INDONESIAN COMPARATIVE LAW REVIEW
Volume 7, Issue. 2, June 2025, 132-146
P-ISSN: 2655-2353, E-ISSN: 2655-6545

# Deepfake and Election Crimes: Comparative Perspectives from Indonesia, India, Pakistan, and the U.S.

**Rofi Aulia Rahman[1], Rizaldy Anggriawan[2*]**
[1]*Faculty of Law, Universitas Surabaya, Indonesia*
[2]*Faculty of Law and Political Sciences, University of Szeged, Hungary*
[2]*Faculty of Law, Universitas Muhammadiyah Yogyakarta, Indonesia*
**Corresponding Author: rofiauliarahman@staff.ubaya.ac.id*

Doi: http://dx.doi.org/10.18196/iclr.xxxx

## Abstract

*This study examines the legal responses to deepfake technology in the context of election crimes, focusing on Indonesia, India, Pakistan, and the United States. The objective is to analyze how criminal law frameworks in these countries address the misuse of deepfakes in political campaigns and to identify legal gaps and challenges. This study used normative legal research method and a comparative approach, the study reviews relevant laws and regulations, including the Electronic and Information Transaction Law and Personal Data Protection Law in Indonesia, as well as corresponding legislation in the other countries. The results show that while Indonesia, India, and Pakistan rely primarily on general cybercrime and penal provisions, the United States has introduced specific state-level laws to criminalize election-related deepfakes. This highlights a regulatory gap in countries that lack targeted legislation. The study recommends the development of more comprehensive and specific legal frameworks to address the risks of deepfake misuse in elections. It also emphasizes the importance of enhancing detection technologies, increasing public awareness, and strengthening international cooperation to uphold electoral integrity and democratic processes.*

**Keywords:** Artificial Intelligence, Deepfake, Election Crime, Indonesia, Political Campaign

## 1. Introduction

Deepfake technology, which is based on artificial intelligence to create visual and audio content that is very similar to the original but completely fake, has raised concerns in various sectors, especially in the political context. Deepfakes have great potential to be used as a manipulation tool during political campaigns, where false or falsified information can spread quickly through social media, influence public opinion, and even manipulate election results. In Indonesia, social media usage is very high, with more than 139 million active users recorded in January 2024, according to data from We Are Social reported by Databoks. This figure is equivalent to 49.9% of the total national population.[1] This has the potential to become a threat of disinformation and digital manipulation, including deepfakes, which is increasingly worrying.

Data from various institutions shows that the spread of false information and disinformation during elections has increased significantly in recent years. Based on the

[1] Mutia Annur Cindy, 'Ini Media Sosial Paling Banyak Digunakan Di Indonesia Awal 2024', *Databoks*, 2024 <https://databoks.katadata.co.id/datapublish/2024/03/01/ini-media-sosial-paling-banyak-digunakan-di-indonesia-awal-2024>.

findings of the General Elections Supervisory Agency (Bawaslu), there were 341 alleged internet content violations, of which 96 percent or 326 were hate speech. In addition, data from Mafindo disclosed by the General Chairperson of Siberkreasi, Donny Budi Utoyo, showed that from January to December 2023, there were 2,330 hoaxes recorded, and 55.5 percent of them were related to politics.[2] The spread of political hoaxes further adds to the challenge of maintaining the quality of information during elections. The risk of spreading false information is also exacerbated by technological advances, such as deepfakes, which allow for the creation of manipulative content, increasing the potential for harm and disinformation during elections.

Research related to the impact of deepfake technology in the political context in Indonesia is still limited. Research by Fadhilah and Retnoningsih (2024) highlights the potential dangers of deepfake in spreading political disinformation in Indonesia, but is limited to the pre-elderly group.[3] Meanwhile, Algamar and Ampri (2022) discuss the legal vulnerability to deepfake technology in Indonesia, but focus more on the protection of child celebrities.[4] A broader study by Perdana and Widianti (2018) discussed the role of social media in the spread of fake news during the 2019 election campaign, but did not specifically discuss deepfake technology as a manipulation tool.[5] On the other hand, in terms of the legal framework, research by Devina et al. (2021) reviewed laws related to hoaxes and disinformation in Indonesia, such as the ITE Law.[6] However, these studies do not explicitly discuss how Indonesian law can or should adapt to address the threat of deepfakes in political campaigns. Thus, there has been no study that combines the aspect of the use of deepfakes in political campaigns with the perspective of criminal law on elections in Indonesia.

Although there have been several studies on deepfake and disinformation in Indonesia, the research gap that still exists lies in the lack of studies that specifically link the use of deepfake in political campaigns with the criminal legal framework for elections in Indonesia and its comparison with other countries. Previous research tends to focus on the social impact of disinformation or on the general legal framework, but not much has discussed how deepfake is used in political campaigns and the legal challenges that arise from its use. This gap is important to address considering that elections are one of the pillars of democracy, and the use of deepfake can significantly damage public trust and the legitimacy of the election process.

To fill this gap, this study aims to focus on discussing three main aspects, namely the understanding and basic concepts of deepfake technology and its application in political

[2] Robi Ardianto, 'Bawaslu Temukan 341 Dugaan Pelanggaran Konten Internet, Paling Banyak Soal Ujaran Kebencian', *Badan Pengawas Pemilu*, 2024 <https://bawaslu.go.id/id/berita/bawaslu-temukan-341-dugaan-pelanggaran-konten-internet-paling-banyak-soal-ujaran-kebencian>.

[3] Almira Daisy Zahrah Fadhilah and Sri Retnoningsih, 'Perancangan Kampanye Digital Melawan Disinformasi Melalui Artificial Intelligence Dan Deepfake Di Kalangan Pra Lansia Usia 45-55 Tahun', *Prosiding FAD*, 3.2 (2024), pp. 1–17 <https://eproceeding.itenas.ac.id/index.php/fad/article/view/2943>.

