Available online at https://ejournal.corespub.com/index.php/ijhlp/index

International Journal of Humanities, Law, and Politics

e-ISSN 3025-0536

Vol. 3, No. 1, pp. 6-15, 2025

Legal Implications of the Use of Deepfake in Politics and National Security in Indonesia

Nestia Lianingsih[1*], Alim Jaizul[2]

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

**Corresponding author email: nestialianingsih@gmail.com*

Abstract

Deepfake technology has developed rapidly and has had a significant impact in various fields, including politics and national security. This study analyzes the legal implications of the use of deepfakes in politics in Indonesia, highlighting regulatory challenges, the effectiveness of technology detection, and its impact on public opinion. This study uses a mixed methods approach, combining literature analysis, case studies, interviews with legal and technology experts, and social media data analysis. The results show that the spread of deepfakes has increased sharply ahead of the 2024 General Election, especially on Twitter, Facebook, and TikTok, contributing to disinformation and public polarization. Existing regulations, such as the Electronic Information and Transactions Law (UU ITE) and the Criminal Code (KUHP), do not specifically regulate deepfakes, thus creating difficulties in law enforcement. In addition, existing detection technologies still face challenges in identifying increasingly sophisticated deepfake content. As a mitigation measure, this study recommends the formation of special regulations regarding deepfakes, improving detection technology through collaboration with the technology sector, increasing the capacity of law enforcement in digital forensics, and public education to improve digital literacy. It is hoped that these steps can reduce the negative impact of deepfake on democracy and national security stability in Indonesia.

Keywords: Deepfake, disinformation, legal regulation, national security, 2024 election

1. Introduction

Artificial Intelligence (AI) technology has experienced rapid development in recent years, having a significant impact on various sectors, including media, entertainment, and cybersecurity (Meng et al., 2024). One AI innovation that is currently in the spotlight is deepfake, a visual and audio manipulation technology that is capable of creating content that is almost indistinguishable from the original. By utilizing sophisticated machine learning algorithms, deepfake allows someone to replace a person's face, voice, or movements in a video in a very realistic manner (Ratnawita, 2025).

Although this technology has various positive applications in the creative industry, education, and security, its irresponsible use can pose a major threat, especially in the realm of politics and national security. Deepfake has been used to spread disinformation, damage an individual's reputation, and create false narratives that can influence public opinion. In some countries, deepfake has even been used as a tool to manipulate election results, exacerbate social tensions, and spread propaganda that can threaten political stability and national security (Langa, 2021).

Indonesia as a democratic country with a large digital population is not free from the threat of deepfake. People who are increasingly dependent on digital information have the potential to become victims of manipulation by deepfake-based content, especially ahead of elections or in sensitive political situations (Purwadi et al., 2022). Deepfake content that spreads widely through social media can create divisions in society, worsen the political climate, and even disrupt national security if used in cyber attacks or espionage (Battista, 2024).

In the legal context, Indonesia still faces challenges in overcoming the misuse of deepfakes. Currently, there are no specific regulations that specifically regulate the use of deepfakes, although several laws such as the Electronic Information and Transactions Law (UU ITE), the Criminal Code (KUHP), and regulations related to defamation can be used to address the negative impacts of deepfakes. However, the complexity of this technology makes legal

evidence difficult, especially in distinguishing between original and manipulated content generated by AI (Hafiz, 2024).

In addition, another challenge faced is the low level of digital literacy among the Indonesian people. Many internet users still do not understand how deepfakes work and how to recognize manipulated content. This makes it easier for deepfakes to spread widely without adequate verification, exacerbating their negative impacts on democracy and national security.

Globally, several countries have begun to draft specific regulations to address deepfakes. For example, the European Union through the Digital Services Act (DSA) and the United States with the Deepfake Detection Act have begun to formulate stricter policies in monitoring and controlling the use of deepfakes (Fabuyi et al., 2024). Indonesia needs to learn from these steps in order to formulate comprehensive and effective legal policies to deal with the misuse of deepfakes domestically.

In addition to legal regulations, it is also necessary to increase the capacity of law enforcement officers in detecting and handling deepfake cases. Digital forensic technology must continue to be developed to ensure that deepfakes can be identified accurately and used as evidence in the judicial process (Delfino, 2022). This requires cooperation between the government, academics, and the technology sector in creating a system that can detect and verify the authenticity of digital content more effectively.

Not only that, the role of social media platforms is also crucial in overcoming the spread of deepfakes. As the main channels for distributing digital content, platforms such as Facebook, Instagram, Twitter, and TikTok need to have stricter policies in identifying and removing dangerous deepfake content. Collaboration between the government and technology companies can help strengthen automatic detection systems to prevent the widespread spread of manipulative content.

