Journal OF CONSTITUTIONAL LAW SOCIETY
E-ISSN: 2829 - 5014

CRIMINALIZATION POLICY OF DEEPFAKE IN INDONESIAN ELECTIONS

KEBIJAKAN KRIMINALISASI DEEPFAKE DALAM PEMILU INDONESIA

Rachmat Irvan[1*], Junet Hariyo Setiawan[2]
[1*] Atma Jaya Catholic University of Indonesia
[2] Faculty of Law, MPU Tantular University, Jakarta, Indonesia
* irvrachmat@gmail.com

Volume 5, Number 1, March 2026
Received: August 8, 2025 Accepted: August 8, 2025 Online Published: March 27, 2026

ABSTRACT
Technological engineering in the form of artificial intelligence (AI), particularly through deepfake content, has given rise to new forms of cybercrime that are complex and multidimensional. However, Indonesia's positive law has yet to specifically regulate this phenomenon, resulting in legal uncertainty. This study aims to examine the effectiveness of existing regulations and to formulate an ideal criminalization policy. It employs normative juridical research with statutory and conceptual approaches. The main findings reveal that regulations such as the Electronic Information and Transactions Law (UU ITE) and the Personal Data Protection Law (UU PDP) are reactive in nature and do not provide a technical definition of deepfake. This absence complicates digital forensic evidence and law enforcement, further exacerbated by structural weaknesses such as poor inter-agency coordination and low levels of digital literacy among the public. The scientific contribution of this article lies in its proposal for a multidimensional regulatory strategy that not only focuses on legal reform through the formulation of new criminal provisions, but also integrates the strengthening of forensic technology and the enhancement of digital literacy as preventive instruments within criminal law policy.

Keywords : Authority, Deepfake, Election Regulations, Digital Disinformation, Artificial Intelligence (AI).

ABSTRAK

Rekayasa teknologi berupa kecerdasan buatan (AI) melalui konten deepfake telah melahirkan kejahatan siber baru yang bersifat kompleks dan multidimensional, namun hukum positif di Indonesia belum secara spesifik mengatur fenomena ini sehingga menimbulkan ketidakpastian hukum. Penelitian ini bertujuan untuk mengkaji efektivitas regulasi yang ada serta merumuskan kebijakan kriminalisasi yang ideal. Penelitian ini merupakan penelitian yuridis normatif dengan pendekatan perundang-undangan dan pendekatan konseptual. Temuan utama menunjukkan bahwa regulasi seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Pelindungan Data Pribadi (UU PDP) bersifat reaktif dan tidak memuat definisi teknis deepfake. Hal ini menyulitkan pembuktian forensik digital dan penegakan hukum, diperparah dengan kelemahan struktural seperti koordinasi antarlembaga yang lemah dan rendahnya literasi digital masyarakat. Kontribusi ilmiah artikel ini terletak pada tawaran strategi regulasi multidimensional yang tidak hanya fokus pada reformasi hukum melalui perumusan delik baru, tetapi juga mengintegrasikan penguatan teknologi forensik dan peningkatan literasi digital sebagai instrumen preventif dalam kebijakan hukum pidana.

Kata Kunci : Kewenangan, Deepfake, Regulasi Pemilu, Disinformasi Digital, Kecerdasan Buatan (AI).

I. INTRODUCTION

The digital revolution triggered by the exponential development of artificial intelligence (AI) technology over the past two decades has created a fundamental disruption in various aspects of human life, including in the political order and modern democratic systems.(Kushariyadi et al., 2024, p. 74) One of the most alarming developments in this digital technology domain is the emergence of deepfake technology, which uses Generative Adversarial Networks (GANs) a machine learning system consisting of two competing neural networks to produce fake audiovisual content with an unprecedented level of realism.(Oza et al., 2024) This technology was initially developed for positive purposes in various fields such as the entertainment industry, education, and medical research,(Sharma et al., 2024) but its development has experienced a distortion of function into an information weapon that is highly effective in manipulating public opinion and damaging the democratic process.

In the context of elections as the main pillar of modern democratic systems, the misuse of deepfake technology has evolved into an existential threat capable of undermining the fundamental foundations of the democratic

process, particularly the principles of information transparency and the freedom to choose based on accurate facts.(Anand et al., 2024, p. 263) The ability of deepfake technology to create nearly perfect fake content both visually and audibly has opened new opportunities for irresponsible political actors to create fictitious political narratives that can massively mislead the public. Even more concerning, the development of this technology is occurring at a pace far exceeding the adaptive capacity of existing legal and regulatory systems, creating a dangerous regulatory gap for the sustainability of digital democracy.(Noerman & Ibrahim, 2024)

From the perspective of Habermas' deliberative democracy theory, the quality of a democratic process greatly depends on the availability of a healthy public sphere where the exchange of information and political argumentation can take place honestly, transparently, and based on facts.(Hakim, 2025, p. 163) Deepfake, with its extraordinary capacity to create alternative realities that are difficult to distinguish from the truth, fundamentally threatens these basic principles. Furthermore, propaganda theory explains how digital information is used to shape public opinion systematically.(Khaeron, 2021, p. 358) This phenomenon is further exacerbated by the characteristics of contemporary social media that tend to prioritize sensational content without in-depth verification, creating a perfect storm for the spread of destructive deepfakes.

The Electronic Information and Transactions Law (Law No. 11 of 2008, commonly referred to as UU ITE), which serves as the primary legal basis for regulating cybercrime, has undergone significant amendments, most recently through Law No. 1 of 2024. These revisions have increased criminal sanctions and expanded the scope of prohibited acts, including provisions on the distribution of electronic information containing obscene content (Article 27 paragraph 1) and the manipulation of electronic information (Article 35 in conjunction with Article 51 paragraph 1).[1]

Nevertheless, the latest amendments have not explicitly accommodated the technical characteristics of deepfakes as AI-based crimes, thereby creating a legal vacuum in the qualification of specific criminal offenses.[2] Comparative studies indicate that conventional regulations addressing hoaxes and fraud remain insufficient to confront the challenges posed by

[1] Article 28F of the 1945 Constitution states: "Everyone has the right to communicate and to obtain information for the development of themselves and their social environment, as well as the right to seek, acquire, possess, store, process, and convey information by utilizing all available channels."