[4] Muhammad Deckri Algamar and Aliya Ilysia Irfana Ampri, 'Hak Untuk Dilupakan: Penghapusan Jejak Digital Sebagai Perlindungan Selebriti Anak Dari Bahaya Deepfake', *Jurnal Yustika: Media Hukum Dan Keadilan*, 25.01 (2022), pp. 25–39, <https://doi.org/10.24123/yustika.v25i01.5091>.

[5] Aditya Perdana and Delia Wildianti, 'Narasi Kampanye Dan Media Sosial Dalam Pemilu Presiden Dan Wakil Presiden Tahun 2019', *Jurnal Bawaslu DKI*, 2018, pp. 21–39.

[6] Cindy Bella Devina and others, 'Tinjauan Hukum Kriminalisasi Berita Hoax: Menjaga Persatuan vs. Kebebasan Berpendapat', *Kosmik Hukum*, 21.1 (2021), p. 44, <https://doi.org/10.30595/kosmikhukum.v21i1.8874>.

campaigns, then exploring how deepfake is used in the context of political campaigns in Indonesia and its comparison with other countries, and finally analyzing the existing legal framework and criminal challenges associated with the use of deepfake in election campaigns. The main objective of this research is to provide in-depth insights into how deepfake technology influences political dynamics in Indonesia and other countries such as the United States, India and Pakistan and to propose policy recommendations and better legal frameworks to address this issue.

## 2. Method

This research is normative research where the majority of data used qualitative approach data with descriptive-analytical discussion techniques to understand and analyze the use of deepfake technology in political campaigns in Indonesia and the legal framework that regulates it. Data was collected through a literature study by reviewing relevant literature, including books, academic journals, legal regulations, and reports from government agencies and non-governmental organizations related to deepfake and elections in Indonesia. In addition, this study will also utilize the analysis of legal documents, such as the Electronic Information and Transactions Law (UU ITE), the Personal Data Protection Law (UU PDP), the Election Law, and the Criminal Code (KUHP), to identify applicable regulations and how they are applied to the use of deepfake in the context of political campaigns. Furthermore, this study also uses a comparative approach with other countries such as the United States, India and Pakistan to find out examples of implementation, issues, and relevant legal frameworks.

In addition to doctrinal analysis, this research incorporates a comparative legal method, which systematically compares the legal responses of Indonesia, India, Pakistan, and the United States to the misuse of deepfakes in elections. This method involves identifying legal similarities and differences across jurisdictions to evaluate the effectiveness and comprehensiveness of each country's criminal law provisions. Furthermore, data analysis is carried out by identifying patterns of deepfake use in elections, both locally and globally, to understand their impact in Indonesia. In addition, this study will evaluate the existing legal framework in addressing the threat of deepfake, including legal loopholes that need to be fixed. This study used a normative approach to analyze relevant legal provisions and regulations, and a limited empirical approach to understand how deepfake is applied in political campaign practices.

## 3. Discussion and Analysis

### 3.1. Basic Concepts of Deepfake: How Does It Work?

Deepfake is a digital media manipulation technology that uses artificial intelligence (AI), specifically deep learning techniques, to create or modify video and audio to appear very realistic. The name deepfake is a combination of "deep learning," an AI method that involves learning from very large amounts of data, and "fake," which refers to the fake or manipulated results of the digital media.[7] This technology uses neural networks to learn and

[7] Shannon Gandrova and Ricky Banke, 'Penerapan Hukum Positif Indonesia Terhadap Kasus Kejahatan Dunia Maya Deepfake', *Madani: Jurnal Ilmiah Multidisiplin*, 1.10 (2023), pp. 650–57. <https://doi.org/10.5281/zenodo.10201140>.

mimic very subtle visual and audio patterns, creating videos and sounds that appear authentic, even though the content has actually been manipulated.

The main technology behind deepfakes is Generative Adversarial Networks (GANs). GANs were first introduced by Ian Goodfellow in 2014, who defined GANs as an AI model consisting of two parts: a generator and a discriminator.[8] These two parts work in opposition to each other to create increasingly more realistic fake content. Here's how GANs work:[9]

1. The generator is tasked with creating fake content, for example by taking visual data such as a person's face, and generating new images or videos based on that data. The generator continuously tries to create content that is as close to the real thing as possible.

2. The discriminator, on the other hand, has the task of distinguishing whether the content generated by the generator is real or fake. It acts as a "rater," providing feedback to the generator if the results are not realistic enough.

This process continues iteratively until the generator is able to produce content that is nearly indistinguishable from the original, resulting in a very convincing deepfake. Ian Goodfellow calls GANs one of the most powerful AI innovations in terms of creating realistic synthetic images and videos.[10]

In addition to using GANs, deepfake technology also utilizes Convolutional Neural Networks (CNNs) to learn and mimic visual patterns from input data such as videos or photos. CNNs can learn specific features of a person's face, movements, and expressions, which are then used to manipulate the original media or create new media that resembles the input data.[11] Deepfake technology has a wide range of applications, from the creative industry to communications, but its most worrying use is in disinformation and political manipulation. In the creative realm, deepfakes are used to create stunning visual effects, for example in filmmaking.[12]

However, the use of deepfakes is problematic in political campaigns, where deepfake videos can be used to create disinformation, falsify politicians' statements or actions, and even change the context of political messages.[13] Hany Farid, a computer science professor at the University of California, Berkeley, said that deepfakes used in disinformation campaigns have the potential to undermine social cohesion and, ultimately, pose a serious threat to

[8] Ian Goodfellow and others, 'Generative Adversarial Nets', *Advances in Neural Information Processing Systems*, 27 (2014), pp. 1–9 <https://doi.org/10.48550/arXiv.1406.2661>.
[9] Tanvi Arora and Rituraj Soni, 'A Review of Techniques to Detect the GAN-Generated Fake Images', in *Generative Adversarial Networks for Image-to-Image Translation* (Elsevier, 2021), pp. 125–59, <https://doi.org/10.1016/B978-0-12-823519-5.00004-X>.
[10] Ian Goodfellow and others, 'Generative Adversarial Networks', *Communications of the ACM*, 63.11 (2020), pp. 139–44.
[11] Santosh Kolagati, Thenuga Priyadharshini, and V. Mary Anita Rajam, 'Exposing Deepfakes Using a Deep Multilayer Perceptron – Convolutional Neural Network Model', *International Journal of Information Management Data Insights*, 2.1 (2022), p. 100054, <https://doi.org/10.1016/j.jjimei.2021.100054>.
[12] Mika Westerlund, 'The Emergence of Deepfake Technology: A Review', *Technology Innovation Management Review*, 9.11 (2019), pp. 39–52.
[13] Jetrin Arfan Santiko and Syaiful Bahri, '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 (2024), pp. 13215–31.

democracy.[14] This statement emphasizes the serious threat deepfakes pose to the integrity of information, especially in the context of political campaigns.