Based on these problems, this study aims to analyze the legal implications of the use of deepfake in politics and national security in Indonesia. This study will examine how existing regulations are able to face the challenges of deepfake, as well as how legal policies can be strengthened to protect political stability and national security from the threats of this technology. With a deeper understanding, it is hoped that this study can provide strategic recommendations for policy makers in formulating regulations that are more adaptive to the development of digital technology.

2. Literature Review

This study aims to analyze the influence of social media on voter participation in the 2024 General Election in Indonesia. To achieve this goal, this study uses a mixed methods approach, which combines quantitative and qualitative methods. This approach was chosen because it can provide a more comprehensive understanding of the phenomena that occur, both in terms of numerical measurements and in-depth insights into voter attitudes and behavior. The following is a detailed explanation of the methodology used in this study.

2.1. Deepfake Concept and Characteristics

Deepfake is an artificial intelligence (AI)-based technology that uses Generative Adversarial Networks (GAN) techniques to create realistic-looking visual and audio manipulations (Masood et al., 2023). This technology allows the creation of content that can resemble certain individuals very realistically, either in the form of video, audio, or static images (Gong, 2021). In its early development, deepfake was used for entertainment and digital art purposes, but recently it has begun to be misused to spread misinformation, create political propaganda, and commit cybercrime (Myers, 2021).

Several studies have examined the technical aspects of deepfake, including detection methods based on digital forensic analysis and machine learning (Heidari, 2024). The deepfake detection system is currently still being developed, given the ability of this technology to produce manipulations that are increasingly difficult to recognize with the naked eye (Mohammed, 2024). However, from a regulatory perspective, many countries still face challenges in accommodating the development of deepfake technology in the existing legal system (Tuysuz & Kılıç, 2023).

2.2. Deepfake in the Context of Politics and National Security

In the context of politics, deepfake poses a significant threat because it can be used to manipulate public opinion, discredit political figures, and spread false information during election campaigns (Islam et al., 2024). A study conducted by Shirish & Komal, (2021) shows that deepfake has been used in various disinformation strategies in several countries, including the United States, the United Kingdom, and India. In Indonesia, cases of the spread of deepfake-based hoaxes have begun to increase along with the increasing consumption of digital media in society (Volkova, 2024).

In addition to politics, deepfake also has the potential to threaten national security. This technology can be used to create more sophisticated social engineering, such as fake identity-based attacks that can deceive security forces or government institutions (Alharbi et al., 2021). Deepfake also plays a role in subversive information campaigns, which aim to undermine public trust in the government or state institutions (Pawelec, 2022). Therefore, countries at high risk of cyberattacks have begun to implement mitigation strategies involving legal regulations and automatic detection technology.

2.3. Legal Aspects of Deepfake Regulation

From a legal perspective, many countries are still looking for the right formulation to regulate the misuse of deepfake. In the European Union, regulations regarding deepfake have begun to be integrated within the framework of the Artificial Intelligence Act, which aims to control the use of AI in creating manipulative content (Kavoliūnaitė-Ragauskienė, 2024). The United States has issued the Deepfake Accountability Act, which demands transparency in the use of deepfake technology for public purposes (Fabuyi et al., 2024).

In Indonesia, regulations related to deepfake are still limited and generally only refer to general rules in the Electronic Information and Transactions Law (UU ITE) No. 19 of 2016, which regulates the spread of false information and violations of privacy rights. In addition, the Criminal Code (KUHP) can also be used to ensnare perpetrators who use deepfakes in criminal acts of fraud or defamation. However, existing regulations are still general and do not explicitly cover the technical aspects of deepfakes, so more specific policy updates are needed (Kirana, 2021). Several studies suggest that Indonesia needs to adopt specific regulations regarding deepfakes that cover aspects of prevention, legal sanctions, and detection and enforcement mechanisms (Mahmuda et al., 2025; Mahendra & Sakti, 2025; Rhogust, 2024). In addition, cooperation between the government, the private sector, and social media platforms is also key to controlling the spread of dangerous deepfakes (Subrahmanyam, 2025).

2.4. Deepfake Mitigation Strategies through Technology and Regulation

A number of studies have proposed various strategies to deal with the spread of deepfakes. From a technological perspective, several approaches that have been developed include AI-based detection, metadata analysis, and digital watermarking that can mark original content and distinguish it from manipulated content (Ghiurău & Popescu, 2024). Convolutional Neural Networks (CNN)-based detection systems have shown high accuracy in identifying deepfakes, but the main challenge still lies in the ability of deepfakes to continue to evolve and evade detection (Hussain & Ibraheem, 2023).