[2] Article 28 Paragraph 1 of the Electronic Information and Transactions Law (UU ITE) states: "Any person who intentionally and without authorization disseminates false and misleading information causing harm to consumers in electronic transactions may be subject to imprisonment for up to six years and/or a maximum fine of IDR 1 billion."

political deepfakes.[3] Research conducted by the Brennan Center for Justice demonstrates how deepfakes have been deployed to manipulate public opinion during elections, while existing regulations have proven inadequate to fully address this threat (Weiner & Norden, 2023). Furthermore, research in Indonesia also confirms the absence of specific regulations that comprehensively govern deepfakes.(Rohmawati et al., 2024)

Empirically, the impact of deepfake misuse in elections has become clearly visible in various parts of the world and is forming an alarming pattern. In the United States (US) elections, political advertisements emerged using deepfakes to depict doomsday scenarios if President Joe Biden were re-elected, including China's invasion of Taiwan and waves of immigrants to the US.(Antara, 2024a) Ahead of the 2024 Election, a deepfake video circulated showing a presidential candidate speaking fluently in Arabic, although the video had been manipulated using AI.(Antara, 2024a)

Research data from Luminate and Ipsos shows that 75% of respondents in Indonesia believe that AI-generated content can influence public political views, while 42% of them admit they are unsure whether they can distinguish between original content and AI-generated content.(LuminateGroup, 2024) These findings indicate the vulnerability of Indonesia's democratic system to increasingly sophisticated digital manipulation threats.

Deepfake is becoming an increasingly serious threat in Indonesian elections due to interconnected technical, regulatory, and socio-cultural aspects. Deepfake technology is developing rapidly, while detection capacity remains limited. Regulations have yet to specifically address its misuse, making legal classification and enforcement of sanctions difficult. On the other hand, low digital literacy among the public reinforces the impact of information manipulation on social media. The legal and public policy urgency in addressing deepfakes includes improving digital literacy, monitoring digital platforms, and developing detection technology. Without appropriate strategic steps, the misuse of deepfakes could further damage the integrity of democracy and public trust in information.

Although several previous studies have examined the issue of deepfakes in Indonesia, significant gaps remain unaddressed. For instance, Nurkholisah et al (2025) analyzed the criminalization of deepfakes in Indonesian criminal law through an integrative approach combining the UU ITE, the Personal Data Protection Law (UU PDP), the Criminal Code (KUHP), and judicial decisions. However, their study was general in scope and did not specifically target the electoral context. Similarly, Rahman & Anggriawan (2025) conducted a comparative study of deepfake legal frameworks in Indonesia, India, Pakistan, and the United States, but their analysis merely highlighted regulatory gaps

[3] Article 520 of Law Number 7 of 2017 concerning Elections regulates sanctions for anyone who intentionally creates or uses forged documents in the election process, with a penalty of imprisonment for up to 6 years and a maximum fine of IDR 72 million.

without offering multidimensional and applicable strategies. Saragih & Kholiq (2024), on the other hand, limited their research to deepfake pornography, thereby excluding electoral crime aspects. Other studies, such as those by Meliana (2025) and Dharmayanti & Soponyono (2025), remain general and have yet to integrate digital forensic analysis and public literacy as part of legal solutions.

This study offers scientific novelty that distinguishes it from prior research through three layers of contribution. First, it specifically examines deepfakes in the electoral context by analyzing the elements of criminal offenses following the latest amendments to the UU ITE under Law No. 1 of 2024, a subject that has not been extensively explored in Indonesian legal literature. Second, unlike purely normative approaches, this research expands its analysis to include technical aspects of digital forensics and the limited capacity of law enforcement in verifying AI-based content, thereby bridging the gap between law and technology. Third, rather than merely identifying legal vacuums, this study proposes a multidimensional regulatory strategy that simultaneously integrates three pillars: legal reform through the formulation of new offenses that comply with the principle of lex certa, the strengthening of accessible and affordable forensic technology, and the enhancement of public digital literacy as a preventive instrument within a unified theoretical framework. Through this holistic approach, the study contributes to the development of criminal law policy that is adaptive to the challenges of the digital era.

Based on an in-depth analysis of the existing conditions, this study aims to answer two main questions: (1) To what extent is the effectiveness of existing regulations in preventing the misuse of deepfake technology in elections in Indonesia? and (2) What regulatory and public policy strategies are needed to address the legal gap in facing the misuse of deepfake technology in elections in Indonesia? This study not only seeks to identify weaknesses in the existing system but also to design implementable solutions by considering the relevant technical, legal, and social aspects. With a holistic approach, it is hoped that the resulting policy recommendations will not only be able to respond to current challenges but also have anticipatory power against future technological developments.

II. METHOD

The research method used in this study is a normative juridical and empirical juridical approach.(Juliardi et al., 2023, p. 241) The normative juridical approach is used to examine relevant legislation such as the 1945 Constitution, the ITE Law, the Election Law, and regulations related to data protection and digital information in the context of deepfake technology misuse. The analysis is conducted on legal principles, constitutional principles, and normative gaps related to regulatory challenges against

deepfake technology. Meanwhile, the empirical juridical approach is carried out by analyzing secondary data from surveys, research institute reports, case studies of deepfake misuse in elections in various countries, as well as limited interviews with legal experts, election organizers, and information technology practitioners. The combination of these two approaches enables a comprehensive legal review, both theoretically and applicatively, in order to formulate regulatory strategies and law enforcement that are effective and responsive to the development of digital technology.

III. ANALYSIS AND DISCUSSION

a. Effectiveness of Existing Regulations in Preventing the Misuse of Deepfake

The development of artificial intelligence (AI) technology has produced increasingly complex digital innovations, one of which is deepfake. This technology allows the manipulation of voice, images, and videos to resemble certain individuals without authenticity.(Herdian & Sumarwan, 2025) In the context of elections, deepfake has great potential in spreading disinformation, creating false narratives, and systematically damaging the reputation of candidates.(Santiko & Bahri, 2024) Although various regulations have been implemented in the Indonesian legal system to address digital information manipulation, the effectiveness of these regulations still faces significant challenges in tackling the misuse of deepfake.

