JICLS
Journal of Ius Comparatum Law Studies
Fakultas Hukum Universitas Pembangunan Nasional "Veteran" Jakarta

Enhancing Digital Security via E-Law Optimisation and Deepfake Regulation: A Comparative Study of China

Widya Tri Lestari[1], Reva Fitri Ramadani[2], Yasinta Diva Negara[3], Fadli Ananda Putra[4]
[1 2 3 4] UPN Veteran Jakarta, Jalan RS. Fatmawati Raya, Jakarta Selatan.
Corresponding email: 2410611200@mahasiswa.upnvj.ac.id

Abstract: *The development of artificial intelligence (AI), especially deepfake technology, presents new challenges in law and digital security. Although initially developed for the creative industry, this technology is often misused to spread false information, defamation, and extortion. Indonesia does not yet have regulations that specifically regulate deepfakes, so law enforcement against their misuse still relies on the Electronic Information and Transactions Law (UU ITE), which does not explicitly cover this technology. This study discusses the urgency of deepfake regulation in Indonesia by analysing the "Deep Synthesis Provisions" policy implemented in China. The results of the analysis show that an adaptive regulatory approach, co-regulation, development of detection technology, increasing digital literacy, and a multistakeholder framework can be solutions in formulating deepfake regulations in Indonesia. Therefore, a revision of the ITE Law is needed to include specific regulations regarding deepfakes, as well as collaboration between the government, technology industry, and society to ensure the responsible and ethical use of AI.*

Keywords *Deepfake, Artificial Intelligence, Regulation, ITE Law, Digital Security*

A. Introduction

The development of digital technology and artificial intelligence (AI) has led to innovations that are changing the way people live. One innovation that is important to note is deepfake, which is digital content that is modified using AI to produce fake images, videos or audio that look very real and convincing. According to a report from DeepTrace Labs, the number of deep fake videos on the internet increased significantly, reaching 330% between June 2019 and July 2020, totalling more than 85,000 videos.[1] This phenomenon has serious implications for society, including the spread of false information, defamation, and potential threats to national security. A survey by the Pew Research Centre revealed that 70% of respondents were concerned that deepfakes could be used to manipulate information and influence the democratic process.[2]

[1] H., Patrini, G., Ajder, L Cullen, and F., Cavalli, "The State of Deepfakes: Landscape, Threats, and Impact.," *DeepTrace Labs.*, 2020.
[2] E. A., Vogels and M Anderson, "Americans' Attitudes Toward AI and Deepfakes," Pew Research Center, 2023.

Deepfake technology has also reached a point of development where its ability to manipulate digital content has become increasingly sophisticated and difficult to detect. Based on a comprehensive study conducted by the Massachusetts Institute of Technology (MIT), the accuracy rate in identifying deepfakes by humans only reaches 65%, indicating significant difficulties in detecting digital manipulation.[3] The urgency of deepfake regulation is based on the various negative impacts that have been identified. A report released by the World Economic Forum classified five main risk categories from deepfakes: the spread of political disinformation, manipulation of financial markets, personal identity fraud, non-consensual pornography, and threats to national security.[4]

In the face of this threat, some countries have taken proactive measures by establishing regulations related to deepfakes. One of them is China, which implemented stricter and more comprehensive rules through the "Regulations on the Administration of Network Audiovisual Information Services" that came into effect on January 1, 2020. This regulation explicitly prohibits the use of deepfake technology without clear markers and requires all content generated or modified using AI to have an indelible digital watermark.[5] It also requires technology platforms to verify the identity of users accessing or using deepfake creation tools, and implements a "publisher responsibility" model where platforms must take responsibility for content uploaded by their users.[6] China's approach reflects a more centralised and strict regulatory model, with a priority on social security and stability over individual freedom of expression.