On the regulatory side, research shows that an effective legal approach must include preventive policies, strict legal enforcement, and increasing digital literacy in the community (Sugeng et al., 2022). The government also needs to work with technology companies to develop a stricter content verification system, so that deepfakes can be detected before they spread widely on social media (Al-Khazraji et al., 2023).

In Indonesia, an effective mitigation strategy must combine legal, technological, and public education approaches. The government can form a special agency to handle deepfake-based digital content and develop a deepfake detection platform that can be used by the public. In addition, a more massive digital literacy campaign is needed to increase public awareness of the dangers of deepfake and how to recognize manipulated content (Hwang et al., 2021).

3. Methods

Research on the legal implications of the use of deepfake in politics and national security in Indonesia is carried out systematically in order to produce valid conclusions and recommendations that can be applied. Therefore, this research will follow structured stages, starting from identifying problems to drawing conclusions. Each stage has an important role to ensure that this research is not only based on theory but also considers relevant empirical and technological aspects. The stages in this research can be seen in Figure 1.

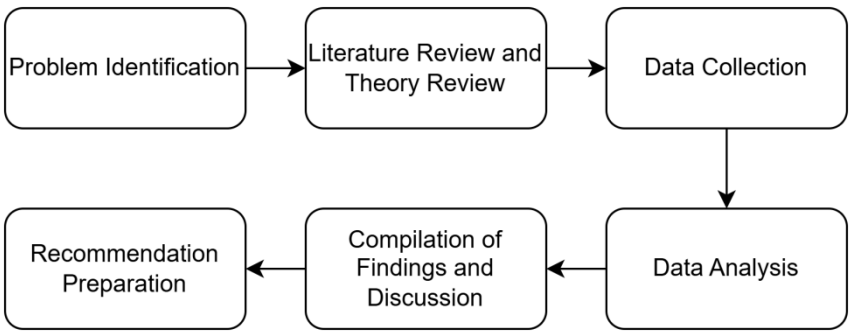

Figure 1: Research Stages

3.1. Problem Identification

The first step in this research is to identify the main problems related to the use of deepfake in the context of politics and national security in Indonesia. Deepfake is an artificial intelligence-based technology that allows the manipulation of a person's face and voice in the form of photos or videos realistically. This technology can be used for good purposes, such as entertainment and education, but it also has the potential to cause serious negative impacts, especially in the spread of disinformation.

In the context of politics, deepfake can be used to falsify statements by public figures, spread propaganda, or manipulate public opinion. Meanwhile, in the context of national security, deepfake can be a threat in the spread of fake news, defamation of state officials, and use in cyber attacks on government institutions. Therefore, this study seeks to answer the main question: How do legal regulations in Indonesia address the threat of deepfakes, and what steps need to be taken to strengthen legal protection against these threats?

3.2. Literature Review and Theory Review

The next stage is to conduct a literature review to understand the legal, technological, and social and political aspects of the use of deepfakes. This literature review will cover various sources, including laws and regulations in Indonesia, academic journals, policy reports, and case studies from various countries.

In terms of law, this study will examine current regulations, such as the Electronic Information and Transactions Law (UU ITE), the Criminal Code (KUHP), and the Personal Data Protection Law (UU PDP). In addition, the literature study will also discuss relevant legal theories, such as freedom of expression, privacy rights, and cybersecurity. In terms of technology, this study will discuss the development of deepfake technology, the detection methods used, and the challenges faced in identifying increasingly sophisticated deepfakes.

3.3. Data Collection

This study will use primary and secondary data to ensure that the analysis is comprehensive and accurate. Primary data will be collected through interviews with experts in the fields of law, cybersecurity, and artificial intelligence technology who have a deep understanding of the impact of deepfakes in the context of politics and national security. These interviews will be conducted using a qualitative approach to gain perspectives from experts regarding legal challenges and law enforcement strategies for deepfake cases. In addition, this study will also examine case studies of several incidents that have occurred in Indonesia and abroad, where deepfakes have been used to manipulate public opinion, spread disinformation, or create political instability. These case studies will help identify patterns of deepfake use and the legal responses that have been taken.