Normatively, several regulations in Indonesia are currently considered applicable to address the impact of deepfake in elections, including the 1945 Constitution of the Republic of Indonesia Article 28F, which grants every citizen the right to obtain and disseminate information through various communication channels.[4] Article 28F of the 1945 Constitution guarantees the freedom to obtain and disseminate information, but it does not contain explicit provisions related to digital manipulation such as deepfake in elections. Deepfake has the potential to be used to spread disinformation, damage the reputation of candidates, and dishonestly influence public opinion. Without specific regulations, perpetrators can exploit legal loopholes to create false narratives that disrupt democratic integrity (Sisephaputra et al., 2024, p. 214). Therefore, additional policies are needed to firmly regulate the detection, labeling, and sanctions against the use of deepfake in the context of elections.

The Electronic Information and Transactions Law (Law No. 11 of 2008, UU ITE), which has undergone significant amendments, most recently through Law No. 1 of 2024, prohibits the dissemination of false information.

[4] Article 28F of the 1945 Constitution of the Republic of Indonesia states: "Everyone has the right to communicate and obtain information for the development of themselves and their social environment, as well as the right to seek, acquire, possess, store, process, and convey information by utilizing all available channels."

Article 27 paragraph (3) of the UU ITE prohibits the distribution of electronic information containing defamation or insult, while Article 28 paragraph (1) prohibits the dissemination of false news that harms consumers. Article 28 paragraph (2) further strengthens regulatory aspects by prohibiting the dissemination of information intended to incite hatred based on ethnicity, religion, race, or inter-group relations (SARA) (Kumalasari, 2020). Most importantly, Article 35 in conjunction with Article 51 paragraph (1) of the UU ITE specifically prohibits the manipulation, creation, alteration, or deletion of electronic information with the intent that it be perceived as authentic data, carrying criminal sanctions of up to 12 years' imprisonment and fines of up to IDR 12 billion (Marpaung, 2022). In the electoral context, the Election Law (Law No. 7 of 2017) also prohibits hate-based and black campaign practices under Article 280 paragraph (1) (Ali et al., 2025), as well as the provision of material inducements to voters as stipulated in Article 523 paragraphs (1) and (2). Although these regulations are relevant in controlling digital information, a legal vacuum persists because no provision explicitly addresses deepfakes or AI-based digital manipulation as criminal offenses.

From the perspective of criminal elements analysis, Article 35 in conjunction with Article 51 paragraph (1) of the UU ITE is the most potentially applicable provision against deepfakes. The element of "manipulation" in this article, in a teleological sense, encompasses actions such as altering a person's face, voice, or identity using AI technology. However, challenges arise in proving the element of intent (mens rea). A crucial question in law enforcement is whether the creator of deepfake content must have precise knowledge that their AI-generated edits would be used for black campaigns or to influence electoral outcomes, or whether intent can be sufficiently established by the act of producing and disseminating manipulative content without the consent of the data subject. Research by Nurkholisah et al. (2025) suggests that the qualification of deepfake-related offenses is more appropriately approached through the lens of cybercrime rather than conventional crime, given the locus and characteristics of deepfake content dissemination. In addition, Article 28 paragraph (1) of the UU ITE concerning false news dissemination is also relevant, though the element of "false news" must be interpreted broadly to encompass content that appears visually authentic but is factually false—precisely the defining characteristic of deepfakes.

From the perspective of legal theory, Hans Kelsen through the Pure Theory of Law emphasizes that law must be normative and systematic to accommodate social changes.(Aprita, 2024, p. 57) When new phenomena such as deepfake emerge and are not yet covered by existing legal norms, regulatory updates are needed to ensure that the norms remain relevant and can address contemporary challenges. On the other hand, the Responsive Law Theory proposed by Nonet and Selznick states that an effective legal system

must be adaptive to societal changes.(Soepadmo, 2020, p. 28) The law not only serves to maintain order but must also be able to respond to new challenges arising from technological developments. In this context, deepfake regulation in Indonesian elections does not fully reflect the principles of responsive law because there are no explicit rules directly addressing the misuse of this technology.

The weaknesses of existing regulations in addressing the misuse of deepfake in elections can be identified in several key aspects. First, the substantive legal vacuum in legislation causes ambiguity in law enforcement.(Novyanti & Astuti, 2021) The principle of *nullum crimen sine lege* in criminal law states that there is no crime without a legal provision that explicitly regulates it.(Kelsen, 2019, p. 128) The absence of rules specifically governing deepfake creates legal uncertainty, making it difficult for law enforcement officers to take action against perpetrators of deepfake distribution in the context of elections. This phenomenon indicates the existence of a legal gap that requires the formation of new rules or revisions to existing regulations.

Second, there is ambiguity in identifying deepfake perpetrators.(Nabhila, 2024) Deepfake technology is often uploaded anonymously through various digital platforms operating across countries, making it difficult to trace based on IP addresses, metadata, or digital fingerprints.(Faathurrahman & Priowirjanto, 2022) In the public policy theory based on *evidence-based policy*, effective policymaking must be based on accurate data and facts.(Djafar, 2024, p. 60) Therefore, digital forensic and cyber intelligence systems must be strengthened to support more accurate perpetrator identification processes. Without these mechanisms, the law is difficult to apply effectively to the distribution of deepfake in elections.

Third, the current regulations do not provide firm provisions regarding the responsibility of digital platforms in handling the spread of deepfake.(Noerman & Ibrahim, 2024) To date, there are no legal rules in Indonesia that specifically require platforms such as YouTube, TikTok, or Facebook to filter or address the spread of deepfake content. In fact, in the *co-regulation* approach, effective regulation requires collaboration between the government and private actors, including digital platforms, to ensure cybersecurity. For comparison, Germany has implemented the NetzDG Law which requires digital platforms to remove illegal content within 24 hours after being reported.(Hukumu et al., 2025) Without similar regulations, Indonesia finds it difficult to enforce collective accountability in the digital ecosystem.