In Indonesia, there is currently no specific regulation regarding deepfakes. This void means that handling deepfake abuse cases relies on a broad interpretation of existing regulations, such as the Electronic Information and Transaction Law (UU ITE) and the Criminal Code (KUHP).[7] This approach has limitations as these regulations are not specifically designed to deal with the complexities of deepfake technology. The unpreparedness of the legal framework is exacerbated by technological developments that are much faster than conventional legislative processes. According to the Indonesian Internet Service Providers Association (APJII), the number of internet users in Indonesia

[3] Matthew, Harris, Zeke, Hsu, Joshua, & Gerstner, Eric Groh, "Human Detection of Machine-Generated Content: An Experimental Analysis," 2023.
[4] World Economic Forum, "The Global Risks of Deepfakes: Classification and Mitigation Strategies. Geneva," *WEF Digital Trust Initiative*, 2023.
[5] Cyberspace Administration of China, "Regulations on the Administration of Network Audio and Video Information Services.," *People's Republic of China.*, 2022.
[6] Huiyao, & Miao, Lu Wang, "China's Approach to Regulating Deepfakes: Balancing Innovation and Security," *International Journal of Law and Information Technology* 30, no. 3 (2022): 215–34.
[7] A Nugroho, "Tantangan Regulasi Teknologi Deepfake Dalam Sistem Hukum Indonesia," *Jurnal Hukum & Teknologi* 12, no. 1 (2023): 78–95.

will reach 196.7 million by 2023, making Indonesia's digital population highly vulnerable to deepfake abuse without adequate legal protection.[8]

Given the significant potential negative impact of the misuse of deepfake technology and the existing regulatory vacuum, it is important to conduct an in-depth study on the challenges and urgency of establishing deepfake regulations in Indonesia. The absence of a clear legal framework not only jeopardises information integrity and individual privacy but can also threaten social stability and national security. This discussion is especially important given the accelerated adoption of digital technology and AI in Indonesia, while the existing legal and policy infrastructure has not been able to keep up with these developments. Therefore, this research will focus on identifying the need for deepfake regulations and legal strategies that can be applied in the context of the Indonesian legal system by comparing deepfake-related regulations that have been created and implemented in other countries.

B. Method

This research uses a qualitative-comparative method. This method was chosen to enable in-depth analysis of various notions, concepts, theories, adages and principles relevant to the research issue. This comprehensive analysis aims to build a solid and comprehensive theoretical foundation for further research discussions. By comparing and contrasting various perspectives and sources, this research provides a richer understanding and more complete nuances of the issues under study. This research uses the literature study data collection method, which involves an in-depth and comprehensive analysis of various documents and literature related to the research topic. The data sources used are diverse and include various types of documents, including relevant legal documents, such as laws and regulations and court decisions; official letters and correspondence related to the issues under study; previous research reports on similar topics; textbooks and academic references that discuss relevant theories and concepts; government policies related to the issues under study; and published scholarly journals that are relevant to the cases raised in this research. By analysing various perspectives and information from these sources, this research seeks to gain a comprehensive and in-depth understanding of the topic under study.[9]

---

[8] Kementerian Komunikasi dan Informatika, "). Evaluasi Program Literasi Digital Nasional Dan Rekomendasi Pengembangan" (Jakarta, 2023).

[9] Salmaa, "Studi Literatur: Pengertian, Ciri, Teknik Pengumpulan Datanya. ," https://penerbitdeepublish.com/studi-literatur/#1_M_Nazir , 2023.

C. Result & Discussion

1. Optimising the ITE Law in Snaring Deepfake Criminals

The development of artificial intelligence (AI) has brought significant impacts in various aspects of life, including in the digital world. AI enables process automation, increased efficiency, and the development of innovative technologies that were previously unimaginable. One technology that is growing rapidly thanks to AI is deepfake. Deepfake is an artificial intelligence-based technology capable of manipulating images, videos, and sounds to create content that appears real but is fake. This deepfake technology was originally developed for creative industries such as film and entertainment. However, it is often misused in various digital crimes such as defamation, spreading false information, extortion, and sexual exploitation.

The Indonesian legal system does not yet have specific regulations that explicitly regulate deepfakes as a cybercrime. In this condition, the Electronic Information and Transaction Law Number 19 of 2016. (ITE Law) It is the main basis for ensnaring deepfake criminals, even though it is still general and has not specifically accommodated the complexity of this technology.[10] The relationship between deepfake technology and the Electronic Information and Transaction Law (ITE Law) is increasingly important to study, given the potential for misuse that can hurt individuals and society at large.

