E-ISSN : 3088-9928
https://ejournal.stainumadiun.ac.id/index.php/opinia/

Regulation of Deepfakes and Public Expression: Balancing Freedom of Expression and Protection from Disinformation

Muhammad Miftah Irfan[1]
[1]STAI Nahdlatul Ulama Madiun, Indonesia

*Correspondence: *muhammadmiftahirfan@gmail.com*

Abstract

This study examines the regulatory challenges posed by the rapid proliferation of deepfake technology in Indonesia, particularly its impact on public communication, democratic processes, and information integrity. The research aims to analyze the adequacy of Indonesia's current legal framework, primarily the Electronic Information and Transactions Law (ITE Law), the Personal Data Protection Law (PDP Law), and relevant provisions of the Criminal Code, in addressing deepfake-related harms, while evaluating the extent to which these regulations embody the principles of responsive regulation. Using a normative juridical method, this study employs statutory, conceptual, and comparative approaches to scrutinize existing laws and assess their capacity to respond adaptively to emerging technological risks. The findings reveal that although Indonesia possesses several legal instruments that can be applied to deepfake misuse, these regulations remain fragmented, reactive, and insufficiently aligned with the evolving nature of AI-generated disinformation. Analysis using Responsive Regulation Theory indicates that the government's current stance leans predominantly on punitive and deterrence-oriented measures, with limited engagement of collaborative, restorative, and preventive strategies that are essential in addressing complex digital harms. The study concludes that Indonesia requires a more integrated and anticipatory regulatory model, including the development of a lex specialis for AI-generated content, mandatory transparency standards for generative-AI platforms, strengthened digital forensic capacities, and enhanced public digital literacy. Such a framework would enable the law to balance freedom of expression with the need to protect the public sphere from manipulation, ensuring that regulatory responses remain proportionate, flexible, and technologically informed.

Keywords: Artificial Intellegence, Deepfake, Indonesian Regulation

Introduction

The rapid advancement of artificial intelligence (AI) technology, particularly in the domain of generative AI, has given rise to numerous innovations that significantly affect the public information ecosystem. One of the most prominent and problematic phenomena is the emergence of deepfake technology, namely the manipulation of visual or audio content using deep learning models to alter a person's face, voice, or movements so that they appear authentic despite being entirely fabricated. Initially developed within the entertainment and video-editing industries, deepfake technology has, in recent years, evolved into a strategic tool for disseminating disinformation, manipulating public opinion, facilitating digital crimes, enabling image-based abuse, extortion, and political propaganda. As the technical quality of deepfakes becomes increasingly difficult to distinguish from authentic content, this technology poses serious risks to social stability, national security, individual privacy, and the integrity of democratic processes.[1]

In Indonesia, deepfake technology has attracted public attention particularly after entering the spheres of electoral politics as well as religious and social discourse. One of the most widely discussed cases involved a manipulated video depicting the Minister of Finance, Sri Mulyani Indrawati, as if she had stated that “teachers are a burden to the state.” In this video, her voice and facial expressions were altered to appear authentic, despite the statement never having been made. The video caused widespread public outrage, particularly among educators, and triggered extensive disinformation across social media platforms. Although various parties clarified that the video was a deepfake, it continued to circulate virally and resulted in tangible reputational harm. This case demonstrates how deepfake technology can obscure the boundary between fact and falsehood and manipulate public perception within a short period of time.[2]

A similar phenomenon occurred extensively during the 2024 Indonesian Presidential Election, when deepfake videos imitating the voices and faces of political figures were used to influence voter perceptions. Numerous deepfake contents circulated on platforms such as TikTok, Instagram, and Twitter/X, including videos portraying political candidates making statements they had never expressed, as well as highly convincing voice-cloning content.[3] These practices illustrate how deepfake technology has become a strategic instrument in information warfare and computational propaganda capable of shaping political preferences. The misuse of deepfake technology in electoral contexts not only undermines democratic quality but also presents significant challenges for election authorities, law enforcement agencies, and fact-checking institutions, which must operate at a pace far slower than the rapid dissemination of manipulative content.