Fourth, inter-agency coordination in handling deepfake remains weak.(Wibowo & Munawar, 2024) Supervision and law enforcement against the spread of deepfake in elections should be carried out through synergy between the Ministry of Communication and Information Technology

(Kominfo), the General Election Supervisory Agency (Bawaslu), the Police, and the National Cyber and Crypto Agency (BSSN). However, inter-agency coordination is still sectoral and tends to be reactive rather than strategic and preventive.(Wibowo & Munawar, 2024) In the theory of *Good Governance*, one of the main pillars of public policy effectiveness is coordination and cooperation among institutions.(Budiyanto, 2023, p. 30) Without strong coordination, existing regulations cannot be implemented optimally.

Fifth, the low level of digital literacy among the public is a major challenge in dealing with the spread of deepfake.(Prayoga & Tuasikal, 2025) Based on the Luminate–Ipsos (2023) survey, around 42% of Indonesians cannot distinguish authentic content from AI-manipulated content.(LuminateGroup, 2024) This lack of digital literacy increases the risk of spreading visually based hoaxes that are difficult to verify conventionally by the public. In the *advocacy coalition framework* of public policy theory, policy actors need to collaborate with civil society groups and the media in building public education that can enhance the public's critical capacity against AI-based disinformation.(Sabatier & Weible, 2019) Without improvements in digital literacy, the public will become increasingly vulnerable to visual manipulation carried out through deepfake technology.

In the 2024 election in Indonesia, several cases of deepfake misuse have been found to spread false narratives that harm certain candidates. One concrete example is a video showing a political figure making a statement that he never actually made. This video was widely circulated on social media ahead of the presidential and vice-presidential debate and sparked public controversy.(Antara, 2024a) The General Election Supervisory Agency (Bawaslu) also reported a drastic increase in the spread of visually based hoaxes that are difficult to verify conventionally.

Based on reports from Bawaslu and the Indonesian Anti-Slander Society (MAFINDO), during the campaign period there was a surge of up to 370% in the spread of visual hoaxes strongly suspected to be based on deepfake and AI editing tools.(Antara, 2024b) Meanwhile, the phenomenon of deepfake in elections has also occurred in several other countries such as India, Nigeria, and the United States, indicating that deepfake is becoming a global trend in electoral disinformation. Thus, existing regulations in Indonesia have not been fully effective in addressing this challenge, particularly due to the absence of specific rules and the weakness of the existing law enforcement system.

b. Deepfake in Elections: Regulatory Challenges, Interpretative Strategies, and New Criminalization Policies

In the ever-advancing digital era, deepfake technology which enables the creation of highly realistic fake videos, audio, or images poses a serious threat to the integrity of democratic processes, particularly elections in Indonesia.

This technology opens opportunities for misuse that can erode public trust in institutions and manipulate voter opinion on a massive and covert scale.(Oza et al., 2024) However, current legal regulations in Indonesia, including the Electronic Information and Transactions Law (ITE Law) and the Election Law, do not explicitly address the dissemination of deepfake content. This creates a legal gap that allows perpetrators to exploit loopholes for certain political gains. Therefore, comprehensive and adaptive regulatory strategies and public policies based on modern legal and policy principles are required to tackle this challenge.

1) Systematic and Extensive Interpretation of Existing Norms

To overcome the limitations of norms within the ITE Law, a systematic interpretation is required, connecting various laws and regulations in an integrated manner. First, the connection with Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) becomes highly significant. A person's face, voice, and biometric identity constitute specific personal data strictly protected by the PDP Law. The use of biometric data to create deepfake content without the consent of the data subject constitutes unlawful processing of personal data, subject to criminal sanctions as regulated in Articles 65 and 66 of the PDP Law, with a maximum imprisonment of 6 years and/or a maximum fine of IDR 6 billion. Rosnidar et al (2017) assert that the right to privacy is a constitutional right and a human right recognized in Article 28G paragraph (1) of the 1945 Constitution, as well as in the Universal Declaration of Human Rights 1948 and the International Covenant on Civil and Political Rights. Thus, the protection of personal data from deepfake misuse is not merely a technical legal issue but is also related to the fulfillment of citizens' human rights.

Second, with the enactment of Law Number 1 of 2023 concerning the Criminal Code (KUHP) effective January 2, 2026, the provisions on fraud in Article 492 can have their meaning extended to encompass deepfake. This article stipulates that anyone who, with the intent to unlawfully benefit themselves or another person, by using a false name or false status, through trickery, or a series of lies, induces another person to surrender an object, incur a debt, or cancel a receivable, is threatened with fraud, facing a maximum imprisonment of 4 years or a maximum fine of Category V (Rohmawati et al., 2024). The use of deepfake technology to convince voters to support a particular candidate based on false information can be qualified as "trickery" or a "series of lies," which are elements of the fraud offense. Rahman & Anggriawan (2025), in their comparative study, found that Indonesia, India, and Pakistan still rely on general provisions of cyber law and criminal law, while the United States has adopted a more proactive approach with legislation at the state level that specifically criminalizes deepfake-based election interference.

Third, an extensive interpretation can be applied to Article 27A of the ITE Law concerning defamation, where deepfake content that places a candidate in a humiliating or defamatory situation can be broadly interpreted as "accusing someone of something" even though the content is entirely a product of digital manipulation (Apriola, 2021). The Constitutional Court, through Decision Number 166/PUU-XXI/2023, provided an important breakthrough by interpreting the phrase "self-image" in Article 1 point 35 of the Election Law. The Constitutional Court requires election participants to display photos/images of themselves that are original, up-to-date, and not excessively engineered/manipulated with the help of AI. This decision serves as a strong constitutional foundation to encourage further regulation regarding the use of AI in election campaigns, including the prohibition of manipulative deepfake (Herdian & Sumarwan, 2025).