In addition to interviews and case studies, this study will also utilize social media and big data analysis to understand the extent to which deepfakes have spread in Indonesia's digital space. Data from various platforms such as Twitter, Facebook, YouTube, and TikTok will be collected to see the trend of deepfake distribution and how the public responds to it. On the other hand, secondary data will be obtained through a review of legal documents, scientific journals, research reports, and publications from international organizations that have discussed deepfake regulations. Some of the main documents that will be analyzed include the Electronic Information and Transactions Law (UU ITE), the Criminal Code (KUHP), and the Personal Data Protection Law (UU PDP), as well as policies implemented in other countries in dealing with deepfakes. With a combination of primary and secondary data, this study is expected to provide a more comprehensive picture of the legal challenges in overcoming deepfakes in Indonesia.

3.4. Data Analysis

After the data is collected, this study will enter the analysis stage to identify patterns, challenges, and opportunities in legal regulations against deepfakes. The main approaches used in this analysis are normative, empirical, and technological approaches. The normative approach is used to evaluate whether the current legal regulations in Indonesia are sufficient in dealing with the threat of deepfakes or still have legal gaps. By comparing policies in various existing regulations, this study will assess whether there is a need for improvement or the formulation of new, more specific rules.

Meanwhile, an empirical approach is taken to understand the real impact of deepfake on politics and national security based on analyzed case studies and interviews with experts. These empirical findings will show how deepfake influences public perception, creates social instability, and becomes a tool in unethical political strategies. On the other hand, a technological and digital forensics approach is used to examine the extent to which deepfake detection tools can be used in the legal process. Some detection methods that will be discussed in this study include the use of

metadata analysis, artificial neural networks to identify visual manipulation patterns, and AI-based software designed to detect irregularities in deepfake videos.

Through this multidisciplinary approach, the study will describe the extent to which the Indonesian legal system is able to face the challenges of deepfake and how technology can support the legal process in identifying and proving the validity of digital content.

3.5. Compilation of Findings and Discussion

The next stage in this research is compiling the findings based on the analysis that has been carried out. One of the main aspects that will be discussed is the effectiveness of current regulations in dealing with deepfakes, including whether existing regulations are sufficient or still have legal gaps that need to be addressed. This research will also examine how deepfakes have been used in the context of national politics and security, both in Indonesia and in other countries, to provide an overview of the potential for broader threats.

In addition, the discussion in this research will highlight how technology can help support the legal process, especially in terms of evidence and investigation. Increasingly sophisticated deepfakes can complicate the legal process in determining the validity of digital evidence. Therefore, this research will explore how the use of deepfake detection technology can be applied in the justice system in Indonesia. One of the main challenges in this aspect is the minimal capacity of law enforcement officers in identifying deepfakes and the limited regulations in accommodating digital evidence in trials.

As part of the discussion, this research will also compare regulations in Indonesia with policies implemented in other countries that already have clearer rules regarding deepfakes. Countries such as the United States, the European Union, and China have begun to draft regulations that specifically address deepfakes in various aspects, including the spread of false information, privacy violations, and threats to political stability. By conducting this comparison, the study will provide insight into policy strategies that can be adopted by Indonesia to deal with deepfakes more effectively.

3.6. Recommendation Preparation

Based on the findings that have been produced, this study will provide recommendations that can be used as a basis for policy makers to strengthen regulations regarding deepfakes in Indonesia. One of the main recommendations proposed is the creation of special regulations that explicitly regulate the use of deepfakes, both in the context of politics, security, and digital media. These regulations must include aspects of prevention, law enforcement mechanisms, and protection for victims who are harmed by the misuse of deepfakes.

In addition, this study recommends increasing the capacity of law enforcement officers in handling deepfake cases, both through technical training in detecting deepfakes and through collaboration with digital forensics experts and technology companies. Currently, many deepfake cases are difficult to investigate due to the lack of technical understanding among law enforcement officers. Therefore, training and development of technological infrastructure to support digital investigations are very important.

Another recommendation proposed in this study is to strengthen cooperation between the government and social media platforms in detecting and removing harmful deepfake content. Many digital platforms have now begun to develop AI-based deepfake detection systems, but their implementation is still limited. Therefore, cooperation between regulators and technology companies needs to be improved in order to limit the spread of harmful deepfakes, especially those related to political and national security disinformation.

Finally, this study emphasizes the importance of increasing digital literacy among the public, so that the public can be more critical in consuming information and not easily influenced by misleading deepfake content. Public education programs on how to identify deepfakes and the dangers posed by the spread of false information need to be encouraged, both through media campaigns and through digital education curricula in schools. With a combination of regulatory, technological, and educational measures, Indonesia can be better prepared to face the threat of deepfakes in the realm of politics and national security.

