Legal Aspects of Using Deepfake in Political Campaigns: A Threat to Democracy?

Mugi Lestari[1*], Riza Ibrahim[2]

[1]*Communication in Research and Publications, Bandung, Indonesia*
[2]*Research Collaboration Community, Bandung, Indonesia*

Corresponding author email: mu2lestari@gmail.com

Abstract

This study examines the legal aspects of the use of deepfake technology in political campaigns and its implications for the integrity of democracy. Through a qualitative approach with normative legal analysis methods, this study maps regulations related to deepfake in various countries, analyzes case studies of the use of deepfake in political campaigns, and evaluates the effectiveness of regulations in Indonesia. The results show that regulations on deepfake in political campaigns vary significantly between countries, with some countries such as the United States (at the state level) and the European Union having implemented specific regulations, while Indonesia still relies on the Electronic Information and Transactions Law (UU ITE) which does not specifically regulate deepfake. Case study analysis reveals the use of deepfake for positive purposes such as translating political speeches (India) and negative purposes such as spreading disinformation (United States, Russia, Philippines). The main challenges to regulation in Indonesia include the lack of public awareness, limited detection technology, the speed of information dissemination on social media, and the absence of specific sanctions for the misuse of deepfake in a political context. Based on these findings, this study recommends the establishment of specific regulations related to deepfake, strengthening multi-party collaboration in developing detection systems, increasing public education through digital literacy campaigns, and implementing strict law enforcement with specific sanctions. A synergy between comprehensive regulation, advanced detection technology, and high public awareness is needed to mitigate the negative impact of deepfakes on democratic integrity and ensure that this technology is used ethically in political communication.

Keywords: Deepfake, political campaigns, digital regulation, democratic integrity, disinformation

1. Introduction

Advances in artificial intelligence (AI) have transformed many aspects of life, including politics. One of the most interesting innovations in recent years is deepfake technology, which allows the creation of highly realistic audio-visual content, either partially or completely, through digital technology (Chakraborty, 2020; Akhtar et al., 2024). This technology can imitate facial expressions, voices, and movements with great accuracy, raising concerns about its impact on political campaigns (Wang et al., 2022).

In politics, campaigns play an important role in shaping public opinion and determining election results. Deepfake technology has the potential to drastically change political campaigns, both in positive and negative aspects. On the one hand, deepfakes can be used for educational purposes and to simulate political messages (Battista, 2024; Islam et al., 2024). However, on the other hand, this technology poses great risks if used to spread false information, manipulate public perception, and create false narratives that undermine the integrity of democracy.

The use of deepfakes in political campaigns poses new challenges in legal regulation. Many countries currently do not have specific regulations regarding deepfake technology, creating loopholes for its misuse. The difficulty in distinguishing deepfake content from original media makes it a powerful tool for spreading propaganda, defamation, and undermining trust in legitimate political systems (Van der Sloot & Wagensveld, 2022).

Several countries have begun to develop legal regulations to address the threat posed by deepfakes, especially in elections. For example, several states in the United States have passed laws banning the use of deepfakes in political

campaigns. However, the main challenge remains how to quickly identify and regulate deepfake content, while balancing law enforcement with freedom of expression.

In Indonesia, regulations related to deepfakes are still in their infancy. Although the Electronic Information and Transactions Law (UU ITE) regulates the spread of false information, this law does not specifically regulate the use of deepfakes in a political context. This creates a legal loophole that allows political actors to exploit this technology to spread misleading narratives in unethical ways (Judijanto et al., 2025).

The negative impact of deepfakes in political campaigns not only affects individuals, but also undermines public trust in democracy. Deepfake videos showing a political candidate making false statements can mislead voters and lead to wrong political decisions. This situation is further exacerbated by the rapid spread of information on social media, which is often difficult to control (Barari et al., 2021; Pawelec, 2022).

In addition to legal challenges, the technical difficulties in detecting and countering deepfakes are also a concern. Researchers and cybersecurity experts continue to develop algorithms that can identify deepfake content with high accuracy. However, deepfake technology is also constantly evolving, creating a race between deepfake creators and detection systems (Ahmad et al., 2024).