2) The Possibility of New Criminalization from a Criminal Policy Perspective

Based on the weaknesses identified in the analysis above, the perspective of criminal policy points towards the need for new, specific criminalization (delictum speciale) to address the challenge of deepfake in elections. Deepfake possesses unique characteristics not accommodated by conventional offenses: ease of mass production, a high level of realism making it difficult to distinguish from authentic content, the potential for very wide-ranging victims, and the ability to shape public opinion and disrupt socio-political stability on an unprecedented scale. The Chairman of the General Election Supervisory Agency (Bawaslu), Rahmat Bagja, has warned that deepfake can endanger election participants because engineered content shapes public opinion about a person, and an image that has already been formed is difficult to erase even if the person is later proven innocent (Rezky, 2025).

From the perspective of the legality principle (lex certa), formulating a technical definition of deepfake in legislation is an urgent necessity to fulfill the element of legal certainty. Nurkholisah et al (2025) assert that current regulations remain reactive, lack a technical definition of deepfake, and fail to meet the principles of legal certainty, preventive and repressive protection functions, proportionality of sanctions, and the balance between freedom of expression and privacy protection. Bagja encourages that regulations concerning artificial intelligence and its development be accommodated in the revision of Law Number 7 of 2017 concerning Elections currently underway in parliament, as well as the need for the issuance of Government Regulations and KPU Regulations that specifically govern the use of AI and deepfake in elections (Novyanti & Astuti, 2021).

New criminalization must be formulated with an integrated approach that encompasses not only substantive aspects but also procedural and institutional aspects. This includes harmonization between laws (ITE Law, PDP Law, Election Law, and the new Criminal Code), strengthening the

capacity of law enforcement officials in verifying AI-based content, and developing affordable and accessible digital forensic technology for the wider community (Diati & Triadi, 2025). At the international level, the European Union has enacted the AI Act which mandates transparency for synthetic content, while the United States has the DEEPFAKES Accountability Act at the federal level and various legislations at the state level that specifically criminalize deepfake for election interference. The comparative study by (Rahman & Anggriawan, 2025) recommends the need for a more comprehensive legal framework to mitigate the risks of deepfake in the electoral process and ensure democratic integrity. Indonesia can adopt best practices from various countries while adapting them to the national legal, social, and cultural context.

3) Multidimensional Regulatory Strategy

First, from a regulatory perspective, establishing specific rules regarding deepfake technology in the electoral context is crucial. The principle of legal certainty as proposed by Hans Kelsen emphasizes that the law must be clear and firm to provide protection and justice for all parties (Rato, 2021, p. 111). In this context, regulation must explicitly define what constitutes a deepfake and limit its use in political campaigns and electoral processes. Such regulation should set strict boundaries prohibiting the dissemination of manipulative content that can damage a candidate's reputation or manipulate election outcomes.

Moreover, the regulation must provide for sanctions that consider not only the actus reus (the actual act of dissemination) but also the mens rea (malicious intent), ensuring the enforcement of law is fair and effective. Haidarrani et al (2024) applying mens rea is important to distinguish between deepfake users who intentionally deceive the public and those who may unknowingly share such content. This aligns with legal responsibility theories that prioritize intent as a critical element in determining the severity of a crime (Mardani, 2024).

Furthermore, practical reporting and detection mechanisms must be established so that the public can actively participate in identifying and reporting deepfake content. Flexible regulation is essential to keep pace with the rapidly evolving field of artificial intelligence, without stifling digital innovation. Rigid regulation that fails to respond to technological change may become a new barrier to law enforcement. Wijaya (2021) Hence, an adaptive regulatory approach based on the principle of smart regulation should be adopted combining formal rules with technology-based monitoring and public participation.

Second, in terms of law enforcement, it is essential to enhance the capacity of officers through the use of advanced digital forensic and cyber intelligence technologies. The Rule of Law principle articulated by A.V. Dicey demands the fair, transparent, and non-discriminatory application of the law.

Rumiartha (2022) However, the main challenge in enforcing laws against deepfake dissemination lies in perpetrators who often operate anonymously using foreign servers and hard-to-trace encryption technology (Mahdi et al., 2023). Therefore, the deployment of digital forensic tools capable of automatically detecting content manipulation is imperative. AI and machine learning technologies can be used to identify patterns in video, audio, and digital metadata that indicate deepfake engineering (Situmeang et al., 2024).

The utilization of blockchain technology also offers an innovative solution, serving as a content-source tracking tool due to its immutable nature, thereby ensuring transparency and traceability. This aligns with the law and technology approach, which integrates the development of cutting-edge technologies into law enforcement systems to ensure their effectiveness in facing contemporary challenges (Andriyani et al., 2023, p. 52). This effort must be supported by strengthening the capacity of law enforcement agencies, including the Indonesian National Police (Polri), the Election Supervisory Body (Bawaslu), the National Cyber and Crypto Agency (BSSN), and the General Elections Commission (KPU), to ensure they possess the technical expertise and resources needed to handle deepfake cases. Synergy among these institutions and technological experts must be reinforced to ensure law enforcement proceeds without impediments and effectively combats technological misuse.

Third, in the context of digital platform regulation, the co-regulation approach is highly relevant. Regulatory governance suggests that regulation in the technological context should involve collaboration among the government, industry, and civil society to produce effective and adaptive governance (Guidi et al., 2020). Social media platforms and digital service providers play a central role in the dissemination of deepfake content; therefore, the government must impose obligations on these platforms to develop automatic detection technologies and mechanisms for removing illegal content within a specified time frame. This model draws inspiration from Germany's NetzDG Law, which mandates social media platforms to address hate speech and illegal content (Hukumu et al., 2025).

Additionally, digital service providers should be granted both authority and corporate social responsibility to safeguard democratic integrity by applying warning labels to content identified as manipulated (Ratna & Rosyidi, 2024). This not only curbs the spread of harmful content but also enhances public literacy regarding the authenticity of the information they consume. Regulation that balances state oversight with technological innovation is crucial to prevent overregulation that may stifle creativity and digital advancement (Rudi, 2023).

Fourth, the establishment of a national coordination mechanism among institutions is a vital aspect that must not be overlooked. Within the framework of network governance, as proposed by Rhodes (Djafar, 2024, p.

52) addressing complex issues such as deepfake misuse must be conducted cross-sectorally and inter-institutionally with effective and sustainable coordination. A National Coordinating Body involving the Ministry of Communication and Informatics (Kominfo), Bawaslu, Polri, BSSN, and KPU should be formed to accelerate real-time responses and the handling of deepfake cases.