The ITE Law has several articles that can be used to ensnare perpetrators of deepfake crimes. Article 27, paragraph (3) of the ITE Law is in line to protect individual honour from attacks carried out through electronic media. The use of deepfake to damage someone's reputation can be categorised as an insult or defamation, so it can be subject to the provisions in this article. Furthermore, Article 28 paragraphs (1) and (2) are also relevant in the context of deepfakes being used to spread false news or provocations that can harm society. This article emphasises the prohibition against false information that can mislead the public, an aspect that often occurs in the dissemination of deepfakes.

The weaknesses in the ITE Law regulation in dealing with the misuse of deepfake technology are mainly due to the absence of a regulation that explicitly addresses this technology, creating various obstacles in the law enforcement process. Without a clear definition of deepfake in the existing regulations, law enforcement officers must interpret the available articles to cover this crime.[11] The rapid development of deepfake technology, which is increasingly sophisticated and capable of producing content that is difficult to distinguish from the original, complicates the identification and proof process in the

[10] H., & Astuti, P. Novyanti, "Jerat Hukum Penyalahgunaan Aplikasi Deepfake Ditinjau Dari Hukum Pidana.," *Novum: Jurnal Hukum*, 2021, 31–40.
[11] Rafi Satrya Arvitto, "Implikasi Hukum Deepfake: Telaah Terhadap UU ITE Dan UU PDP," *Jurnal Ilmmu Hukum* 4, no. 2 (2024).

justice system. Limitations in technical aspects and digital forensics are also a major challenge in proving crimes that use deepfakes as the main tool.

In facing legal challenges due to the increasingly complex misuse of deepfake technology, steps are needed to optimise the ITE Law to make it more effective in ensnaring criminals. The government needs to revise the ITE Law to include a clear definition and more specific regulations related to deepfakes. This step is important to provide legal certainty in ensnaring the perpetrators of its misuse and avoiding multiple interpretations in its application. This revision should also include the formulation of strict and proportional sanctions to anticipate various forms of crimes involving deepfakes, both in the realm of defamation, dissemination of false information, sexual exploitation, and extortion.

The next effort that can be made is to expand the specific meaning in Article 1 of the ITE Law, which is considered insufficient in defining AI systems specifically. Therefore, Article 1 can be amended to define AI as an electronic or machine-based system that can perform work that requires human reasoning, such as decision-making and data analysis. Article 40 and Article 43 of the ITE Law could also be reformulated to add a new article to regulate the transparency and accountability obligations of AI providers and developers. Article 40 A, which requires developers to be transparent about algorithms, data sources, and evaluation procedures, also emphasises transparency and the rights of data users. Article 43 A is to authorise the government to supervise developers and managers regarding the process of accountability and transparency, and can impose administrative sanctions if there is abuse.[12]

2. Development Strategy of Deepfake Regulation in Indonesia (Comparative Study with Policy in China)

In Indonesia, cases of deepfake abuse have experienced a significant increase of 145% from 2021 to 2023, based on data from the Ministry of Communication and Information Technology. This makes Indonesian society vulnerable to information manipulation through deepfakes, especially in the context of pre-existing political and social polarisation. A survey conducted by the Indonesian Institute of Sciences (LIPI) of 2,500 respondents revealed that 78% of respondents had difficulty distinguishing original content from deepfakes, and 64% had shared content that was later found to be deepfake manipulation.[13] This data shows the urgency to develop a comprehensive regulatory

[12] A, A Respati, "Reformulasi UU ITE Terhadap Artificial Intelligence Dibandingkan Dengan Uni Eropa Dan China AI Act Regulation," *Jurnal USM Law Review* 7, no. 3 (2024).
[13] Lembaga Ilmu Pengetahuan Indonesia, *Survei Nasional: Pengetahuan Dan Persepsi Masyarakat Indonesia Terhadap Teknologi Deepfake.* (Jakarta: LIPI, 2023).

framework to mitigate the risks and negative impacts of the misuse of deepfake technology in Indonesia.