Beyond politics, deepfake technology has also penetrated the realm of digital sexual exploitation, particularly through the creation of non-consensual pornographic content using ordinary photographs of women. Reports from digital advocacy organizations indicate a significant increase in deepfake pornography cases in Indonesia between 2022 and 2024, facilitated by the accessibility of open-source deepfake tools and AI-based voice cloning services.[4] This phenomenon threatens the safety of women and vulnerable groups and raises

[1] Robert Chesney and Danielle Citron, “Deepfakes and the New Disinformation War,” *Council on Foreign Relations*, Vol. 98:1, (January: 2019), . 145.

[2] Antara, “Kemenkeu: Video Sri Mulyani Bilang Guru Beban Negara Merupakan Hoaks,” https://www.tempo.co/ekonomi/kemenkeu-video-sri-mulyani-bilang-guru-beban-negara-merupakan-hoaks-2060796, akses 18 November 2025.

[3] Gede Arga Adrian, “Deepfake: A Weapon of Mass Deception in the 2024 Election?,” https://www.ums.ac.id/en/news/featured/deepfake-a-weapon-of-mass-deception-in-the-2024-election-, akses 18 November 2025.

[4] Sarah Amanda Uly Sijabat dan Diana Lukitasari, “Konten Gambar dan Video Pornografi Deepfake Sebagai Suatu Bentuk Tindak Pidana Pencemaran Nama Baik,” *Jurnal Recidive: Jurnal Hukum Pidana dan Penanggulangan Kejahatan*, Vol. 13: 2, (Agustus: 2024), . 180.

complex debates regarding moral boundaries, privacy rights, and bodily autonomy in digital spaces.

The increasing prevalence of deepfake technology in Indonesia is exacerbated by relatively low levels of digital literacy, leaving many social media users without the cognitive or technical capacity to verify content. The combination of increasingly sophisticated technology, a hyper-viral information ecosystem, and inadequate regulation creates ideal conditions for AI-driven disinformation. Deepfake technology directly threatens three fundamental aspects:

1. The right to accurate information as a core component of democracy;
2. Freedom of expression, given that overly restrictive regulation risks suppressing artistic creativity and technological innovation;
3. Protection of individual dignity and reputation, including privacy rights, personal data protection, and safeguards against defamation.

The tension among these three aspects creates a complex regulatory dilemma. The state must anticipate the misuse of deepfake technology without imposing excessive censorship that could stifle creativity, freedom of expression, and the development of a national AI ecosystem.

Methodology

This study employs a normative juridical approach that conceptualizes law as a system of norms requiring analysis to address the technological risks posed by deepfake technology to freedom of expression and public protection.[5] This approach is selected because the issue under examination is not merely a social phenomenon but a problem rooted in the gap between rapid advancements in AI-based visual manipulation technologies and the preparedness of legal instruments to respond effectively. The normative juridical method enables the examination of applicable legal rules, legal principles, academic manuscripts, and regulatory frameworks governing technology through analysis of primary legal materials, including the Electronic Information and Transactions Law (Law No. 11 of 2008 as amended by Law No. 19 of 2016), the Personal Data Protection Law (Law No. 27 of 2022), the Copyright Law, the Criminal Code, and subsidiary regulations such as Ministerial Regulations of the Ministry of Communication and Information Technology related to disinformation control. Secondary legal materials include technology law textbooks, international journal articles on AI regulation, and scholarly publications on deepfake technology. Tertiary legal materials encompass legal dictionaries, digital law encyclopedias, and technology regulation indices.