This body would be responsible for monitoring, analyzing, and coordinating actions and policies required to address the spread of deepfakes. Data collection and periodic evaluation functions based on policy feedback theory are also crucial to ensure that regulations and policies are continually adapted to technological developments and misuse trends (SoRelle & Michener, 2022). A multi-stakeholder approach will ensure that the resulting policies are not only reactive but also preventive, minimizing the risk of manipulative content dissemination from the outset.

Fifth, public policy strategies must also include strengthening digital literacy among the population as an effective form of public information resilience (Sutalhis & Novaria, 2024). Media literacy, as introduced by Renee Hobbs, underscores the importance of equipping the public with critical thinking skills to filter and analyze the information they receive (Utama & Irwansyah, 2021). In the context of deepfake dissemination, increasing public awareness about the risks and how to recognize manipulative content is key to preventing its negative impact on public opinion and democratic processes.

Behavioral insights and nudging theory by Richard Thaler can be applied through educational campaigns that subtly encourage the public to be cautious and skeptical of the information they encounter and to report suspicious content (Hallsworth & Kirkman, 2020). Applying warning labels to deepfake content circulated on social media is also a form of nudge that can effectively increase public vigilance. Enhancing digital literacy is not solely the responsibility of the government; digital platforms and civil society organizations, acting as social watchdogs, must also play a role.

A multidimensional regulatory strategy that combines legal reform (formulation of technical definitions of deepfake and specific offenses), strengthening affordable and accessible forensic technology, harmonization between laws, and the development of national digital literacy is a necessity in realizing a criminal law system that is adaptive and just in the digital era. Without appropriate strategic steps, the misuse of deepfake has the potential to further damage the integrity of democracy and public trust in information, ultimately threatening the foundations of the rule of law and constitutional democracy in Indonesia.

In conclusion, effective regulatory and public policy strategies to address the legal gaps in the misuse of deepfake technology in Indonesia's elections must emphasize five complementary aspects. First, the creation of specific, clear, and flexible regulations based on Hans Kelsen's legal certainty principle

to ensure legal clarity and prevent exploitation. Second, strengthening law enforcement with advanced digital forensic and cyber intelligence tools to uphold justice and effectiveness in line with Dicey's Rule of Law. Third, implementing co-regulation with digital platforms through regulatory governance to balance state oversight and technological freedom. Fourth, establishing a national inter-agency coordination mechanism based on network governance and good governance for rapid response and continuous evaluation. Fifth, enhancing public digital literacy using media literacy and behavioral nudging as preventive strategies.

With the integrated implementation of these strategies, the legal gap in addressing the misuse of deepfake technology in elections can be significantly reduced. Indonesian democracy can be protected from digital manipulation that threatens public trust, thereby safeguarding a fair, transparent, and democratic electoral process amid the rapid advancement of information technology.

IV. CONCLUSION

The existing regulations in Indonesia, such as the Electronic Information and Transactions Law (UU ITE) and the Election Law (UU Pemilu), are not yet effective in preventing the misuse of deepfakes in elections, as they do not specifically regulate AI-based content manipulation. The main challenges include difficulties in tracing perpetrators, weak oversight of digital platforms, and the low level of digital literacy among the public. As a result, deepfakes can easily spread and influence public opinion without a clear preventive mechanism. Without stricter regulations and a robust detection system, the threat to electoral integrity will continue to escalate in this digital era.

To address this legal gap, a more comprehensive strategy is required, including the establishment of specific regulations that explicitly prohibit and impose strict sanctions on political deepfakes. In addition, law enforcement efforts must be strengthened through the use of digital forensic technologies and artificial intelligence to more effectively detect and prove deepfake cases. The government must also collaborate with social media platforms to remove fake content and enhance public digital literacy through educational campaigns. With this multidimensional approach, Indonesia can safeguard its democracy from the threat of digital manipulation and ensure elections that are fairer and more transparent.

REFERENCE

Ali, M., Fernando, Z. J., Huda, C., & Mahmutarom, M. (2025). Deepfakes and Victimology: Exploring the Impact of Digital Manipulation on Victims. *Substantive Justice International Journal of Law*, *8*(1), 1–12. https://doi.org/https://doi.org/10.56087/substantivejustice.v8i1.306

Anand, A., Madaan, A., & Danielsson, A. (2024). *Intersections Between Rights and Technology*. IGI Global.

Andriyani, W., Sacipto, R., Susanto, D., Vidiati, C., Kurniawan, R., & Nugrahani, R. A. G. (2023). *Technology, Law And Society*. Tohar Media.

Antara. (2024a). *"Deepfake", pemanfaatan AI, dan Pemilu*. Antara. https://www.antaranews.com/berita/3897330/deepfake-pemanfaatan-ai-dan-pemilu#google_vignette

Antara. (2024b). *Mafindo catat hoaks politik meningkat dibanding pemilu lalu*. Antara. https://www.antaranews.com/berita/3944460/mafindo-catat-hoaks-politik-meningkat-dibanding-pemilu-lalu#google_vignette

Apriola. (2021). *Tindak Pindana Kejahatan Undang-Undang ITE*. GUEPEDIA. https://books.google.co.id/books?id=WpGFEAAAQBAJ

Aprita, S. (2024). *Pengantar Ilmu Hukum*. Prenada Media.

Budiyanto, T. S. (2023). *KOLABORASI: Strategi Mengurangi Risiko Pengulangan Kejahatan Terorisme-Jejak Pustaka*. Jejak Pustaka.

Dharmayanti, Y. P., & Soponyono, E. (2025). Criminal Law Policy in Efforts to Combat Artificial Intelligence (AI) in Cyber Crime. *Jurnal Hukum Khaira Ummah*, *20*, 2255–2274. https://doi.org/10.30659/jhku.v20i2.46251

Diati, R., & Triadi, I. (2025). Doxing as a Cybercrime: A Comparative Study Between Indonesia and Singapore: Doxing Sebagai Kejahatan Siber: Studi Komparatif Antara Indonesia dan Singapura. *JIC: Jurnal Hukum Dan Konstitusi*, *1*(4), 175–183. https://doi.org/10.64272/43ax5b53

Djafar, F. (2024). *Teori administrasi publik pendekatan analisis dan penerapan*. Media Nusa Creative (MNC Publishing).