To take action against the perpetrators of deepfake technology abuse, Indonesia refers to several legal instruments such as Article 35 of Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) and Article 27 paragraph (1) of Law Number 1 of 2024, which is the second revision of the ITE Law, which also has relevance in handling deepfake-related cases. However, the current regulations do not specifically regulate the use of artificial intelligence (AI), especially deepfakes. Therefore, firmer and more comprehensive regulations are needed to address the threats posed by this technology. Such regulations should include not only sanctions for individuals who create and disseminate deepfake content, but also the responsibility of platforms that facilitate its dissemination, as well as strong legal protection for victims.[14]

The misuse of deepfake technology has become a widespread concern, and China is no exception. This concern over AI-generated media in China began to emerge with the availability and increasing popularity of apps that allow users to create their deepfakes. In 2019, an app called ZAO became famous for the "face swap" feature it offered. However, it soon faced controversy over its data collection policies. Although ZAO later made significant changes to its privacy agreement, the public backlash prompted Chinese authorities to first try to regulate deepfakes, even considering a total ban on the technology.

The Cyberspace Administration of China published several articles in the three months following the launch of ZAO discussing the need for regulation of artificial intelligence (AI) and management of its development. This led to the publication of the "Regulations on the Administration of Network Audiovisual Information Services" in November 2019, which came into effect on January 1, 2020. The regulation establishes new rules and responsibilities for providers of audio and video information services, as well as for users of such services. Many media outlets reported that this regulation makes it a criminal offence to publish deepfakes without clear labels, and prohibits the use of deep learning and virtual reality to create fake news.[15] Despite this, the popularity of deepfake videos in China remains high, with the Bilibili platform being one of the main places to share such content.

In January 2022, the Cybercrime Administration of China released a new draft regulation, the "Regulations on the Management of Deep Synthesis for Internet Information Services." Ten months later, the regulation was officially issued and came

---

[14] I., Junaidi, A., & Khaerudin, A. Rohmawati, "Urgensi Regulasi Penyalahgunaan Deepfake Sebagai Perlindungan Hukum Korban Kekerasan Berbasis Gender Online (KBGO," *Innovative: Journal Of Social Science Research* 4, no. 6 (2024): 1779–94.

[15] Respati, "Reformulasi UU ITE Terhadap Artificial Intelligence Dibandingkan Dengan Uni Eropa Dan China AI Act Regulation."

into effect on January 10, 2023. The regulation focuses more on deepfakes by setting specific responsibilities for the management of Deep Synthesis technology and services by internet information service providers, a broader category than audio and visual information service providers. Although deepfakes are one of the main products of this technology, the definition of Deep Synthesis covers more aspects, including technologies that generate text, images, audio, video, virtual environments, and other information using deep learning, virtual reality, and other synthesis algorithms. Therefore, the scope of the regulation includes not only deepfakes but also virtual environments, chatbots, and other AI-based technologies. The regulation focuses on how the technology is used, not just the results produced by the technology.[16]

The Deep Synthesis Terms explicitly set out the primary responsibilities for Deep Synthesis service providers in several key aspects, including:

a. Data Security and Personal Information Protection.
   Deep Synthesis service providers are required to strengthen data management and implement personal information protection measures by applicable regulations, such as the Data Security Act and the Personal Information Protection Act. They must also develop and improve a management system that includes staff training, algorithm evaluation, user registration, data protection, child safety, and personal information protection.
b. Transparency.
   Service providers must establish guidelines and procedures to identify and handle false or damaging information generated using Deep Synthesis technology. They are also required to draft and disclose platform rules and policies, update service agreements, and implement user identity verification systems. In addition, transparency must be supported by mechanisms for reviewing synthetic data, creating databases to detect illegal or false information, and recording relevant network activity logs.
c. Content Management and Labelling
   This provision requires service providers to take steps to prevent the spread of fake news generated by Deep Synthesis technology. If abuse is found, they must delete the content, record it, and report it to the relevant authorities, such as the Internet Information Department. In addition, all information generated by Deep Synthesis technology, such as voice simulation, AI-based conversations, text that imitates a person's style, and image or facial manipulation, must be labelled or identified.

d. Technical Security

[16] Respati. *Loc. Cit.*

> To ensure user security, service providers must conduct regular evaluations of their algorithms and assess security risks before providing models, templates, or tools related to editing faces, voices, and other biometric information. These measures also include supervision of technologies that may affect national security, the country's image, national interests, and the public interest.