4. Result and Discussion

4.1. General Description of Respondents

This section will discuss the results of research related to the legal implications of the use of deepfake in politics and national security in Indonesia. The results of the research will be presented in the form of qualitative analysis from interviews, case studies, and big data analysis from social media. Data will also be displayed in tabular form to facilitate understanding.

4.2. Problem Identification

From the results of the problem identification, it was found that the use of deepfake in the context of politics and national security in Indonesia still has many challenges, both in terms of law, technology, and public awareness. Deepfake is often used to spread disinformation, defame political figures, and influence public opinion ahead of elections. This phenomenon is increasing with the advancement of artificial intelligence technology that allows the creation of increasingly realistic and difficult-to-detect deepfakes. Problems in the use of deepfake in Table 1.

Table 1: Identification of Problems in the Use of Deepfake

Aspects	Problems Found
Regulation	There is no specific regulation regarding deepfake in Indonesian law.
Technology	Deepfake detection technology is still limited and easily bypassed by more sophisticated deepfakes.
Public Awareness	The public still has low digital literacy in recognizing deepfakes.
Law Enforcement	Difficulties in proving the law in cases involving deepfakes.

Table 1 shows various aspects of the problems that arise in the use of deepfake in Indonesia, especially in the context of politics and national security. In terms of regulation, until now there have been no specific regulations that explicitly regulate deepfake in the Indonesian legal system. In terms of technology, although there have been efforts to develop a deepfake detection system, the available technology is still limited and can be easily bypassed by more sophisticated deepfakes.

In addition, public awareness of the threat of deepfake is still low, which is caused by the lack of digital literacy in recognizing manipulated content. Meanwhile, in terms of law enforcement, there are difficulties in proving the involvement of perpetrators in deepfake cases, especially because of the nature of this technology which can be used anonymously and is difficult to track. The challenges in dealing with deepfake in Indonesia not only cover the technological aspect, but also include regulation, public awareness, and the effectiveness of law enforcement. Therefore, a multidisciplinary approach is needed involving the government, academics, and the community in an effort to mitigate the negative impacts of deepfake on political stability and national security.

4.3. Process in the Research Method

This research uses a multidisciplinary approach that includes legal, technological, and social analysis to understand the impacts and regulations related to deepfake. Literature studies were conducted to collect references regarding deepfake regulations in various countries. Case studies are used to analyze the use of deepfake in Indonesia and other countries. Expert interviews were conducted with legal, technology, and cybersecurity experts to gain deeper insights. In addition, social media data analysis was conducted to monitor the spread of deepfakes on platforms such as Twitter, Facebook, and TikTok. The process can be seen in Table 2.

Table 2: Process in Research Methods

Stage	Description
Literature Study	Collecting references related to deepfake regulations in various countries.
Case Study	Analyzing deepfake use cases in Indonesia and other countries.
Expert Interview	Exploring insights from legal, technology, and cybersecurity experts.
Social Media Data Analysis	Monitoring the spread of deepfakes on platforms such as Twitter, Facebook, and TikTok.

Table 2 shows that this study uses a comprehensive approach by combining several methods to understand the impact and regulations related to deepfake. The first stage is a literature study, which aims to collect references on deepfake policies and regulations in various countries as a comparison with conditions in Indonesia.

Next, case studies are conducted to analyze various examples of the use of deepfake, both in Indonesia and other countries, in order to identify patterns and impacts in various contexts, especially in politics and national security. Then, interviews with experts were conducted to gain a deeper perspective on the legal, technological, and cybersecurity challenges in dealing with deepfake. The experts interviewed included legal experts, artificial intelligence technology, and cybersecurity specialists who have experience in dealing with digital threats. Finally, social media data analysis was conducted with the aim of monitoring how deepfake is spread on platforms such as

Twitter, Facebook, and TikTok. This process helps identify distribution patterns, actors involved, and public responses to deepfake content.

With this combination of methods, research can provide a more comprehensive picture of the challenges faced in dealing with deepfake as well as more accurate recommendations for policymakers, technology practitioners, and the wider community.

4.4. Results of Literature and Case Studies

In the literature study, it was found that several countries such as the United States and the European Union have begun to implement specific regulations to address the threat of deepfakes. However, in Indonesia, the use of deepfakes is still included in the general violation category in the ITE Law and the Criminal Code.

In addition, the results of case studies in Indonesia show that the use of deepfakes has been found in several political incidents, including in black campaigns during elections and the spread of fake news attacking public officials. Some of the deepfakes that have been distributed have even been used to incite and create social instability can be seen in Table 3.