The main question that arises is how legal regulations can effectively address the threat posed by deepfakes in political campaigns without violating freedom of expression. In addition, how can governments, social media platforms, and the public work together to mitigate the negative impacts of deepfakes on democratic processes?

This study examines the legal aspects of the use of deepfakes in political campaigns by analyzing existing regulations, challenges in law enforcement, and steps that can be taken to maintain the integrity of democracy. By reviewing previous cases and exploring regulatory developments in various countries, this study aims to provide a comprehensive understanding of the legal implications of deepfakes in politics and provide effective policy recommendations.

2. Methods

This study uses a qualitative approach with a normative legal analysis method to examine the legal aspects of the use of deepfake in political campaigns. This approach was chosen because the focus of the study is to analyze existing regulations, challenges in law enforcement, and the impact of deepfake on democracy and the political process. The stages in this study can be seen in Figure 1.
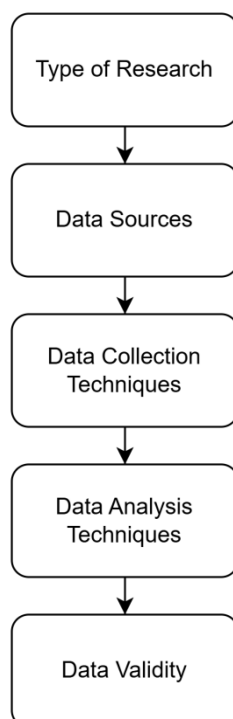
Figure 1: Research Stages

2.1. Type of Research

This study is descriptive-analytical, which aims to describe the phenomenon of the use of deepfake in political campaigns and analyze its legal implications. This approach is used to understand how existing regulations address the challenges of deepfake and assess the effectiveness of policies that have been implemented in several countries.

2.2. Data Sources

This study uses two types of data, namely primary data and secondary data. Primary data is obtained from laws and regulations governing the spread of false information, digital manipulation, and protection of election integrity in Indonesia and in various other countries. In addition, policies from social media platforms regarding deepfake mitigation in political campaigns are also the main sources of this research. Meanwhile, secondary data includes academic literature, legal journals, research reports, news, and case studies of the use of deepfake in political campaigns in various countries. This data source is used to enrich the analysis with academic perspectives and empirical experience.

2.3. Data Collection Techniques

Data collection in this study was carried out through literature studies, where various legal documents, policies, and scientific literature were reviewed to understand existing regulations and legal challenges. In addition, this study also conducted a case analysis, namely by examining several real cases of the use of deepfake in political campaigns to understand its impact on public opinion and trust in the democratic system. If necessary, this study will also conduct interviews with legal experts, academics, or policy makers to gain deeper insight into the legal challenges in overcoming deepfake in the political realm.

2.4. Data Analysis Techniques

Data analysis was carried out through several main approaches. First, normative analysis is used to examine applicable laws and regulations and their relevance to deepfake in political campaigns. Second, critical analysis is applied to evaluate the effectiveness of existing regulations and identify legal loopholes that can be exploited for deepfake abuse. Third, this study uses comparative analysis, namely by comparing deepfake regulations in several countries to find best practices that can be applied in the Indonesian context.

2.5. Data Validity

To ensure the validity and accuracy of the data, this study uses source triangulation techniques. This technique is carried out by comparing information from various legal sources, academic journals, and real cases that have occurred. This approach aims to avoid bias in the analysis and ensure that the research findings are credible and reliable. Thus, the results of the study are expected to provide a comprehensive understanding of the legal aspects of deepfake in political campaigns and offer policy recommendations that can be implemented to address the challenges posed by this technology.

3. Result and Discussion

In this study, various legal sources, case studies, and regulations related to deepfake in political campaigns have been studied in depth. The results of this study include a mapping of regulations in various countries, the effectiveness of existing laws, and an analysis of the impact of deepfake on democracy.