In this study, legal norms are analyzed by focusing on how the existing regulatory framework responds to the emergence of deepfake technology that has become increasingly accessible to the public, as evidenced by several prominent cases in Indonesia. These include a manipulative video depicting the Minister of Finance, Sri Mulyani, as if she had stated that "teachers are a burden to the state,"[1] which was widely interpreted by the public as an authentic

[5] Moh. Mujibur Rohman dkk, "Methodological Reasoning FindsLaw Using Normative Studies (Theory, Approach,and Analysis of Legal Materials)," *Jurnal Maqashidi: Jurnal Hukum Pidana Islam, Perundang-undangan, dan Pranata Sosial*, Vol. 4:2, (Desember:2024), . 204-208.

statement, as well as the widespread circulation of deepfake videos during the 2024 Presidential Election² that triggered an escalation of political disinformation. These phenomena constitute the object of normative inquiry aimed at assessing whether the current legal framework provides sufficient protection or whether a regulatory gap persists. The normative analysis further seeks to identify the legal classification of deepfake practices within existing categories of legal violations such as defamation, violations of privacy, manipulation of personal data, or the dissemination of false information and to evaluate whether these categories are normatively adequate to address the novel risks posed by deepfake technology. In this context, a prescriptive analytical method is employed to formulate recommendations for an ideal regulatory structure grounded in the principles of normative clarity, legal certainty, proportionality, and the precautionary principle in technology regulation.

The primary analytical framework employed in this study is Responsive Regulation Theory, as developed by Ayres and Braithwaite. This theory conceptualizes regulation not as a rigid and repressive instrument, but as a mechanism that must be adaptive to the behavior of various actors—whether individuals, groups, or corporations—and flexible in determining the most effective form of intervention within a given context. The theory is grounded in the premise that regulatory effectiveness depends on the state's capacity to provide a graduated scale of interventions, commonly referred to as the regulatory pyramid, which begins with persuasive, educational, and dialogical approaches and escalates to stringent sanctions only when lower-level responses prove ineffective.[6] In the context of deepfake technology, this theory offers a conceptual framework for assessing whether Indonesia's current regulatory mechanisms exhibit such adaptive and responsive characteristics or instead remain predominantly reactive. Through the lens of responsive regulation, this study evaluates how the law governs the presence of deepfake technology across three principal dimensions: (1) the extent to which regulation is capable of detecting the risks posed by synthetic content; (2) the manner in which the state undertakes adaptive responses through public education, technological transparency obligations, and responsibilities imposed on digital platforms; and (3) how the legal system designs enforcement escalation mechanisms in cases where violations result in serious harm to information integrity or individual rights.[7]

Discussion and Analysis

Discussion

The development of digital manipulation technology has reached a highly advanced stage with the emergence of deepfakes, an artificial intelligence (AI)–based product that enables the creation of visual or audio content that closely and realistically resembles real individuals. This phenomenon did not arise abruptly but is the result of a long historical trajectory rooted in advances in machine learning, computer vision, and generative modeling research. Historically, deepfake technology is grounded in two major developments: first, the

[6] Ian Ayres dan John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate*, (Oxford: Oxford University Press, 1992), . 44.

[7] Melissa Rorie, "Responsive Regulation," dalam *Oxford Handbook Topics in Criminology and Criminal Justice,* (Oxford: Oxford University Press, 2012), . t.th.

advancement of autoencoders in neural network research since the early 2010s; and second, the breakthrough of Generative Adversarial Networks (GANs) introduced by Ian Goodfellow in 2014, which enabled computers to autonomously generate synthetic content with a level of quality approaching reality.[8] GANs, consisting of a generator and a discriminator, provided the foundational architecture for the emergence of face-swapping applications that later became widely known as deepfakes. The year 2017 marked a transformative moment when a Reddit user operating under the username "deepfakes" introduced GAN-based face-swapping techniques to produce pornographic videos featuring the faces of celebrities.[9] Since then, the term "deepfake" has been widely adopted to describe forms of deep learning–based visual manipulation.

Conceptually, deepfakes refer to synthetic media generated by artificial intelligence models through deep learning techniques that enable the accurate reproduction of an individual's facial features, voice, and expressions. Chesney and Citron define deepfakes as "hyper-realistic digital falsifications created through deep learning techniques capable of mimicking real individuals' visual and auditory features."[10] Deepfakes are not merely editing techniques but constitute a form of digital representation capable of blurring the boundary between reality and fabrication. Consequently, their legal implications are highly complex, encompassing issues of privacy rights, information manipulation, defamation, national security, and electoral integrity.