Faathurrahman, M. F., & Priowirjanto, E. S. (2022). Pengaturan Pertanggungjawaban Pelaku Penyalahgunaan Deepfakes Dalam Teknologi Kecerdasan Buatan Pada Konten Pornografi Berdasarkan Hukum Positif Indonesia. *Jurnal Indonesia Sosial Teknologi*, *3*(11). https://doi.org/10.36418/jist.v3i11.528

Guidi, M., Guardiancich, I., & Levi-Faur, D. (2020). Modes of regulatory governance: A political economy perspective. *Governance*, *33*(1), 5–19. https://doi.org/10.1111/gove.12479

Haidarrani, A., Hairani, J., Mubarokah, W., & Sulistianingsih, D. (2024). Pertanggungjawaban Pidana Pelaku Forward Berita Hoax: Telaah dalam Perspektif Undang-Undang ITE. *Hukum Dan Politik Dalam Berbagai Perspektif*, *3*. https://doi.org/10.15294/hp.v3i1.201

Hakim, C. (2025). *Mimpi Demokrasi: Antara Harapan dan Kenyataan*. Yayasan Pustaka Obor Indonesia.

https://books.google.co.id/books?id=NqRZEQAAQBAJ

Hallsworth, M., & Kirkman, E. (2020). *Behavioral insights*. MIT Press.

Herdian, A., & Sumarwan, U. (2025). Analisis Kriminologi Deepfake Melalui Media Sosial Berdasarkan Teori Rational Choice. *IKRA-ITH HUMANIORA: Jurnal Sosial Dan Humaniora*, *9*(1), 323–331. https://journals.upi-yai.ac.id/index.php/ikraith-humaniora/article/view/4496

Hukumu, S., Syahrir, M., & Lukum, A. F. (2025). Criminalization of Online Gender-Based Violence (OGBV): Challenges and Solutions in Indonesian Criminal Law. *Hakim: Jurnal Ilmu Hukum Dan Sosial*, *3*(1), 1013–1031. https://doi.org/10.51903/hakim.v3i1.2297

Juliardi, B., Runtunuwu, Y. B., Musthofa, M. H., TL, A. D., Asriyani, A., Hazmi, R. M., Syahril, M. A. F., Saputra, T. E., Arman, Z., & Rauf, M. A. (2023). *Metode penelitian hukum*. CV. Gita Lentera.

Kelsen, H. (2019). *Teori hukum murni: Dasar-dasar ilmu hukum normatif*. Nusamedia.

Khaeron, H. (2021). *Etika Politik: Paradigma Politik Bersih, Cerdas, Santun Berbasis Nilai Islam*. Nuansa Cendekia.

Kumalasari, T. (2020). Konsep "Antargolongan" dalam Pasal 28 Ayat (2) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (UU ITE). *Media Iuris*, *3*(2), 199. https://doi.org/10.20473/mi.v3i2.20892

Kushariyadi, K., Apriyanto, H., Herdiana, Y., Asy'ari, F. H., Judijanto, L., Pasrun, Y. P., & Mardikawati, B. (2024). *Artificial Intelligence: Dinamika Perkembangan AI Beserta Penerapannya*. PT. Sonpedia Publishing Indonesia.

LuminateGroup. (2024). *Banyak Orang Indonesia Belum Yakin Bisa Bedakan Konten Buatan AI*. https://www.luminategroup.com/posts/news/riset-luminate-ipsos-banyak-orang-indonesia-belum-yakin-bisa-bedakan-konten-buatan-ai

Mahdi, M., Moridu, I., Wibowo, T. S., Utama, A. S., Adinugroho, I., & Amalia, A. (2023). The Effect Of Profitability Mediation On Increasing Company Value Through Corporate Social Responsibility. *International Journal of Economics, Business and Accounting Research (IJEBAR)*, *7*(1).

Mardani. (2024). *Teori Hukum: Dari Teori Hukum Klasik Hingga Teori Hukum Kontemporer*. Prenada Media. https://books.google.co.id/books?id=o6_8EAAAQBAJ

Marpaung, S. A. A. P. (2022). Tindak Pidana Manipulasi Informasi Elektronik Dalam Usaha Transportasi Yang Menggunakan Aplikasi Berbasis

Teknologi Informasi (Analisis Putusan No. Reg: 797/Pid. Sus/2018/Pn. Mks). *Jurnal Ilmiah Mahasiswa Hukum [JIMHUM]*, *2*(5). https://jurnalmahasiswa.umsu.ac.id/index.php/jimhum/article/view/1825

Meliana, Y. (2025). Urgensi formulasi perlindungan hukum dan kepastian pidana terhadap pengaturan tindak pidana deepfake dalam sistem hukum pidana nasional. *Jurnal Hukum Lex Generalis*, *6*(7). https://doi.org/10.56370/jhlg.v6i7.1087

Nabhila, C. (2024). Analisis Tentang Respon Hukum Terkait Penggunaan Artificial Intelligence Di Indonesia. *Pancasila Law Review*, *1*(2), 69–87. https://doi.org/10.46306/rj.v5i1.181

Noerman, C. T., & Ibrahim, A. L. (2024). Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Pelindungan Negara. *Jurnal USM Law Review*, *7*(2), 603–621. https://doi.org/10.26623/julr.v7i2.8995

Novyanti, H., & Astuti, P. (2021). Jerat Hukum Penyalahgunaan Aplikasi Deepfake Ditinjau Dari Hukum Pidana. *Novum: Jurnal Hukum*, 31–40. https://doi.org/10.2674/novum.v0i0.43571

Nurkholisah, S., Rismana, D., Nugroho, A. E., Munjiyah, A., & Ayunisa, Q. (2025). Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan Kriminalisasi Dalam Hukum Pidana Indonesia. *JURNAL USM LAW REVIEW*, *8*(3), 2421–2445. https://doi.org/10.26623/julr.v8i3.13060