Deepfakes are becoming increasingly complex and difficult to detect due to AI's ability to learn detailed patterns of a person's facial expressions, voice intonation, and body movements. High-quality deepfake videos are able to not only realistically fake a person's face, but also mimic their voice and movements. This is further enhanced by the development of audio synthesis technology, which uses AI models to mimic a specific individual's speech and voice patterns based on recordings of their real voice.[15]

In addition to being used for visual manipulation, audio deepfakes have been able to mimic voices very realistically. For example, several voice actors have been used as data to train audio deepfake models, which can then reproduce their voices with high accuracy. This allows content creators to imitate or reanimate the voices of famous figures in different contexts than the original.[16] Available data shows that deepfake technology continues to grow rapidly. Deeptrace reported in 2021 that the number of deepfakes on the internet increased by 330%, reaching more than 50,000 at its peak between October 2019 and June 2020. Since then, the number has continued to grow. Video-sharing websites like YouTube and Facebook are a source of news for one in five internet users.[17] The growth in the number of deepfake videos shows how quickly this technology is spreading, especially in a digital context.

### 3.2. Deepfake Influence to Elections: Experiences from Indonesia and Selected Countries

Deepfake is one of the products of artificial intelligence (AI) technology that is increasingly developing and is starting to be widely used in the political realm, especially campaigns. This technology allows the manipulation of audio, video, and image content with very realistic results, so that it can create disinformation that is difficult to distinguish from facts. The use of deepfake in political campaigns has a significant impact because it can be used to damage the reputation of candidates, influence voter perceptions, and disrupt the democratic process as a whole.[18]

Real-world examples of the impact of deepfake use in politics can be seen in several international cases. One famous case is the Canadian startup Lyrebird, which caused a sensation in 2017 with an audio recording of Barack Obama, Donald Trump, and Hillary Clinton talking about "fake news."[19] While the video was created for educational purposes about the dangers of deepfakes, it shows how this technology can manipulate public

[14] Hany Farid and Hans-Jakob Schindler, *Deep Fakes* (Konrad-Adenauer-Stiftung, 2020).
[15] Zaynab Almutairi and Hebah Elgibreen, 'A Review of Modern Audio Deepfake Detection Methods: Challenges and Future Directions', *Algorithms*, 15.5 (2022), p. 155, <https://doi.org/10.3390/a15050155>.
[16] Jan Kietzmann, Adam J Mills, and Kirk Plangger, 'Deepfakes: Perspectives on the Future "Reality" of Advertising and Branding', *International Journal of Advertising*, 40.3 (2021), pp. 473–85, <https://doi.org/10.1080/02650487.2020.1834211>.
[17] Achhardeep Kaur and others, 'Deepfake Video Detection: Challenges and Opportunities', *Artificial Intelligence Review*, 57.6 (2024), pp. 1–47, <https://doi.org/10.1007/s10462-024-10810-6>.
[18] Nicholas Diakopoulos and Deborah Johnson, 'Anticipating and Addressing the Ethical Implications of Deepfakes in the Context of Elections', *New Media & Society*, 23.7 (2021), pp. 2072–98, <https://doi.org/10.1177/1461444820925811>.
[19] Miriam Meckel and Léa Steinacker, 'Hybrid Reality: The Rise of Deepfakes and Diverging Truths', *Morals & Machines*, 1.1 (2021), pp. 10–21.

perception. Maria Pawelec, a political scientist with a focus on digitalization, ethics and impacts and governance of technology, underlines that deepfakes pose a significant threat in politics, because video is a medium that the public trusts very much. Once a deepfake is shared, even if it is later revealed to be fake, the damage to trust is already done.[20]

Another example is the Indian 2024 general elections. India has seen a significant increase in the use of deepfake technology for political campaigning. One prominent example is the Dravida Munnetra Kazhagam (DMK) party using deepfakes to "resurrect" their former leader, M. Karunanidhi, who had died in 2018. The deepfake video featured Karunanidhi ostensibly endorsing the party, with the aim of leveraging his popularity to influence voters. In addition, AI technology has been used to translate political speeches in real-time, allowing candidates to reach voters in different languages and dialects. However, the use of this technology has raised concerns about the potential for the spread of misleading information. The Indian government is aware of the threat posed by deepfakes. Prime Minister Narendra Modi has called deepfake videos a "major concern," and authorities have warned social media platforms that they could lose their safe-harbour status, which protects them from liability for content posted by third parties on their sites, if they do not act.[21]

In addition to the mentioned case, it also occurred in Pakistan during the 2023 elections, where former Prime Minister Imran Khan, while in prison, appeared in a deepfake video to campaign for his party, Pakistan Tehreek-e-Insaf (PTI). He used AI technology to create an image and voice clone that allowed him to address an online rally. The speech was viewed more than 1.4 million times on YouTube and attended live by tens of thousands of people. Although Pakistan has drafted an AI law, digital rights activists have criticized the lack of safeguards against disinformation and protections for vulnerable communities, including women. Nighat Dad, co-founder of the Digital Rights Foundation, said the threat of disinformation to elections and the democratic process in Pakistan cannot be underestimated.[22]