The deepfake phenomenon has developed rapidly on a global scale, particularly within the contexts of politics, entertainment, cybersecurity, and disinformation. During the 2020 and 2024 United States elections, institutions such as the Brookings Institution warned of the potential use of deepfakes to influence public perception through the manipulation of political candidates' visual and auditory representations.[11] In India, reports by The Economic Times documented the use of deepfake technology in political campaigns, where politicians employed this technology to deliver speeches in multiple dialects in order to reach diverse voter groups. In the European Union, concerns over information destabilization prompted the European Commission to adopt the Artificial Intelligence Act (AI Act), which classifies manipulative deepfake-based content as a category of "high-risk AI."[12]

[8] Ian J. Goodfellow dkk, "Generative Adversarial Networks," *Advances in Neural Information Processing Systems*, Vol. 3:11, (June:2014), 1-2.

[9] Britt Paris dan Joan Donovan. *Deepfakes and Cheap Fakes: The Manipulation of Audio and Visual Evidence. Data & Society*, (California: Data & Society's Media Manipulation research initiative, 2019), 10-11.

[10] Bobby Chesney dan Danielle Citron. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, *California Law Review*, Vol. 107:1753 (Desember:2019), 1758.

[11] David Nicholas Allen, Deepfake Fight: AI-Powered Disinformation and Perfidy Under the Geneva Conventions. *Notre Dame Journal on Emerging Technologies*, Vol. 3: 2, (November 2022), T.H.

[12] 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).

The deepfake phenomenon entered Indonesia's public sphere in a significant manner starting in 2020, but reached its peak during the 2024 general election period.[13] One of the most prominent cases involved a manipulative video depicting the Minister of Finance, Sri Mulyani, as if she had stated that "teachers are a burden to the state." This video, produced using lip-sync deepfake techniques, circulated widely on social media before being officially confirmed as false. Other manifestations include videos of various political figures whose faces or voices were altered to convey statements they never made, including videos of presidential candidates presented in inauthentic campaign styles. In addition, cases of non-consensual deepfake pornography targeting numerous women in Indonesia have emerged. These practices have resulted in severe psychological harm and constitute serious violations of the right to privacy.[14]

From a regulatory perspective, Indonesia does not yet have a specific legal framework that explicitly governs deepfake technology. Nevertheless, several existing regulations may serve as a basis for law enforcement. First, the Electronic Information and Transactions Law (ITE Law), Law No. 1 of 2024, regulates prohibitions against the dissemination of false information, defamation, and the manipulation of electronic data. Article 28 paragraph (1) stipulates that "any person who intentionally and/or transmits Electronic Information and/or Electronic Documents containing false notifications or misleading information that result in material losses to consumers in Electronic Transactions" is subject to legal sanctions. Furthermore, Article 28 paragraph (2) provides that "any person who intentionally and without lawful authority distributes and/or transmits Electronic Information and/or Electronic Documents that are inciting, encouraging, or influencing others so as to generate hatred or hostility against individuals and/or certain groups of society based on race, nationality, ethnicity, skin color, religion, belief, gender, mental disability, or physical disability."[15]

Second, the Personal Data Protection Law (PDP Law) provides legal protection against the misuse of an individual's image, facial features, and voice, which constitute biometric data and fall within the category of sensitive personal data.[16] Third, the Copyright Law affords protection against the unauthorized reproduction or redistribution of a person's likeness in the context of creative works, particularly where such use serves commercial purposes or infringes upon the holder's moral rights.[17] Fourth, the Criminal Code may be applied in cases of defamation involving the public display of images, as stipulated in Article 433 paragraphs (1) and (2), which carries a maximum penalty of 1 year 6 months' imprisonment.[18] Fifth, Ministerial Regulations of the Ministry of Communication and Information Technology concerning the handling of negative content provide an administrative basis for the removal of deepfake content from digital platforms.[19] Nevertheless, these regulatory instruments

[13] Gede Arga Adrian, "Deepfake: A Weapon of Mass Deception in the 2024 Election?"