The implementation of deepfake regulations in China has shown some indicators of success in combating the misuse of this technology. Based on an evaluation report released by the CAC in 2023, there was an 84% decrease in cases of deepfake distribution that violated regulatory provisions within one year of implementation.[17] Large digital platforms such as Baidu, Alibaba, Tencent, and ByteDance have implemented automatic detection systems that have successfully identified and flagged more than 95% of content generated or modified using AI.[18] Meanwhile, from a law enforcement perspective, China's Ministry of Public Security reported the resolution of 347 criminal cases involving deepfakes in the period 2022-2023, with a prosecution success rate of 92%. This figure is much higher compared to countries that do not yet have specific regulations on deepfakes, including Indonesia. This success is supported by a legal framework that provides a clear definition of violations and specific standards of proof for deepfake cases.

Despite some successes, China's deepfake regulation implementation also faces significant challenges. First, the rapid development of AI technology has made technical standards for detecting and tagging deepfake content quickly obsolete. Research from the China Academy of Information and Communications Technology shows that the latest generation of deepfake technology can penetrate detection systems developed only 12-18 months earlier with a success rate of up to 40%. Second, there are challenges related to the balance between regulation and innovation. Several tech startups in China have reported a 15-25% increase in compliance costs due to the implementation of deepfake regulations, which have the potential to stifle innovation, especially for small and medium-sized companies. This raises concerns that overly stringent regulations could create barriers to entry and strengthen the dominance of large tech companies that have more resources to comply with regulations.

Third, implementation of the regulation faces jurisdictional challenges in the context of cross-border platforms and content. The CAC reported that 38% of deepfake content that violates China's regulations originates from servers outside the country, creating difficulties for law enforcement. Fourth, there are concerns about the potential for abuse of the regulation to restrict freedom of expression and censor political content. The Freedom House report noted several cases where deepfake regulation was used to

[17] Cyberspace Administration of China, "Regulations on the Administration of Network Audio and Video Information Services."
[18] *Ibid.*

crack down on legitimate satirical or politically critical content under the guise of preventing disinformation. These challenges reflect the fundamental dilemmas in regulating digital technologies that can be used for a variety of purposes.

The "Deep Synthesis Provisions" policy, as implemented in China, can be a consideration for Indonesia in implementing more specific regulations related to deepfake technology that is currently being discussed by the public. This regulation prohibits the use of deepfakes in spreading disinformation, requires service providers to add labels to content generated by this technology, and establishes responsibilities in maintaining data security and protecting users' personal information. The absence of clear and specific regulations regarding deepfakes can make it difficult to prosecute perpetrators of AI technology abuse and weaken the deterrent effect on such actions.[19]

Currently, Indonesia does not have a law that specifically regulates deepfakes, which is part of artificial intelligence technology. However, on December 19, 2023, the government, through the Ministry of Communication and Information, issued Circular Letter of the Minister of Communication and Information Number 9 of 2023 concerning the Ethics of Artificial Intelligence. This policy can be the first step in regulating artificial intelligence and can be the basis for more comprehensive regulations in the future. Along with the rapid development of deepfake technology, appropriate regulations not only play a role in protecting the public from its negative impacts but can also encourage responsible and ethical innovation in the development of artificial intelligence.[20]

Based on the analysis of the successes and challenges of deepfake regulation in China, several solutions can be identified for the development of a regulatory framework in Indonesia: first, an adaptive regulatory approach that includes regular evaluation and update mechanisms to keep pace with technological developments. A “regulatory sandbox” model that allows for limited-scale regulatory experimentation before national implementation could be an effective alternative, as has been implemented by the Indonesian Financial Services Authority in the context of financial technology.[21] Second, the implementation of a co-regulation approach involves collaboration between the government, the technology industry, and civil society. The existing Electronic System Operators Forum platform could be expanded to include a specific focus on deepfake