Table 3: Regulations Related to Deepfakes in Various Countries

Country	Regulations Related to Deepfake
United States	Deepfake Accountability Act, a regulation on transparency in the use of deepfake.
European Union	The Digital Services Act (DSA) regulates the use of AI in digital media.
Indonesia	The ITE Law and the Criminal Code do not explicitly cover deepfake.

Table 3 shows the differences in regulatory approaches related to deepfakes in various countries. The United States has implemented the Deepfake Accountability Act, which regulates transparency in the use of deepfakes and provides a legal basis for legal action against misuse of this technology. The European Union through The Digital Services Act (DSA) has regulated the use of artificial intelligence in digital media, including deepfakes, to ensure that online platforms are responsible for the spread of manipulative content.

In Indonesia, there is no specific regulation that explicitly regulates deepfakes. Currently, cases involving deepfakes can only be prosecuted under the Electronic Information and Transactions Law (UU ITE) and the Criminal Code (KUHP), which are still general in nature and do not cover the technical aspects and specific impacts of deepfake technology.

The absence of specific regulations is a challenge in dealing with the misuse of deepfakes in Indonesia, especially in the context of politics and national security. Based on the results of case studies, deepfakes have been used in black campaigns during elections, the spread of fake news attacking public officials, and content that triggers social instability. Therefore, more specific policies are needed to effectively address the threat of deepfakes and protect society from their negative impacts.

4.5. Results of social media data analysis

This study also conducted a big data analysis of the spread of deepfakes on social media in Indonesia. From the analysis results, it was found that the number of deepfake content related to politics increased significantly ahead of the 2024 election. This data was obtained through monitoring various platforms such as Twitter, Facebook, and TikTok. The results can be seen in Table 4.

Table 4: Results of Social Media Data Analysis

Platforms	Deepfake Content Count (2023)	Deepfake Content Count (2024)	Percentage Increase (%)
Twitter	2,300 cases	5,600 cases	143%
Facebook	1,800 cases	4,200 cases	133%
TikTok	3,500 cases	8,000 cases	129%

The results in Table 4 show that the number of deepfake content circulating on social media has increased significantly ahead of the 2024 Election. Platforms such as Twitter, Facebook, and TikTok experienced a spike in deepfake cases with a fairly high percentage increase, ranging from 129% to 143% compared to the previous year.

The highest increase occurred on Twitter with an increase of 143%, followed by Facebook (133%), and TikTok (129%). This indicates that social media has become the main means of spreading deepfakes, especially in a political context. This spike is most likely related to political campaigns, digital propaganda, and disinformation efforts that are increasingly rampant ahead of the election. This pattern also shows that deepfakes have become a strategic tool in influencing public opinion in the digital world.

With the increasing threat of deepfakes on social media, stronger mitigation measures are needed, such as improving detection technology, public digital literacy, and stricter regulations to reduce their negative impact on democracy and social stability.

4.6. Results of Interviews with Legal and Technology Experts

Interviews with legal and technology experts revealed several key points related to the challenges of deepfake regulation and mitigation in Indonesia. Current regulations are considered weak in dealing with deepfakes because there are no specific rules governing the use of AI technology in creating digital content. In terms of technology, deepfake detection is still developing, but is not yet strong enough to keep up with the progress of deepfake technology itself. Meanwhile, from a cybersecurity perspective, deepfakes can be a threat to national security, especially if used in the context of espionage and political propaganda. The results can be seen in table 5.

Table 5: Results of Interviews with Legal and Technology Experts

Expert	Opinion
Legal Expert	Current regulations are still weak in dealing with deepfakes because there are no specific rules governing the use of AI technology in creating digital content.
Technologist	Deepfake detection technology continues to develop, but is still not strong enough to keep up with the progress of deepfake technology itself.
Cyber Security Expert	Deepfakes pose a threat to national security, especially when used in the context of espionage and political propaganda.

Table 5 shows various perspectives from legal, technology, and cybersecurity experts on the challenges in regulating and mitigating deepfakes in Indonesia. From a legal perspective, experts assess that existing regulations are still weak because there are no specific rules governing the use of artificial intelligence in creating digital content. As a result, law enforcement against deepfake abuse is difficult and less effective.