[14] Doni Noviantama dan Alif AlfaniRahman, "Deepfake:A Reviewfrom The Victimology Perspective," *Contemporary Issues In Criminal Law,* Vol.1:2, (Desember: 2024), 123.

[15] "Electronic Information and Transactions Law No. 1 of 2024, Article 28 paragraph (1) dan (2)."

[16] "Personal Data Protection Law No. 27 of 2022."

[17]" Copyright Law No. 28 of 2014."

[18] "Criminal Code No. 1 of 2023."

[19] "Regulation of the Minister of Communication and Information Technology No. 19 of 2014."

collectively constitute a fragmented patchwork and are not fully adaptive to the rapidly evolving and highly elusive characteristics of deepfake technology.

In this context, Indonesia faces serious challenges in the form of substantive legal gaps, inadequate detection mechanisms, the absence of mandatory content labeling requirements, and the lack of enforceable obligations for digital platforms to identify or mark synthetic content. These conditions underscore that Indonesia’s regulatory approach remains predominantly reactive rather than proactive, with law enforcement often initiated only after tangible harm has occurred. Consequently, numerous academic studies and policy analyses have emphasized the necessity of establishing a new legal framework that explicitly governs the identification, production, distribution, and use of deepfake content, including the adoption of co-regulatory approaches involving digital platforms, as has been implemented in the European Union.

Analysis

The deepfake phenomenon, as a product of artificial intelligence–based visual manipulation, has generated highly complex legal challenges for Indonesia, particularly when such synthetic content is used for disinformation, defamation, public deception, or the escalation of political conflict. The existing legal framework—comprising the Electronic Information and Transactions Law and its amendments, the Personal Data Protection Law, the new Criminal Code, and various sectoral regulations—formally provides a legal basis for addressing unlawful conduct related to deepfake technology. However, the effectiveness of these instruments in responding to technological risks is largely determined by the regulatory approach adopted by the government. Accordingly, the application of the Responsive Regulation Theory framework becomes crucial for assessing whether Indonesia’s regulatory regime operates in a proportional, adaptive, and effective manner in confronting the rapidly evolving dynamics of technological development.

Responsive Regulation Theory emphasizes the importance of regulators selecting interventions that are varied and graduated, beginning with educational and persuasive measures, progressing to cooperative mechanisms, and resorting to stringent sanctions only when all preceding approaches have failed. Responsive regulation does not rely solely on the strength of written rules, but rather on the regulator’s capacity to assess the motivations of regulated actors, the level of risk generated by their conduct, and the system’s readiness to implement enforcement escalation. When this theoretical framework is applied to the issue of deepfake technology, it becomes evident that Indonesia remains at an early stage in developing a system capable of governing the synthetic content ecosystem in a progressive and effective manner.

From the perspective of legal substance, the existing legal bases appear theoretically adequate. The Electronic Information and Transactions Law, through its provisions on defamation, the dissemination of false information, manipulation of electronic information, and hate speech, can be applied to prosecute perpetrators who disseminate harmful deepfake content. In addition, the Personal Data Protection Law provides a strong legal foundation, as deepfake practices almost invariably involve the use of biometric data without consent, while the new Criminal Code updates offenses related to defamation and the falsification of electronic documents that are relevant to synthetic video content. Nevertheless, when viewed through the lens of responsive regulation, this normative framework is not yet fully fit for purpose, as no regulation provides an explicit legal definition of deepfake technology. The absence of such a definition generates interpretive uncertainty for law enforcement authorities, the public, and digital platforms alike, thereby hindering the implementation of early-stage regulatory measures such as education, clarification, and the establishment of operational standards. In other words, general legal norms are insufficient to effectively guide persuasive actions, which constitute the foundational layer of the responsive regulatory pyramid.

