terhadap Malfungsi Penggunaan Artificial Intelligence Di Indonesia." PhD diss., UNS (Sebelas Maret University), 2023.

Mitchell, T. M., *Machine Learning*, vol. 1, no. 9 (New York: McGraw-Hill, 1997), 2.

Nuhi, Muhammad Hanan, Logan Al Ghozi, Syakira Nazla, and Davina Syakirah. "Pembaharuan Hukum Penanganan Tindak Pidana Pemalsuan Identitas Akibat Penyalahgunaan Artificial Intelligence Di Indonesia." *Jurnal Batavia* 1, no. 02 (2024): 80-88.

Personal Data Protection Commission (PDPC) Singapore, Model AI Governance Framework, 2nd ed. (Singapore: IMDA, 2023).

Putra, Akbar Rajendra, and Gialdah Tapiansari Batubara. "Analisis Dampak Penggunaan Ai Terhadap Tindak Pidana Penipuan Online Bagi Masyarakat Di Indonesia." *Jurnal Ilmiah Multidisiplin Terpadu* 8, no. 6 (2024).

Putra, Muh Abduh Dwi. "Pelacakan Pelaku Kejahatan Siber Pengguna Virtual Private Network (Vpn) Pada Jaringan The Onion Router (Tor)(Studi Kasus Di Badan Siber Dan Sandi Negara)." PhD diss., Universitas Airlangga, 2020.

Rahman, Rofi Aulia, and Rizki Habibulah. "The criminal liability of artificial intelligence: is it plausible to Hitherto Indonesian criminal system?." *Legality: Jurnal Ilmiah Hukum* 27, no. 2 (2019): 147-160.

Singapore Statutes Online, Protection from Online Falsehoods and Manipulation Act (POFMA) (2019).

Stuart J. Russell dan Peter Norvig, *Artificial Intelligence: A Modern Approach*, edisi ke-4 (Boston: Pearson, 2016), 3.

Szeliski, Richard. *Computer Vision: Algorithms and Applications* (Springer Nature, 2022), 78.

U.S. Congress, H.R.5586 Deepfake Accountability Act of 2023 (2023).

***

Acknowledgment
None.

Funding Information
None

Conflicting Interest Statement
There is no conflict of interest in the publication of this article.

Publishing Ethical and Originality Statement
All authors declared that this work is original and has never been published in any form and in any media, nor is it under consideration for publication in any journal, and all sources cited in this work refer to the basic standards of scientific citation.

Droíl ne done, pluís que soít demaunde