Meanwhile, in Indonesia, the 2024 election has shown how deepfake technology is starting to be used in political campaigns. One prominent example is a deepfake video that shows President Soeharto, who died in 2008, urging people to vote for the Golkar Party. The video became controversial because it showed the use of iconic historical figures to influence voters.[23] The presence of deepfakes in the context of elections in Indonesia adds to the challenges for election organizers and the public. In addition to the video of Soeharto, a video of President Joko Widodo is also circulating, appearing to be giving a speech in Mandarin.[24] The video has raised speculation among the public about its authenticity and purpose. This kind of content can create confusion and doubt among voters, especially in an

[20] Maria Pawelec, 'Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions', *Digital Society*, 1.2 (2022), p. 19, <https://doi.org/10.1007/s44206-022-00010-6>.
[21] Abhinaba Datta and Subarno Banerjee, 'Unmasking Deepfakes-A Legal Perspective', *Jus Corpus Law Journal*, 4.4 (2023), pp. 336–58.
[22] Thomas Gaulkin, 'The Campaign Volunteer Who Used AI to Help Swing Pakistan's Elections: Interview with Jibran Ilyas', *Bulletin of the Atomic Scientists*, 80.5 (2024), pp. 275–80, <https://doi.org/10.1080/00963402.2024.2388458>.
[23] Heather Chen, 'AI "Resurrects" Long Dead Dictator in Murky New Era of Deepfake Electioneering', *CNN*, 2024 <https://www.cnn.com/2024/02/12/asia/suharto-deepfake-ai-scam-indonesia-election-hnk-intl/index.html>.
[24] Laila Afifa, 'Kominfo Ministry Asserts Jokowi's Speech in Chinese Produced by Deepfake', *Tempo*, 2023 <https://en.tempo.co/read/1789306/kominfo-ministry-asserts-jokowis-speech-in-chinese-produced-by-deepfake>.

already polarized political climate. Moreover, the use of AI in the 2024 Indonesian Election also includes candidate animations. One example is the candidate pair Prabowo Subianto-Gibran Rakabuming Raka who used animated photos in the "*gemoy*" style for their campaign.[25] While the use of AI in animation may seem more light-hearted and entertaining, it still shows how digital technology is increasingly involved in political campaigns in Indonesia.

While Indonesia has begun to witness the use of deepfake content in electoral contexts—such as the manipulated videos involving Soeharto and Joko Widodo—the legal response remains largely reactive and fragmented. Current laws like the ITE Law and PDP Law may provide some coverage, but they were not designed with synthetic media in mind, leading to interpretive uncertainty and enforcement limitations. The absence of specific provisions targeting deepfakes creates a normative gap that undermines legal certainty and poses a threat to electoral justice. Deepfakes can manipulate voter perception, distort candidate reputations, and exploit identity-based sentiment, yet the lack of clear criminal classifications risks rendering such acts unpunishable under existing law.

Therefore, the use of deepfakes in political campaigns is not only an ethical issue, but also involves serious violations of the law. According to Article 45A of Law Number 1 of 2024 concerning the second amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions, it regulates the matter of taking action against cases of spreading fake news. Perpetrators who spread false information are threatened with a maximum prison sentence of six years and/or a maximum fine of IDR 1 billion. In this context, deepfakes that spread false information can be categorized as an election crime that has the potential to mislead voters. Then considering that much deepfake content targets sensitive issues and manipulates someone's speech or actions, this technology has great potential to cause social conflict, especially during political campaigns that are full of tension.

### 3.3. Criminal Provisions on the Use of Deepfakes in Political Campaigns

The constitutional policy of general elections (Pemilu) in Indonesia is regulated in Article 22 E paragraph (1) of the 1945 Constitution, which states that elections must be carried out directly, generally, freely, secretly, honestly and fairly every five years. Although the principle of "fairness" is one of the important principles in organizing elections, there is no official definition of the meaning of justice in the constitution. The International Institute for Democracy and Electoral Assistance (IDEA) defines electoral justice as an effort to:[26]

- Ensure that all actions, procedures and decisions related to the electoral process comply with the applicable legal framework;
- Protect or restore electoral rights; and
- Provide persons who believe their electoral rights have been violated with the ability to lodge complaints, have their cases heard and receive a decision.

[25] Yarnis Yarnis and Nani Nurani Muksin, 'Semiotics Analysis of'Gemoy'Animations Political Communication Strategy in Efforts to Change Prabowo-Gibran's Branding', *Lentera: Jurnal Ilmu Dakwah Dan Komunikasi*, 2024, pp. 1–23, <https://doi.org/10.21093/lentera.v8i1.8069>.
[26] International Institute for Democracy and Electoral Assistance, *Electoral Justice* (International IDEA, 2010).

Fraud in the election process is a form of violation of the principle of justice and can damage the integrity of the democratic process. Injustice in elections not only tarnishes the reputation of procedural democracy, but also threatens the substance of justice in the democratic system. Fraudulent elections can result in the election of individuals who are not in accordance with the will of the people, ignoring the principle that the voice of the people is the voice of God *(vox populi vox dei)*[27] and the highest law *(vox populi suprema lex)*.[28] Therefore, maintaining fairness in elections is key to ensuring that democracy functions well and legitimately reflects the will of the people.

Deepfake technology is a sophisticated innovation that allows image or video engineering by integrating a person's face into new content. By utilizing biometric data, such as very specific facial images, this technology can create very realistic content.[29] The use of deepfakes has great potential in a variety of applications, but also carries serious risks regarding privacy and security.[30]

However, Law Number 7 of 2017 concerning General Elections does not specifically regulate the use of artificial intelligence in an election crime. If referring to Chapter II concerning Election Criminal Provisions in Articles 488 to 554 of the Election Law, not a single article can be found that regulates election crimes related to the use of artificial intelligence, which includes deepfake. Therefore, in the event of a violation in a political campaign caused by the use of deepfake, law enforcement is left to other relevant sectoral regulations. One of the regulations that can ensnare deepfake perpetrators is Law Number 27 of 2022 concerning Personal Data Protection (UU PDP), where Article 66 regulates the prohibition on the creation of false personal data or falsification of personal data for personal or group gain, and which can cause harm to other individuals. Violations of these provisions can be subject to criminal sanctions, including imprisonment of up to six years and/or a maximum fine of IDR 6 billion. This provision affirms the commitment to protect personal data and prevent misuse of deepfake technology that can harm many parties.