[19] R. S. N., & Nuriyatman, E. (2024). URGENSI PENGATURAN PERLINDUNGAN HUKUM TERHADAP KORBAN DEEPFAKE MELALUI Haida, “URGENSI PENGATURAN PERLINDUNGAN HUKUM TERHADAP KORBAN DEEPFAKE MELALUI ARTFICIAL INTELIGENCE (AI) DARI PERSPEKTIF HUKUM PIDANA INDONESIA.,” *Jurnal Hukum Respublica* 24, no. 1 (2024).

[20] S. M. I., Salsabila, N., & Hosnah, A. U Putri, “Kriminalisasi Penggunaan Deepfake Dalam Tindak Pidana Penipuan Dan Pencemaran Nama Baik: Tantangan Dan Solusi Hukum,” *Jurnal Hukum Legalita* 6, no. 2 (2024): 83–90.

[21] Otoritas Jasa Keuangan, *Framework for Regulatory Sandbox Application in Digital Technology Regulation* (Jakarta: OJK Press, 2022).

content, with an obligation for digital platforms to develop and implement codes of conduct and industry standards under the supervision of regulators.[22]

Third, the development of technological infrastructure that supports content detection and verification. The National Cyber and Crypto Agency can collaborate with universities and industry to develop open-source deepfake detection technology that is available for various digital platforms in Indonesia, such as the Digital Content Provenance model developed by the Coalition for Content Provenance and Authenticity (C2PA).[23] Fourth, a national digital literacy program that focuses on the ability to identify manipulative content. The National Digital Literacy Program, launched by the Ministry of Communication and Informatics, can be expanded with a special module on deepfakes that is tailored to the context and needs of the Indonesian people. Fifth, the development of a multistakeholder framework for deepfake governance involves actors from various sectors. The Indonesian Internet Governance Forum can be a platform for ongoing dialogue on deepfake regulation that balances the needs of security, innovation, and digital rights.

D. Conclusion

The rapid development of artificial intelligence (AI), especially deepfake technology, has had a major impact on the digital world. Although initially developed for the creative industry, deepfakes are now often misused in various digital crimes, such as defamation, spreading false information, and extortion. Existing regulations in Indonesia, especially the ITE Law, do not specifically regulate deepfakes, so there are still obstacles in law enforcement efforts. Therefore, a revision of the ITE Law is needed to include a clearer definition of AI, specific rules regarding deepfakes, and transparency and accountability of AI technology developers. This step aims to provide legal certainty, prevent misuse of technology, and protect the public from the various negative impacts of the misuse of deepfake technology.

The significant increase in cases of deepfake abuse in Indonesia shows the urgency of more specific legal protection and regulation for this technology. Although the ITE Law can be used to ensnare perpetrators, existing regulations do not explicitly regulate deepfakes and artificial intelligence (AI). Case studies from China show that strict, transparent regulations that adapt to technological developments can effectively reduce deepfake abuse. Therefore, Indonesia needs to develop regulations that cover aspects of data security, transparency, content management, and stronger law enforcement. In

[22] Kementerian Komunikasi dan Informatika, "). Evaluasi Program Literasi Digital Nasional Dan Rekomendasi Pengembangan."

[23] Badan Siber dan Sandi Negara, "). Rencana Strategis Pengembangan Teknologi Deteksi Konten Manipulatif 2023-2027. " (Jakarta, 2023).

addition, a multi-stakeholder approach, development of deepfake detection technology, and increasing digital literacy are strategic steps to reduce the negative impacts of deepfakes and ensure responsible and ethical use of AI.

E. References

Ajder, H., Patrini, G., L Cullen, and F. Cavalli. "The State of Deepfakes: Landscape, Threats, and Impact." *DeepTrace Labs.*, 2020.

Badan Siber dan Sandi Negara. "). Rencana Strategis Pengembangan Teknologi Deteksi Konten Manipulatif 2023-2027. ." Jakarta, 2023.