Meanwhile, from a technological perspective, experts highlight that although deepfake detection technology continues to develop, its capabilities are still lagging behind the progress of deepfake technology itself. This creates a gap that makes it increasingly difficult to recognize and overcome deepfakes. And from a cybersecurity perspective, experts emphasize that deepfakes can be a serious threat to national security, especially if used for espionage and political propaganda purposes. The use of deepfakes in this context can trigger social instability, manipulation of public opinion, and the spread of information that can disrupt national order. With these findings, it can be concluded that the challenges in dealing with deepfakes require a multidisciplinary approach involving regulatory updates, strengthening detection technology, and increasing readiness to face cybersecurity threats posed by deepfakes.

4.7. Discussion and Recommendations

Based on the research results, it was found that Indonesia needs a more comprehensive approach to address the threat of deepfakes. Some of the proposed recommendations include special regulations governing the use of deepfakes, strengthening detection technology through collaboration with technology companies, increasing the capacity of law enforcement through digital forensics training, and increasing the digital literacy of the community to be more critical in receiving digital information.

Table 6: Strategies and Implementation Steps in Addressing Deepfakes

Strategy	Implementation Steps
Special Regulations	Drafting specific laws related to deepfakes.
Detection Technology	Developing an AI system to detect deepfakes.
Law Enforcement Training	Workshops and training for police and law enforcement officers.
Digital Literacy	Socialization and education through social media and seminars.

Table 6 shows various strategies and implementation steps that can be taken to address the threat of deepfakes in Indonesia. In terms of regulation, a special law is needed that specifically regulates the use, distribution, and sanctions against misuse of deepfakes, so that it can provide a stronger legal basis in handling related cases.

In terms of detection technology, the development of an artificial intelligence (AI)-based system that is able to accurately identify deepfakes is a crucial step. This can be done through collaboration between the government, technology companies, and academics to create more effective solutions in recognizing and reducing the spread of deepfake content. In terms of law enforcement, digital forensics training is needed for law enforcement officers so that they have the skills to identify, prove, and handle deepfake cases more efficiently. This training can be done through workshops, seminars, and collaboration with cybersecurity experts. Finally, increasing the digital literacy of the community is an important factor in deepfake mitigation efforts. Socialization and education through various channels, such as social media, seminars, and public campaigns, can help the public become more critical and aware of the potential for manipulation carried out with deepfake technology.

Overall, these steps need to be implemented simultaneously to create a digital ecosystem that is safer and more resilient to deepfake threats, especially in the context of politics and national security.

5. Conclusion

This study highlights the legal implications of the use of deepfake in politics and national security in Indonesia. The results of the study show that deepfake has become a significant threat in the political realm, especially in the spread of disinformation, defamation, and manipulation of public opinion ahead of the election. Although existing regulations, such as the Electronic Information and Transactions Law (UU ITE) and the Criminal Code (KUHP), can be used to ensnare perpetrators, there are no specific rules that explicitly regulate deepfake technology.

From the analysis of social media data, it was found that the spread of deepfake content increased significantly ahead of the 2024 Election, with the largest spike on the platforms Twitter, Facebook, and TikTok. In addition, interviews with legal and technology experts revealed that existing deepfake detection systems still have limitations in identifying increasingly realistic content. Another challenge is the low digital literacy of the community, which makes them vulnerable to deepfake manipulation.

To overcome this problem, a comprehensive approach is needed that includes the formulation of special regulations, strengthening detection technology through collaboration with technology companies, increasing the capacity of law enforcement in digital forensics, and public education to improve digital literacy. With an integrated strategy, it is hoped that Indonesia can be better prepared to face the threat of deepfakes to political stability and national security.

References

Alharbi, A., Dong, H., Yi, X., Tari, Z., & Khalil, I. (2021). Social media identity deception detection: a survey. *ACM computing surveys (CSUR), 54*(3), 1-35.

Al-Khazraji, S. H., Saleh, H. H., Khalid, A. I., & Mishkhal, I. A. (2023). Impact of deepfake technology on social media: Detection, misinformation and societal implications. *The Eurasia Proceedings of Science Technology Engineering and Mathematics, 23*, 429-441.

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

Delfino, R. A. (2022). Deepfakes on trial: a call to expand the trial judge's gatekeeping role to protect legal proceedings from technological fakery. *Hastings LJ, 74*, 293.

Fabuyi, J., Olaniyi, O. O., Olateju, O., Aideyan, N. T., Selesi-Aina, O., & Olaniyi, F. G. (2024). Deepfake Regulations and Their Impact on Content Creation in the Entertainment Industry. *Archives of Current Research International, 24*(12), 10-9734.

Ghiurău, D., & Popescu, D. E. (2024). Distinguishing Reality from AI: Approaches for Detecting Synthetic Content. *Computers, 14*(1), 1.