Despite the existence of various legal instruments, such as the ITE Law, PDP Law, and KUHP, the Indonesian legal framework against deepfakes remains fragmented and reactive. These laws do not explicitly regulate synthetic media or AI-generated deception, raising concerns about their effectiveness. While they may provide prosecutorial tools under general provisions like defamation, false information, or data falsification, they lack doctrinal coherence when applied to deepfake-specific harms such as audiovisual impersonation or synthetic speech. As a result, they function more as temporary patchwork solutions rather than a comprehensive regime capable of anticipating and mitigating evolving digital threats. The absence of clear definitions and thresholds also creates legal uncertainty for both law enforcers and potential perpetrators, undermining deterrence.

---

[27] Wesley Enoch, 'Vox Populi, Vox Dei (The Voice of the People Is the Voice of God)', *Voice and Speech Review*, 12.1 (2018), pp. 77–85, <https://doi.org/10.1080/23268263.2017.1398919>.
[28] Sarno Wuragil and Widayati Widayati, 'Development of Democracy & Phenomenon of Single Candidate in Regional Election (Pilkada)', *Law Development Journal*, 3.1 (2021), pp. 120–29, <https://doi.org/10.30659/ldj.3.1.120-129>.
[29] John Wojewidka, 'The Deepfake Threat to Face Biometrics', *Biometric Technology Today*, 2020.2 (2020), pp. 5–7, <https://doi.org/10.1016/S0969-4765(20)30023-0>.
[30] Runi Hilda Fadlani Siregar and Muhammad Vicky Afris Suryono, 'Towards Transparent and Secure Elections: The Legal Landscape of Digital Electoral Systems in Indonesia', *E-Justice: Journal of Law and Technology*, 1.2 (2025), pp. 15–30.

Deepfake-related offenses raise significant challenges for fundamental principles of criminal law. The principle of legality (*nullum crimen sine lege*) requires that criminal conduct be clearly defined by law. Deepfakes, being a new and evolving form of deception, often fall outside existing definitions, thereby risking violations of *lex certa* (clarity of the norm) and *lex scripta* (written law). For instance, a manipulated video designed to sway voters may not meet the traditional legal elements of fraud or defamation. This ambiguity creates prosecutorial gaps and invites constitutional challenges. If criminal provisions are to apply fairly, they must be adapted or reformed to provide legal certainty while balancing due process and technological neutrality. Indonesia's reliance on general provisions without explicit references to deepfakes potentially weakens the application of these core principles, risking both undercriminalization and overreach.

The regulation on deepfake, which includes the act of changing a person's face so that it looks authentic, can also be in conflict with Article 35 of Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE). This article states that anyone who intentionally and without the right manipulates, creates, changes, removes, or destroys electronic information and/or electronic documents with the aim of making the information considered authentic, can be subject to legal sanctions. Electronic information in this context includes various types of data, such as writing, sound, images, and other electronic documents that have been processed and can be understood by authorized persons.

Violations of these provisions are subject to quite severe criminal penalties. Based on Article 51 of the ITE Law, perpetrators can be subject to imprisonment of up to 12 years or a maximum fine of IDR 12 billion. This provision reflects the government's serious efforts to handle and overcome the misuse of deepfake technology, which can threaten the integrity and public trust in electronic information. In addition, the provisions regarding the use of deepfake can also be related to Law No. 1 of 2023 concerning the Criminal Code (New Criminal Code). In the New Criminal Code, deepfakes containing elements of insult and defamation can be subject to criminal penalties in accordance with Articles 433, 434, and 436 in conjunction with Article 441. Meanwhile, deepfakes containing hatred and hostility are regulated in Article 243.

### 3.3.1. Criminal Provisions in India

Currently, India lacks specific legislation targeting deepfake technology. However, various provisions within the Information Technology Act, 2000 (IT Act) and the Indian Penal Code, 1860 (IPC) are invoked to combat offenses arising from the malicious use of deepfakes in political contexts. For instance, Section 66D of the IT Act penalizes cheating by personation using computer resources,[31] which can include the creation and distribution of deepfakes intended to deceive voters or tarnish the reputation of political figures. Conviction under this section can result in imprisonment of up to three years and a fine of up to ₹1 lakh. Moreover, Section 66E of the IT Act addresses violations of privacy through the intentional capture, publication, or transmission of images of private areas without consent.[32] This provision is pertinent when deepfakes involve compromising or fabricated imagery of

[31] Debarati Halder, 'A Retrospective Analysis of S. 66a: Could S. 66a of the Information Technology Act Be Reconsidered for Regulating'Bad Talk'in the Internet?', *Indian Student Law Review (ISLR)*, 3 (2015), pp. 91–118.

[32] Sumanjeet, 'The State of E‐commerce Laws in India: A Review of Information Technology Act', *International Journal of Law and Management*, 52.4 (2010), pp. 265 – 82, <https://doi.org/10.1108/17542431011059322>.

political candidates, with penalties including imprisonment for up to three years or fines reaching ₹2 lakh.

The IPC further supplements these measures. Section 469 pertains to forgery intended to harm reputation, directly applicable to deepfakes crafted to damage the public image of political figures. Offenders under this section may face imprisonment of up to three years and fines. Moreover, Section 500 of the IPC deals with criminal defamation, prescribing imprisonment for up to two years, fines, or both for individuals who defame others through false representations, including deepfakes.

The Representation of the People Act, 1951, also plays a crucial role in maintaining electoral integrity.[33] Section 125 prohibits the promotion of enmity between classes during elections, a provision that can extend to the dissemination of deepfakes designed to incite societal divisions. Violations can lead to imprisonment of up to three years and fines. Furthermore, Section 126 restricts election-related content dissemination through cinematography, television, or similar mediums in the 48 hours preceding the conclusion of polling, a timeframe within which deepfakes could critically influence voter decisions.