Cyberspace Administration of China. "Regulations on the Administration of Network Audio and Video Information Services." *People's Republic of China*, 2022.

Groh, Matthew, Harris, Zeke, Hsu, Joshua, & Gerstner, Eric. "Human Detection of Machine-Generated Content: An Experimental Analysis," 2023.

Haida, R. S. N., & Nuriyatman, E. (2024). URGENSI PENGATURAN PERLINDUNGAN HUKUM TERHADAP KORBAN DEEPFAKE MELALUI. "URGENSI PENGATURAN PERLINDUNGAN HUKUM TERHADAP KORBAN DEEPFAKE MELALUI ARTFICIAL INTELIGENCE (AI) DARI PERSPEKTIF HUKUM PIDANA INDONESIA." *Jurnal Hukum Respublica* 24, no. 1 (2024).

Kementerian Komunikasi dan Informatika. "). Evaluasi Program Literasi Digital Nasional Dan Rekomendasi Pengembangan." Jakarta, 2023.

Lembaga Ilmu Pengetahuan Indonesia. *Survei Nasional: Pengetahuan Dan Persepsi Masyarakat Indonesia Terhadap Teknologi Deepfake.* Jakarta: LIPI, 2023.

Novyanti, H., & Astuti, P. "Jerat Hukum Penyalahgunaan Aplikasi Deepfake Ditinjau Dari Hukum Pidana." *Novum: Jurnal Hukum*, 2021, 31–40.

Nugroho, A. "Tantangan Regulasi Teknologi Deepfake Dalam Sistem Hukum Indonesia." *Jurnal Hukum & Teknologi* 12, no. 1 (2023): 78–95.

Otoritas Jasa Keuangan. *Framework for Regulatory Sandbox Application in Digital Technology Regulation*. Jakarta: OJK Press, 2022.

Putri, S. M. I., Salsabila, N., & Hosnah, A. U. "Kriminalisasi Penggunaan Deepfake Dalam Tindak Pidana Penipuan Dan Pencemaran Nama Baik: Tantangan Dan Solusi Hukum." *Jurnal Hukum Legalita* 6, no. 2 (2024): 83–90.

Rafi Satrya Arvitto. "Implikasi Hukum Deepfake: Telaah Terhadap UU ITE Dan UU PDP." *Jurnal Ilmmu Hukum* 4, no. 2 (2024).

Respati, A, A. "Reformulasi UU ITE Terhadap Artificial Intelligence Dibandingkan Dengan Uni Eropa Dan China AI Act Regulation." *Jurnal USM Law Review* 7, no. 3 (2024).

Rohmawati, I., Junaidi, A., & Khaerudin, A. "Urgensi Regulasi Penyalahgunaan Deepfake Sebagai Perlindungan Hukum Korban Kekerasan Berbasis Gender Online (KBGO." *Innovative: Journal Of Social Science Research* 4, no. 6 (2024): 1779–94.

Salmaa. "Studi Literatur: Pengertian, Ciri, Teknik Pengumpulan Datanya. ." https://penerbitdeepublish.com/studi-literatur/#1_M_Nazir , 2023.

Vogels, E. A., and M Anderson. "Americans' Attitudes Toward AI and Deepfakes." Pew Research Centre, 2023.

Wang, Huiyao, & Miao, Lu. "China's Approach to Regulating Deepfakes: Balancing Innovation and Security." *International Journal of Law and Information Technology* 30, no. 3 (2022): 215–34.

World Economic Forum. "The Global Risks of Deepfakes: Classification and Mitigation Strategies. Geneva." *WEF Digital Trust Initiative*, 2023.

Author(s) Biography

Widya Tri Lestari is a law student at Universitas Pembangunan Nasional "Veteran" Jakarta.

Reva Fitri Ramadani is a law student at Universitas Pembangunan Nasional "Veteran" Jakarta.

Yasinta Diva Negara is a law student at Universitas Pembangunan Nasional "Veteran" Jakarta.

Fadli Ananda Putra is a law student at Universitas Pembangunan Nasional "Veteran" Jakarta.