3.1. Regulation of Deepfake in Political Campaigns in Various Countries

This study found that regulations related to deepfake in political campaigns still vary greatly between countries. Some countries already have specific policies, while others still rely on general regulations related to digital disinformation. Table 1 below summarizes some of the regulations that have been implemented in several countries.

Table 1a: Regulation of deepfake in political campaigns in various countries

Countries	Regulations Regarding Deepfakes	Effectiveness	Notes
United States (Some States: Texas, California, etc.)	A ban on the use of deepfakes in political campaigns within 30 days before an election.	Quite effective in preventing information manipulation ahead of elections.	Only applicable in certain states, no federal regulation yet.
European Union	The Digital Services Act (DSA) requires digital platforms to identify and mark deepfakes.	Effective in increasing transparency of digital platforms.	There are still challenges in technical implementation and enforcement.

Table 1b: Regulation of deepfake in political campaigns in various countries

Countries	Regulations Regarding Deepfakes	Effectiveness	Notes
China	Prohibits the production and distribution of deepfakes that can mislead the public.	Effective due to strict government oversight.	Tight restrictions on deepfake technology could stifle AI innovation.
Indonesia	The ITE Law prohibits the spread of fake news, but there are no specific regulations regarding deepfakes.	Less effective in dealing with deepfakes specifically.	Specific regulations are needed to anticipate the misuse of deepfakes in politics.

Table 1 shows that regulations regarding deepfakes in political campaigns vary across different countries. Some countries, such as the United States (in certain states) and China, have implemented specific rules to limit the spread of deepfakes in political contexts. Meanwhile, the European Union has adopted a transparency-based approach by requiring digital platforms to label deepfake content through the Digital Services Act (DSA). In Indonesia, there are no specific regulations addressing the use of deepfakes in political campaigns. Currently, the dissemination of false or misleading information is regulated under the Electronic Information and Transactions Law (UU ITE). However, this law is broad in scope and does not explicitly address deepfakes, making its effectiveness in handling this issue somewhat limited. The variation in regulations across countries highlights the need for a more comprehensive approach to addressing deepfakes in politics. Countries with specific regulations tend to be better prepared to prevent the misuse of this technology, while those relying on general laws may need to consider additional policies to keep up with technological advancements. As artificial intelligence continues to evolve, it is crucial for governments to regularly evaluate and adjust their policies to ensure the integrity of public information while also fostering technological innovation.

3.2. Case Studies of Deepfake use in Political Campaigns

Analysis of several case studies shows that deepfakes have been used in political campaigns for various purposes, both positive and negative. Some of the main cases studied in this study can be seen in Table 2.

Table 2: Case studies of deepfake use in political campaigns

Cases	Countries	Source	Types of Deepfake	Impact
Joe Biden deepfake video (2020)	United States	Blum (2020)	Manipulation of voices and faces to spread false statements.	Increasing disinformation in the run-up to elections.
Narendra Modi deepfake (2021)	India	Sen & Jha, (2024)	Positive campaigns use deepfakes to translate speeches into regional languages.	Increasing the reach of political communication.
Russian opposition leader video manipulation	Russia	Samoilenko & Suvorova (2023)	Deepfakes are used to discredit the opposition.	Influencing public opinion and inhibiting political freedom.
Philippines deepfake hoax campaign (2022)	Philippines	Blancaflor et al. (2023)	Creation of deepfake videos of candidates to spread misleading information.	Increasing distrust of the democratic process.

Table 2 explains that the use of deepfake in political campaigns can serve various purposes, both in supporting political communication and in disseminating less accurate information. Some cases show that deepfake is used in campaign contexts to expand the reach of political messages, such as in Narendra Modi's 2021 campaign in India, where deepfake technology was used to translate speeches into different regional languages, making them more accessible to the public. However, there are also cases where deepfake has been used in ways that influence public perception of political figures, such as in the Joe Biden deepfake video in the United States in 2020 or during the 2022 campaign in the Philippines. These videos utilized deepfake technology to deliver messages that could shape voter opinions ahead of elections. As this technology continues to evolve, it is important for various stakeholders to

understand how deepfake can be used in political campaigns and to consider the necessary steps to ensure its responsible use.