### 3.3.2. Criminal Provisions in Pakistan

In January 2025, Pakistan's parliament enacted amendments to the Prevention of Electronic Crimes Act (PECA), aiming to strengthen regulations against the spread of disinformation, including deepfakes. The revised law criminalizes the intentional dissemination of false or fake information likely to cause fear, panic, or unrest in society. Offenders may face imprisonment of up to three years, fines reaching 2,000,000 Pakistani Rupees, or both. These measures underscore the state's commitment to curbing the malicious use of digital technologies in the political sphere. [34]

Complementing PECA, provisions within the Pakistan Penal Code (PPC) are also applicable to deepfake-related offenses. Section 500 addresses defamation, prescribing imprisonment for up to two years, fines, or both for individuals who harm another's reputation through false representations. Section 504 deals with intentional insults intended to provoke breaches of peace, with similar penalties. Moreover, Section 505 paragraph (1) letter (c) targets statements likely to incite offenses against different classes or communities, carrying imprisonment terms of up to seven years and fines.

The practical application of these laws is evident in recent legal actions. In February 2025, Punjab police registered three cases under PECA and relevant PPC sections against individuals accused of uploading AI-generated deepfake content targeting Punjab Chief Minister Maryam Nawaz. The accused allegedly disseminated fabricated and immoral videos and images on social media, aiming to defame the chief minister and incite public unrest. These cases highlight the authorities' proactive stance in addressing the misuse of deepfake technology in political contexts.[35]

---

[33] Sankar Rajeev, 'Thematic Analysis on the Indian Representation of People's Act, 1951', *International Journal of Human Rights and Constitutional Studies*, 7.3 (2020), pp. 209–32.
[34] Muhammad Awais Aslam, Abdullah Kanrani, and Muhammad Adil Shehroz, 'Regulating Misinformation or Silencing Dissent? A Constitutional Analysis of the PECA Amendments 2025', *The Critical Review of Social Sciences Studies*, 3.1 (2025), pp. 1809–15, <https://doi.org/10.59075/t1c1hz64>.
[35] Asif Chaudhry, 'Punjab Police File Three Cases under Peca for Deepfake Content', *Dawn*, 2025 <https://www.dawn.com/news/1893349> [accessed 22 March 2025].

### 3.3.3. Criminal Provisions in the US

In comparison, the United States (US) has been one of the most active countries in addressing the threat of deepfakes, although there is no comprehensive federal law. However, several states have passed relevant regulations. For example, Texas Senate Bill 751 makes it a crime to create a fake video with the intent of harming a candidate or influencing the outcome of an election. This offence is a class A misdemeanor and violators can be sentenced to up to one year in county jail and a fine of up to $4,000.[36] Furthermore, in another state, Indiana House Bill 1133 requires election campaign communications containing fake media to include a disclaimer, and candidates depicted in the fake media can file a civil lawsuit. On the other hand, Oregon Senate Bill 1571 requires disclosure of the use of synthetic media in election campaign communications. These regulations show serious efforts to protect election integrity from the threat of deepfakes.

Another example is Minnesota Statute Section 609.771 where it was enacted in 2023. It specifically addresses the use of deepfake technology in elections, criminalizing its dissemination within 90 days before an election if done without the depicted individual's consent and with the intent to harm a candidate or influence the election's outcome. The law defines a "deepfake" as media so realistic that a reasonable person would believe it depicts the speech or conduct of an individual who did not actually engage in such actions, produced primarily through technical means rather than physical or verbal impersonation.[37]

A violation occurs when a person knowingly or recklessly disseminates a deepfake with the intent to injure a candidate or sway election results, particularly within key timeframes such as 90 days before a political party's nominating convention or after the start of the absentee voting period. The penalties vary based on the severity of the violation. A first-time offense is considered a misdemeanor, carrying a sentence of up to 90 days in prison or a fine of up to $1,000. If the offense involves intent to incite violence or bodily harm, the penalty increases to a possible 364 days of imprisonment or a fine of up to $3,000. Repeat offenders within five years of a prior conviction face felony charges, with sentences of up to five years in prison or fines up to $10,000.[38]

Although there is no comprehensive federal law, several bills are being considered by the US Congress. The Deepfake Report Act of 2019 requires reporting on digital content forgery technologies. The Deepfakes Accountability Act aims to protect national security and provide legal protection to victims of deepfakes. The Defiance Act of 2024 improves the rights of victims of non-consensual deepfakes.[39] The Protecting Consumers from Deceptive AI Act requires disclosure of the origins of AI-generated content. This legislative project represents a serious effort to address the threat of deepfakes and protect election integrity.

The United States has shown greater legal responsiveness to deepfakes in elections, primarily due to its federalist structure, which allows states to experiment with targeted

[36] Matthew Bodi, 'The First Amendment Implications of Regulating Political Deepfakes', *Rutgers Computer & Technology Law Journal*, 47.1 (2021), p. 143.
[37] Jack Wampler, 'Deep Concern: Safeguarding Elections in the Age of Deepfakes', *Arizona Law Review*, 66.3 (2024), p. 815.
[38] Steven Carver, 'Election Integrity and the First Amendment: A Statutory Analysis of States' Regulations of Election Deepfakes', *Mitchell Hamline Law Review*, 50.3 (2024), p. 596.
[39] Alena Birrer and Natascha Just, 'What We Know and Don't Know about Deepfakes: An Investigation into the State of the Research and Regulatory Landscape', *New Media & Society*, 2024, <https://doi.org/10.1177/14614448241253138>.

legislation. States like Texas, Minnesota, and Oregon have passed election-specific deepfake laws, often prompted by public pressure, civil society advocacy, or election security concerns. Their laws incorporate forward-looking elements, such as clear definitions of synthetic media, time-bound restrictions (e.g., 90 days before an election), and intent-based thresholds. This legal innovation contrasts with countries like Indonesia, where the central legislative process is slower and often less responsive to emerging technological harms.