Beyond issues of legal substance, the existing law enforcement architecture reveals structural limitations that hinder the implementation of a responsive regulatory model. The handling of deepfake-related cases tends to be reactive, as state intervention is typically initiated only after such content has gone viral and generated social unrest. This approach runs counter to the principle of responsiveness, which requires preventive action and proactive risk management prior to the escalation of harm. Furthermore, administrative sanction mechanisms—an essential component of the enforcement pyramid—are rarely optimized in practice. The government tends to resort directly to criminal law instruments, particularly through the ITE Law, despite responsive regulation positioning criminal sanctions as a last resort after persuasive and administrative measures have failed. An enforcement practice that is overly and prematurely oriented toward criminalization risks producing over-criminalization, which may threaten freedom of expression and generate negative deterrent effects on legitimate digital creativity.

Responsive regulation also requires the presence of co-regulation, namely close collaboration among government authorities, digital platforms, academic institutions, and civil society. To date, however, Indonesia has not established a structured co-regulatory mechanism for governing synthetic content. Existing regulations issued by the Ministry of Communication and Information Technology, which require platforms to remove problematic content only after a report has been submitted, do not constitute a preventive oversight framework for deepfake content. There are no proactive obligations imposed on platforms to conduct automated detection, labeling, or watermarking of AI-generated content. Yet, Responsive Regulation Theory emphasizes that effective governance does not rely solely on state law, but also on the capacity of industry actors and social organizations to develop internal compliance norms. In the absence of co-regulatory mechanisms, the government loses the middle-tier layer of the responsive regulatory pyramid, which is essential for preventing escalation toward severe sanctions.

Moreover, Responsive Regulation Theory requires law enforcement authorities to possess adequate technical capacity to ensure that the interventions imposed are genuinely proportional. In the context of deepfake technology, such technical capacity is closely linked to digital forensic capabilities to distinguish between authentic and manipulated videos. This limitation is clearly evident, as Indonesian law enforcement institutions currently lack sufficient multimedia forensic infrastructure. As a result, determining whether administrative intervention is adequate or whether escalation to criminal enforcement is necessary becomes increasingly difficult. When technical evidence is weak or inconclusive, the responsive regulatory model is difficult to implement because there is no objective basis for selecting the appropriate level of sanction.

Based on this analysis, it can be concluded that Indonesia's current regulatory framework has not yet been able to respond to the dynamics and complexity of deepfake technology in a responsive manner. The government continues to rely excessively on reactive criminal law provisions and has not sufficiently developed regulatory instruments that are preventive, educational, and cooperative, as emphasized in Responsive Regulation Theory. This condition indicates the need for more fundamental and carefully planned legal reform to ensure that the regulatory pyramid can function in a comprehensive and effective manner.

It is recommended that the government promptly formulate a lex specialis on deepfake technology that, at a minimum, provides a clear legal definition, classifies synthetic content based on its purpose, imposes labeling or watermarking obligations on AI-generated content, and establishes algorithmic audit mechanisms for large digital platforms. Such provisions would create a foundational regulatory layer capable of encouraging compliance without resorting to excessive criminalization. In addition, the government should develop co-regulatory mechanisms involving digital platforms in the prevention and mitigation of deepfake-related risks, including the strengthening of notice-and-action procedures and the implementation of integrated public reporting systems. Furthermore, the government must invest significant resources in enhancing national digital forensic capabilities to ensure that law enforcement can be conducted in a proportional and evidence-based manner. Moreover, safe harbor provisions should be established to protect parody, artistic, and research-related content in order to safeguard freedom of expression. Collectively, these recommendations not only align with the principles of responsive regulation but also ensure that Indonesia can address technological risks while maintaining a balance between public protection and respect for freedom of expression.