Gong, Y. (2021). Application of virtual reality teaching method and artificial intelligence technology in digital media art creation. *Ecological Informatics, 63*, 101304.

Hafiz, M. (2024). The Era of Artificial Intelligence: Examining Indonesia's Adaptability and Legal Challenges. *Available at SSRN 4967017*.

Heidari, A., Jafari Navimipour, N., Dag, H., & Unal, M. (2024). Deepfake detection using deep learning methods: A systematic and comprehensive review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 14*(2), e1520.

Hussain, Z. F., & Ibraheem, H. R. (2023). Novel convolutional neural networks based Jaya algorithm approach for accurate deepfake video detection. *Mesopotamian Journal of CyberSecurity, 2023*, 35-39.

Hwang, Y., Ryu, J. Y., & Jeong, S. H. (2021). Effects of disinformation using deepfake: The protective effect of media literacy education. *Cyberpsychology, Behavior, and Social Networking, 24*(3), 188-193.

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.

Kavoliūnaitė-Ragauskienė, E. (2024). Artificial Intelligence in Manipulation: The Significance and Strategies for Prevention. *Baltic Journal of Law & Politics, 17*(2), 116-141.

Kirana, Y. (2021). PROTECTION OF PERSONAL DATA ON WHATSAPP IN THE PERSPECTIVE OF LAW NO. 19 OF 2016 ABOUT ELECTRONIC INFORMATION AND TRANSACTION (ITE). *Awang Long Law Review, 3*(2), 78-87.

Langa, J. (2021). Deepfakes, real consequences: Crafting legislation to combat threats posed by deepfakes. *BUL Rev., 101*, 761.

Mahendra, R. S., & Sakti, M. (2025). LEGAL LIABILITY FOR DEEPFAKES WITHOUT CONSENT ON SOCIAL MEDIA. *Syiah Kuala Law Journal, 9*(1).

Mahmuda, A. F., Gusti, M. C., & Anrusfi, F. (2025). Exploring the potential crimes and legal liability of artificial intelligence within the framework of Indonesian criminal law. *Ex Aequo Et Bono Journal Of Law, 2*(2), 96-107.

Masood, M., Nawaz, M., Malik, K. M., Javed, A., Irtaza, A., & Malik, H. (2023). Deepfakes generation and detection: State-of-the-art, open challenges, countermeasures, and way forward. *Applied intelligence, 53*(4), 3974-4026.

Meng, Y., Jungjin, K., Hak-Chun, L., Je, C. D., & Cheng, P. (2024). The impact of artificial intelligence big data technology on the development of media economy information security. *Journal of Computational Methods in Sciences and Engineering, 24*(2), 675-695.

Mohammed, A. (2024). Deep Fake Detection and Mitigation: Securing Against AI-Generated Manipulation. *Journal of Computational Innovation, 4*(1).

Myers, M. E. (2021). Propaganda, Fake News, and Deepfaking. In *Understanding Media Psychology* (pp. 161-181). Routledge.

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.

Purwadi, A., Serfiyani, C. Y., & Serfiyani, C. R. (2022). Legal landscape on national cybersecurity capacity in combating cyberterrorism using deep fake technology in Indonesia. *International Journal of Cyber Criminology, 16*(1), 123-140.

Ratnawita, R. (2025). Cybersecurity in the AI Era Measures Deepfake Threats and Artificial Intelligence-Based Attacks. *Journal of the American Institute, 2*(2), 180-189.

Rhogust, M. (2024). Legal Framework for Cybersecurity in the Digital Economy: Challenges and Prospects for Indonesia. *Journal of Law, Social Science and Humanities, 1*(2), 166-180.

Shirish, A., & Komal, S. (2023). A Socio-Legal Inquiry on Deepfakes. *Cal. W. Int'l LJ, 54*, 517.

Subrahmanyam, S. (2025). Collaboration and Collective Action: Addressing the Deepfake Challenge as a Community. In *Deepfakes and Their Impact on Business* (pp. 143-172). IGI Global Scientific Publishing.

Sugeng, S., Fitria, A., & Rohman, A. N. R. A. N. (2022). Promoting digital literacy for the prevention of risk behavior in social media for adolescents. *Jurnal Keamanan Nasional, 8*(1).

Tuysuz, M. K., & Kılıç, A. (2023). Analyzing the legal and ethical considerations of Deepfake Technology. *Interdisciplinary Studies in Society, Law, and Politics, 2*(2), 4-10.

Volkova, S. (2024). Deepfakes: Fraud and Cybercrime. *Deepfakes and Their Impact on Business, 221*.