Indonesia can draw several lessons from these jurisdictions. First, the use of precise legal language to define deepfakes helps satisfy the principle of lex certa, reducing ambiguity for both citizens and law enforcement. Second, linking the offense to electoral manipulation grounds the law in a concrete public interest, enhancing its legitimacy. Third, procedural innovations—like mandatory disclaimers or civil remedies—expand enforcement beyond traditional criminal sanctions. Adopting a similar multi-pronged approach could enhance Indonesia's legal preparedness without waiting for national crises to prompt reform.

## 4. Conclusion

Deepfake technology is increasingly posing a challenge to the integrity of political campaigns and election processes around the world. As seen in cases in Indonesia, India, Pakistan, and the United States, the use of artificial intelligence-based synthetic media can manipulate public perception, spread disinformation, and undermine trust in democratic institutions. While some countries have legal frameworks to combat the misuse of deepfakes, there are still gaps in regulations that specifically address their impact on elections. In Indonesia, for example, handling deepfake cases still relies on broader legal provisions such as the ITE Law and the Personal Data Protection Law, but there is no specific regulation that explicitly targets AI-based election manipulation. Similarly, India and Pakistan rely on provisions in existing cyber and criminal laws, while the United States has taken steps at the state level to implement more specific regulations on the use of deepfakes in elections. These differences in approach demonstrate the need for a more comprehensive and coordinated legal framework to effectively address the deepfake challenge.

To reduce the negative impact of deepfakes on elections, strategic steps are needed, including the strengthening of regulations through the introduction of clear and specific legal provisions that define deepfakes, criminalize their malicious use in electoral contexts, and establish thresholds for liability. This includes updating existing laws such as the ITE Law and Election Law to explicitly cover AI-generated disinformation, setting clear standards for evidence and intent, and creating procedural mechanisms such as fast-track content removal during campaign periods.. Governments and election institutions must also work together with digital platforms to ensure that the spread of manipulative content can be prevented more effectively. In addition, international cooperation is needed given the global nature of this challenge. With a comprehensive and adaptive approach to technological developments, countries can be better prepared to face the threat of deepfakes and maintain public trust in the democratic process.

## References

Afifa, Laila, 'Kominfo Ministry Asserts Jokowi's Speech in Chinese Produced by Deepfake', *Tempo*, 2023 <https://en.tempo.co/read/1789306/kominfo-ministry-asserts-jokowis-speech-in-chinese-produced-by-deepfake>

Algamar, Muhammad Deckri, and Aliya Ilysia Irfana Ampri, 'Hak Untuk Dilupakan: Penghapusan Jejak Digital Sebagai Perlindungan Selebriti Anak Dari Bahaya Deepfake', *Jurnal Yustika: Media Hukum Dan Keadilan*, 25.01 (2022), pp. 25–39, <https://doi.org/10.24123/yustika.v25i01.5091>.

Almutairi, Zaynab, and Hebah Elgibreen, 'A Review of Modern Audio Deepfake Detection Methods: Challenges and Future Directions', *Algorithms*, 15.5 (2022), p. 155, <https://doi.org/10.3390/a15050155>.

Ardianto, Robi, 'Bawaslu Temukan 341 Dugaan Pelanggaran Konten Internet, Paling Banyak Soal Ujaran Kebencian', *Badan Pengawas Pemilu*, 2024 <https://bawaslu.go.id/id/berita/bawaslu-temukan-341-dugaan-pelanggaran-konten-internet-paling-banyak-soal-ujaran-kebencian>

Arora, Tanvi, and Rituraj Soni, 'A Review of Techniques to Detect the GAN-Generated Fake Images', in *Generative Adversarial Networks for Image-to-Image Translation* (Elsevier, 2021), pp. 125–59, <https://doi.org/10.1016/B978-0-12-823519-5.00004-X>

Birrer, Alena, and Natascha Just, 'What We Know and Don't Know about Deepfakes: An Investigation into the State of the Research and Regulatory Landscape', *New Media & Society*, 2024, <https://doi.org/10.1177/14614448241253138>.

Bodi, Matthew, 'The First Amendment Implications of Regulating Political Deepfakes', *Rutgers Computer & Technology Law Journal*, 47.1 (2021), p. 143

Carver, Steven, 'Election Integrity and the First Amendment: A Statutory Analysis of States' Regulations of Election Deepfakes', *Mitchell Hamline Law Review*, 50.3 (2024), p. 596

Chaudhry, Asif, 'Punjab Police File Three Cases under Peca for Deepfake Content', *Dawn*, 2025 <https://www.dawn.com/news/1893349> [accessed 22 March 2025]

Chen, Heather, 'AI "Resurrects" Long Dead Dictator in Murky New Era of Deepfake Electioneering', *CNN*, 2024 <https://www.cnn.com/2024/02/12/asia/suharto-deepfake-ai-scam-indonesia-election-hnk-intl/index.html>

Cindy, Mutia Annur, 'Ini Media Sosial Paling Banyak Digunakan Di Indonesia Awal 2024', *Databoks*, 2024 <https://databoks.katadata.co.id/datapublish/2024/03/01/ini-media-sosial-paling-banyak-digunakan-di-indonesia-awal-2024>

Datta, Abhinaba, and Subarno Banerjee, 'Unmasking Deepfakes-A Legal Perspective', *Jus Corpus Law Journal*, 4.4 (2023), pp. 336–58

Devina, Cindy Bella, Dissa Chandra Iswari, Go Christian Bryan Goni, and Devi Kimberly Lirungan, 'Tinjauan Hukum Kriminalisasi Berita Hoax: Menjaga Persatuan vs. Kebebasan Berpendapat', *Kosmik Hukum*, 21.1 (2021), p. 44, <https://doi.org/10.30595/kosmikhukum.v21i1.8874>.

Diakopoulos, Nicholas, and Deborah Johnson, 'Anticipating and Addressing the Ethical Implications of Deepfakes in the Context of Elections', *New Media & Society*, 23.7 (2021), pp. 2072–98, <https://doi.org/10.1177/1461444820925811>.