3.3. Effectiveness of Regulation in Indonesia and Challenges of Implementation

Regulations in Indonesia regarding the spread of false information currently still refer to the Electronic Information and Transactions Law (UU ITE), but there are no rules that specifically regulate the use of deepfakes in a political context. This raises several challenges in implementing the law, especially in handling cases of digital manipulation that can influence public opinion and democracy. One of the main challenges is the lack of public awareness about the existence of deepfakes and their impacts. Many people are still unable to distinguish between original videos and manipulated videos, making them more vulnerable to information manipulation.

In addition, the limitations of deepfake detection technology are also an obstacle to law enforcement. Although various artificial intelligence-based systems have been developed to detect deepfakes, this technology still has limitations, especially in dealing with videos made with advanced manipulation techniques. The speed of information dissemination on social media also worsens the situation, because deepfakes can spread widely before being detected and deleted. Another challenge is the absence of specific sanctions for the spread of deepfakes in political campaigns. Currently, deepfake cases are still handled in the general hoax distribution category, which is less specific in addressing this problem.

Regulations that are too strict in dealing with deepfakes also risk curbing freedom of expression, while regulations that are too loose can open up opportunities for abuse. Therefore, a balance is needed between law enforcement and protection of freedom of expression. The government must be able to formulate policies that are not only repressive, but also able to prevent misuse of deepfakes through preventive measures, such as education and cooperation with digital platforms.

3.4. Policy Recommendations

To address the challenges posed by deepfakes in political campaigns, more comprehensive policy measures are needed. One of the main steps is the establishment of specific regulations governing the use of deepfakes in political campaigns. The Indonesian government can refer to regulations that have been implemented in other countries, such as the United States and the European Union, which require digital platforms to mark deepfake content and prohibit its use in political campaigns without valid approval. These regulations must include a clear definition of deepfake, an identification mechanism, and strict sanctions for perpetrators of spreading deepfakes that mislead the public.

In addition to regulations, collaboration between the government, social media platforms, and academic institutions needs to be strengthened to develop a more effective deepfake detection system. Social media platforms have an important role in monitoring and removing deepfake content that has the potential to damage democracy, while academics and researchers can help develop more sophisticated detection technologies. Investment in artificial intelligence research to detect deepfakes needs to be increased so that digital security systems are able to identify manipulation with higher accuracy before the content spreads widely.

Public education is also a key factor in dealing with the threat of deepfakes. The public needs to be given an understanding of how to recognize deepfakes and their impact on public opinion and democracy. Digital literacy campaigns can be conducted through social media, schools, and other educational institutions to raise public awareness about the dangers of deepfake in politics. In addition, the government needs to implement strict and measurable law enforcement, with more specific sanctions for perpetrators of deepfake distribution that harm the public interest. With the right policies and synergy between various parties, the negative impact of deepfake in political campaigns can be minimized, so that this technology is not used for purposes that damage democracy, but is instead utilized ethically for the benefit of more transparent and responsible political communication.

4. Conclusion

This study has analyzed the legal aspects of the use of deepfake technology in political campaigns through a qualitative approach with normative legal analysis methods. The results of the study show that regulations related to deepfake in political campaigns still vary greatly across countries. Several countries such as the United States (at the state level) and the European Union have implemented specific regulations to deal with deepfake, while Indonesia still relies on the Electronic Information and Transactions Law (UU ITE) which is general and does not specifically regulate the use of deepfake in a political context.

The case studies analyzed show that deepfake has been used in political campaigns for various purposes, both positive such as translating speeches into regional languages (the case of India), and negative such as spreading false information (the cases of the United States, Russia, and the Philippines). The negative impact of the misuse of this

technology is not only detrimental to the targeted individuals, but can also erode public trust in the democratic process.