Conclusion

The conclusion of this study indicates that the widespread use of deepfake technology in Indonesia across political, economic, and social contexts has generated significant regulatory challenges for the state, particularly with regard to protecting the public sphere from disinformation and digital manipulation. Analysis based on Responsive Regulation Theory demonstrates that Indonesia's current legal framework, including the Electronic Information and Transactions Law, the Personal Data Protection Law, and several provisions of the Criminal Code, has essentially provided a normative foundation for addressing the misuse of deepfake technology; however, it remains partial, fragmented, and not fully aligned with the growing complexity of technological risks. The government tends to prioritize a deterrence-based approach through the threat of sanctions, while insufficiently integrating responsive regulatory strategies that involve collaboration with industry actors, platform providers, technology communities, and civil society. Accordingly, this study recommends the formulation of specific regulation or a lex specialis concerning digital content integrity and generative AI technology, the implementation of algorithmic audit standards, the enhancement of law enforcement capacity in advanced digital forensics, and the strengthening of public digital literacy as a preventive pillar. Furthermore, cross-sectoral policy harmonization should be prioritized to ensure that Indonesia's regulatory response remains adaptive, proportionate, and capable of maintaining a balance between freedom of expression and the protection of the public from deepfake-based disinformation.

Bibliography

"Regulation of the Minister of Communication and Information Technology No. 19 of 2014." "Personal Data Protection Law No. 27 of 2022."

Allen, D. N. (2022). *Deepfake fight: AI-powered disinformation and perfidy under the Geneva Conventions*. *Notre Dame Journal on Emerging Technologies*, 3(2), t.t.

Antara. (2025). *Kemenkeu: Video Sri Mulyani bilang guru beban negara merupakan hoaks*. Tempo. https://www.tempo.co/ekonomi/kemenkeu-video-sri-mulyani-bilang-guru-beban-negara-merupakan-hoaks-2060796

Ayres, I., & Braithwaite, J. (1992). *Responsive regulation: Transcending the deregulation debate*. Oxford University Press.

Chesney, R., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107, 1753–1819.

Chesney, R., & Citron, D. (2019). Deepfakes and the new disinformation war. *Council on Foreign Relations*, 98(1), 145.

"Copyright Law No. 28 of 2014."

"Criminal Code No. 1 of 2023."

"Electronic Information and Transactions Law No. 1 of 2024."

European Parliament & Council of the European Union. (2024). *Regulation (EU) 2024/1689 ... (Artificial Intelligence Act)*.

Goodfellow, I. J., et al. (2014). Generative adversarial networks. *Advances in Neural Information Processing Systems*, 3(11), 1–2.

Noviantama, D., & Rahman, A. A. (2024). Deepfake: A review from the victimology perspective. *Contemporary Issues in Criminal Law*, 1(2), 123.

Paris, B., & Donovan, J. (2019). *Deepfakes and cheap fakes: The manipulation of audio and visual evidence*. Data & Society.

Rain, P. (2024). *Year of elections: Lessons from India's fight against AI-generated misinformation*. World Economic Forum. https://www.weforum.org/stories/2024/08/deepfakes-india-tackling-ai-generated-misinformation-elections/

Rohman, M. M., et al. (2024). Methodological reasoning finds law using normative studies (theory, approach, and analysis of legal materials). *Jurnal Maqashidi: Jurnal Hukum Pidana Islam, Perundang-undangan, dan Pranata Sosial*, 4(2), 204–208.

Sijabat, S. A. U., & Lukitasari, D. (2024). Konten gambar dan video pornografi deepfake sebagai suatu bentuk tindak pidana pencemaran nama baik. *Jurnal Recidive: Jurnal Hukum Pidana dan Penanggulangan Kejahatan*, 13(2), 180.

Uly Sijabat, S. A., & Lukitasari, D. (2024). Konten gambar dan video pornografi deepfake sebagai suatu bentuk tindak pidana pencemaran nama baik. *Jurnal Recidive*, 13(2), 180.

Universitas Muhammadiyah Surakarta. (2025). Adrian, G. A. *Deepfake: A weapon of mass deception in the 2024 election?* https://www.ums.ac.id/en/news/featured/deepfake-a-weapon-of-mass-deception-in-the-2024-election-