Enoch, Wesley, 'Vox Populi, Vox Dei (The Voice of the People Is the Voice of God)', *Voice and Speech Review*, 12.1 (2018), pp. 77–85, <https://doi.org/10.1080/23268263.2017.1398919>

Fadhilah, Almira Daisy Zahrah, and Sri Retnoningsih, 'Perancangan Kampanye Digital Melawan Disinformasi Melalui Artificial Intelligence Dan Deepfake Di Kalangan Pra

Lansia Usia 45-55 Tahun', *Prosiding FAD*, 3.2 (2024), pp. 1–17 <https://eproceeding.itenas.ac.id/index.php/fad/article/view/2943>

Farid, Hany, and Hans-Jakob Schindler, *Deep Fakes* (Konrad-Adenauer-Stiftung, 2020)

Gandrova, Shannon, and Ricky Banke, 'Penerapan Hukum Positif Indonesia Terhadap Kasus Kejahatan Dunia Maya Deepfake', *Madani: Jurnal Ilmiah Multidisiplin*, 1.10 (2023), pp. 650–57

Gaulkin, Thomas, 'The Campaign Volunteer Who Used AI to Help Swing Pakistan's Elections: Interview with Jibran Ilyas', *Bulletin of the Atomic Scientists*, 80.5 (2024), pp. 275–80, <https://doi.org/10.1080/00963402.2024.2388458>

Goodfellow, Ian, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, and others, 'Generative Adversarial Nets', *Advances in Neural Information Processing Systems*, 27 (2014), pp. 1–9

———, 'Generative Adversarial Networks', *Communications of the ACM*, 63.11 (2020), pp. 139–44

Halder, Debarati, 'A Retrospective Analysis of S. 66a: Could S. 66a of the Information Technology Act Be Reconsidered for Regulating'Bad Talk'in the Internet?', *Indian Student Law Review (ISLR)*, 3 (2015), pp. 91–118

International Institute for Democracy and Electoral Assistance, *Electoral Justice* (International IDEA, 2010)

Kaur, Achhardeep, Azadeh Noori Hoshyar, Vidya Saikrishna, Selena Firmin, and Feng Xia, 'Deepfake Video Detection: Challenges and Opportunities', *Artificial Intelligence Review*, 57.6 (2024), pp. 1–47, <https://doi.org/10.1007/s10462-024-10810-6>.

Kietzmann, Jan, Adam J Mills, and Kirk Plangger, 'Deepfakes: Perspectives on the Future "Reality" of Advertising and Branding', *International Journal of Advertising*, 40.3 (2021), pp. 473–85, <https://doi.org/10.1080/02650487.2020.1834211>.

Kolagati, Santosh, Thenuga Priyadharshini, and V. Mary Anita Rajam, 'Exposing Deepfakes Using a Deep Multilayer Perceptron – Convolutional Neural Network Model', *International Journal of Information Management Data Insights*, 2.1 (2022), p. 100054, <https://doi.org/10.1016/j.jjimei.2021.100054>

Meckel, Miriam, and Léa Steinacker, 'Hybrid Reality: The Rise of Deepfakes and Diverging Truths', *Morals & Machines*, 1.1 (2021), pp. 10–21

Muhammad Awais Aslam, Abdullah Kanrani, and Muhammad Adil Shehroz, 'Regulating Misinformation or Silencing Dissent? A Constitutional Analysis of the PECA Amendments 2025', *The Critical Review of Social Sciences Studies*, 3.1 (2025), pp. 1809–15, <https://doi.org/10.59075/t1c1hz64>.

Pawelec, Maria, 'Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions', *Digital Society*, 1.2 (2022), p. 19, <https://doi.org/10.1007/s44206-022-00010-6>.

Perdana, Aditya, and Delia Wildianti, 'Narasi Kampanye Dan Media Sosial Dalam Pemilu Presiden Dan Wakil Presiden Tahun 2019', *Jurnal Bawaslu DKI*, 2018, pp. 21–39

Rajeev, Sankar, 'Thematic Analysis on the Indian Representation of People's Act, 1951', *International Journal of Human Rights and Constitutional Studies*, 7.3 (2020), pp. 209–32

Santiko, Jetrin Arfan, and Syaiful Bahri, '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 (2024), pp. 13215–31

Siregar, Runi Hilda Fadlani, and Muhammad Vicky Afris Suryono, 'Towards Transparent and Secure Elections: The Legal Landscape of Digital Electoral Systems in Indonesia', *E-Justice: Journal of Law and Technology*, 1.2 (2025), pp. 15–30

Sumanjeet, 'The State of E-commerce Laws in India: A Review of Information Technology Act', *International Journal of Law and Management*, 52.4 (2010), pp. 265–82, <https://doi.org/10.1108/17542431011059322>.

Wampler, Jack, 'Deep Concern: Safeguarding Elections in the Age of Deepfakes', *Arizona Law Review*, 66.3 (2024), p. 815

Westerlund, Mika, 'The Emergence of Deepfake Technology: A Review', *Technology Innovation Management Review*, 9.11 (2019), pp. 39–52

Wojewidka, John, 'The Deepfake Threat to Face Biometrics', *Biometric Technology Today*, 2020.2 (2020), pp. 5–7, <https://doi.org/10.1016/S0969-4765(20)30023-0>.

Wuragil, Sarno, and Widayati Widayati, 'Development of Democracy & Phenomenon of Single Candidate in Regional Election (Pilkada)', *Law Development Journal*, 3.1 (2021), pp. 120–29, <https://doi.org/10.30659/ldj.3.1.120-129>.

Yarnis, Yarnis, and Nani Nurani Muksin, 'Semiotics Analysis of'Gemoy'Animations Political Communication Strategy in Efforts to Change Prabowo-Gibran's Branding', *Lentera: Jurnal Ilmu Dakwah Dan Komunikasi*, 2024, pp. 1–23, <https://doi.org/10.21093/lentera.v8i1.8069>>.