The main challenges in regulating deepfake in Indonesia include: lack of public awareness of the existence and impact of deepfake, limitations in detection technology, the speed of information dissemination on social media, and the absence of specific sanctions for the spread of deepfake in political campaigns. In addition, there is a need to balance law enforcement with protection of freedom of expression.

Based on these findings, this study recommends several policy steps, including: the establishment of specific regulations governing the use of deepfake in political campaigns, strengthening collaboration between the government, social media platforms, and academic institutions to develop a more effective deepfake detection system, increasing public education through digital literacy campaigns, and implementing strict law enforcement with more specific sanctions for perpetrators of deepfake distribution that harm the public interest. With the right policies and synergy between various parties, the negative impact of deepfake in political campaigns can be minimized, so that this technology is not used for purposes that damage democracy, but is used ethically for the interests of more transparent and responsible political communication.

References

Ahmad, J., Salman, W., Amin, M., Ali, Z., & Shokat, S. (2024). A Survey on Enhanced Approaches for Cyber Security Challenges Based on Deep Fake Technology in Computing Networks. *Spectrum of engineering sciences, 2*(4), 133-149.

Akhtar, Z., Pendyala, T. L., & Athmakuri, V. S. (2024). Video and audio deepfake datasets and open issues in deepfake technology: being ahead of the curve. *Forensic Sciences, 4*(3), 289-377.

Barari, S., Lucas, C., & Munger, K. (2021). Political deepfake videos misinform the public, but no more than other fake media. *OSF Preprints, 13*, 1-16.

Battista, D. (2024). Political communication in the age of artificial intelligence: an overview of deepfakes and their implications. *Society Register, 8*(2), 7-24.

Blancaflor, E., Anave, D. M., Cunanan, T. S., Frias, T., & Velarde, L. N. (2023, July). A Literature Review of the Legislation and Regulation of Deepfakes in the Philippines. In *Proceedings of the 2023 14th International Conference on E-business, Management and Economics* (pp. 392-397).

Blum, S. (2020, January 2). *Misleading Joe Biden Video Is the First Viral Controversy of 2020.* GQ. https://www.gq.com/story/misleading-joe-biden-video-first-controversy-2020. Retrieved March 3, 2025.

Chakraborty, U. (2020). *Artificial Intelligence for All: Transforming Every Aspect of Our Life.* Bpb publications.

Islam, M. B. E., Haseeb, M., Batool, H., Ahtasham, N., & Muhammad, Z. (2024). AI threats to politics, elections, and democracy: a blockchain-based deepfake authenticity verification framework. *Blockchains, 2*(4), 458-481.

Judijanto, L., Utama, A. S., & Setiyawan, H. (2025). Implementation of Ethical Artificial Intelligence Law to Prevent the Use of AI in Spreading False Information (Deepfake) in Indonesia. *The Easta Journal Law and Human Rights, 3*(02), 101-109.

Pawelec, M. (2022). Deepfakes and democracy (theory): How synthetic audio-visual media for disinformation and hate speech threaten core democratic functions. *Digital society, 1*(2), 19.

Samoilenko, S. A., & Suvorova, I. (2023). Artificial intelligence and deepfakes in strategic deception campaigns: The US and Russian experiences. In *The Palgrave handbook of malicious use of AI and psychological security* (pp. 507-529). Cham: Springer International Publishing.

Sen, R., & Jha, S. (2024). Women Under Hindutva: Misogynist Memes, Mock-Auction and Doxing, Deepfake-Pornification and Rape Threats in Digital Space. *Journal of Asian and African Studies*, 00219096241257686.

Van der Sloot, B., & Wagensveld, Y. (2022). Deepfakes: regulatory challenges for the synthetic society. *Computer Law & Security Review, 46,* 105716.

Wang, H., Sharma, A., & Shabaz, M. (2022). Research on digital media animation control technology based on recurrent neural network using speech technology. *International Journal of System Assurance Engineering and Management, 13*(Suppl 1), 564-575.