Oza, P., Patel, N., & Patel, A. (2024). Deepfake Technology: Overview and Emerging Trends in Social Media. *Available at SSRN 4981040*. https://doi.org/10.2139/ssrn.4981040

Prayoga, H., & Tuasikal, H. (2025). Penyebaran Konten Deepfake Sebagai Tindak Pidana: Analisis Kritis Terhadap Penegakan Hukum Dan Perlindungan Publik Di Indonesia. *Abdurrauf Law and Sharia*, *2*(1), 22–38. https://doi.org/10.70742/arlash.v2i1.194

Rahman, R. A., & Anggriawan, R. (2025). Deepfake and electoral crimes: Criminal law perspectives from Indonesia, India, Pakistan, and the US. *Indonesian Comparative Law Review (ICLR)*, *7*(2), 132–146. https://doi.org/10.18196/iclr.v7i2.26337

Ratna, S. A., & Rosyidi, I. (2024). Implementasi Program CSR Dalam Non-Governmental Organization Melalui Ngo Go Digital. *Reputation: Jurnal Ilmu Hubungan Masyarakat*, *9*(1), 61–80. https://doi.org/10.15575/reputation.v9i1.38834

Rato, D. (2021). *Dasar-Dasar Ilmu Hukum: Memahami Hukum Sejak Dini*. Prenada Media.

Rezky. (2025). *Ketua Bawaslu Ingatkan Bahaya Deepfake dalam Pemilu*. Politikindonesia. https://www.politikindonesia.id/ketua-bawaslu-

ingatkan-bahaya-deepfake-dalam-pemilu?utm_source=copilot.com

Rohmawati, I., Junaidi, A., & Khaerudin, A. (2024). Urgensi Regulasi Penyalahgunaan Deepfake Sebagai Perlindungan Hukum Korban Kekerasan Berbasis Gender Online (KBGO). *Innovative: Journal Of Social Science Research*, *4*(6), 1779–1794. https://doi.org/10.31004/innovative.v4i6.16559

Rosnidar, R., Afrita, A., & Zulkifli, Z. (2017). The Shift of Karo Adat Inheritance Law on Daughter and Widow's Portion. *Jurnal Dinamika Hukum*, *16*(3), 235–242.

Rudi, J. (2023). Penyelarasan Peraturan Perundang-Undangan Sebagai Langkah Reformasi Hukum di Indonesia. *Populer: Jurnal Penelitian Mahasiswa*, *2*(4), 215–233. https://doi.org/10.58192/populer.v2i4.1474

Rumiartha, I. N. P. B. (2022). Correlation Theory of AV Dicey Perspective of the Rule of Law in Indonesia. *Focus Journal Law Review*, *2*(1). https://doi.org/10.62795/fjl.v2i1.19

Sabatier, P. A., & Weible, C. M. (2019). The advocacy coalition framework: Innovations and clarifications. In *Theories of the policy process, second edition* (pp. 189–220). Routledge. https://doi.org/10.4324/9780367274689-7

Santiko, J. A., & Bahri, S. (2024). Analisis Wacana Pada Fenomena Pengunaan Artificial Intelligence (Ai) Dalam Konten Pemilu: Studi Kasus Konten Deepfake Soeharto Mengajak Untuk Memilih Partai Golkar Pada Media Sosial Twitter (X). *Innovative: Journal Of Social Science Research*, *4*(3), 13215–13231. https://doi.org/10.31004/innovative.v4i3.11824

Saragih, G. C., & Kholiq, A. (2024). Criminal Policy on Combating Deepfake Pornography in Indonesia. *Syiah Kuala Law Journal*, *8*(3), 529–547. https://doi.org/10.908/unsyh/24i

Sharma, P., Kumar, M., Sharma, H. K., & Biju, S. M. (2024). Generative adversarial networks (GANs): introduction, taxonomy, variants, limitations, and applications. *Multimedia Tools and Applications*, 1–48. https://doi.org/10.1007/s11042-024-18767-y

Sisephaputra, B., Judijanto, L., Apriyanto, A., Lukman, L., Migunani, M., Umar, N., Sepriano, S., Khairunnisa, K., & Wati, D. C. (2024). *Generative Artificial Intelligence (GenAI): Pengetahuan Dasar GenAI Beserta Penerapannya*. PT. Green Pustaka Indonesia.

Situmeang, B. S., Silitonga, I. Y., Silaen, R. F., Siringoringo, T. H., & Sipayung, E. E. (2024). Pengaruh Artificial Intelligence Terhadap Tingkat Kasus Deep Fake Pada Selebritas di Twitter. *Device*, *14*(1), 80–91. https://doi.org/10.32699/device.v14i1.6984

Soepadmo, H. N. R. (2020). *Buku Ajar Filsafat Hukum*. Zifatama Jawara.

SoRelle, M., & Michener, J. (2022). Methods for applying policy feedback theory. In *Methods of the policy process* (pp. 80–104). Routledge. https://doi.org/10.4324/9781003269083-4

Sutalhis, M., & Novaria. (2024). Literasi Digital dan Pelayanan Publik yang Baik. *ACADEMIA: Jurnal Inovasi Riset Akademik*, *4*(1), 17–23. https://doi.org/10.30656/jpmwp.v6i2.4052

Utama, A. C. C., & Irwansyah, I. (2021). Indonesia dan Dunia: Komparasi Pendidikan Literasi Media untuk Masyarakat yang Beragam. *Media Komunikasi FPIPS*, *20*(2), 93–105. https://doi.org/10.23887/mkfis.v20i2.35729

Wibowo, M. S. I., & Munawar, A. (2024). Kendala Teknis dan Hukum dalam Proses Penyidikan Tindak Pidana Siber di Indonesia. *Jurnal Hukum Lex Generalis*, *5*(7). https://ojs.rewangrencang.com/index.php/JHLG/article/view/641

Wijaya, V. (2021). Perubahan paradigma penataan regulasi di indonesia. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, *10*(2), 167–186. https://doi.org/10.33331/rechtsvinding.v10i2.712