

Deepfake Technology and Electoral Integrity: A Socio-Legal Analysis of Digital Manipulation and Democratic Rights in Indonesia

Nanda Pratama^{1*}, Bilaly Sangare²
¹ Master of Laws, Tanjungpura University, Indonesia
² Department of Islamic Economics and Law, Faculty of Islamic Economics and Law, Istanbul Sabahattin Zaim University, Istanbul
*Corresponding author: n.pratama@gmail.com

ARTICLE INFO	ABSTRACT
Article history Received: 05 January, 2026 Revised: 09 January, 2026 Accepted: 25 May, 2026 Published: 31 May, 2026 Keywords Deepfake Technology; Electoral Integrity; Digital Disinformation; Democratic Rights; Socio-Legal Analysis;  License by CC-BY-SA Copyright © 2026, The Author(s).	The rapid development of deepfake technology has generated significant challenges for electoral integrity, democratic legitimacy, and digital rights protection in Indonesia. During the 2024 Indonesian presidential election, the increasing circulation of AI-generated political content intensified concerns regarding disinformation, voter manipulation, and the weakening of public trust in democratic institutions. This study examines the socio-legal implications of deepfake technology in Indonesian electoral processes and evaluates the adequacy of existing legal frameworks in addressing AI-driven political manipulation. The research employs a qualitative socio-legal approach using statutory analysis, conceptual analysis, and thematic analysis of academic literature, legal instruments, and recent electoral developments. The findings demonstrate that Indonesian regulations, including the Electronic Information and Transactions Law and the Personal Data Protection Law, remain fragmented and insufficient to comprehensively regulate deepfake-based electoral disinformation. Deepfake dissemination during political campaigns creates substantial risks to democratic participation, electoral fairness, and informational integrity, particularly through social media amplification and algorithmic targeting. This article argues that Indonesia requires a specific and integrated regulatory framework combining electoral law reform, digital platform accountability, and AI governance mechanisms to protect democratic rights in the digital era. The study contributes to contemporary socio-legal debates concerning artificial intelligence, cyber democracy, and electoral governance in emerging democracies.
How to cite: Pratama, N., & Sangare, B. (2026). Deepfake Technology and Electoral Integrity: A Socio-Legal Analysis of Digital Manipulation and Democratic Rights in Indonesia. <i>Justicia Insight</i>, 2(2), 85-97. https://doi.org/10.70716/justin.v2i2.385	

INTRODUCTION

The expansion of artificial intelligence technology has transformed the global digital communication landscape, including political communication and electoral campaigns. One of the most concerning developments is the emergence of deepfake technology, which enables the creation of highly realistic manipulated audio, video, and visual content through machine learning systems (Westerlund, 2019). Deepfakes increasingly threaten democratic systems because they can spread political disinformation, distort public perception, manipulate voter behavior, and undermine institutional legitimacy (Chesney & Citron, 2019). The rapid circulation of synthetic media through social media platforms has intensified concerns regarding post-truth politics, declining public trust, and the erosion of democratic accountability (Bennett & Livingston, 2018). Several recent studies demonstrate that political deepfakes possess measurable effects on voter attitudes, political trust, and electoral participation, especially during election periods characterized by high polarization and digital dependence (Dobber et al., 2021; Vaccari & Chadwick, 2020). In many democratic states, deepfake technology has therefore emerged not merely as a technological issue, but as a serious socio-legal challenge affecting electoral integrity and democratic rights.

In Indonesia, the risks associated with deepfake technology have become increasingly relevant during the 2024 presidential election and the broader expansion of cyber democracy. Indonesia represents one of the world's largest digital democracies, with social media serving as a primary arena for political campaigns, public opinion formation, and electoral mobilization (Nugroho & Fahadayna, 2025). The rapid increase in digital political engagement has simultaneously increased vulnerabilities to online disinformation, black campaigns, and AI-generated political manipulation. Reports and scholarly analyses

concerning the 2024 election identified growing concerns regarding digital electoral fraud, misinformation campaigns, and manipulative online narratives capable of influencing public trust and democratic legitimacy (Alghan et al., 2025; Karim et al., 2025). The dissemination of manipulated political content through social media platforms creates significant legal challenges because Indonesian electoral law and cyber law frameworks were originally designed to regulate conventional digital misinformation rather than AI-generated synthetic media. Consequently, the emergence of deepfake technology has exposed substantial regulatory gaps in Indonesia's legal system concerning electoral protection, personal data security, and digital accountability.

Recent global developments further demonstrate that deepfake technology has become an increasingly urgent concern within contemporary electoral governance. Several democratic jurisdictions have begun introducing specific regulatory responses to synthetic political media due to growing fears regarding AI-driven electoral interference. The European Union, through the AI Act and Digital Services Act, has introduced transparency obligations and risk-based governance mechanisms for artificial intelligence systems capable of manipulating public information environments (Veale & Borgesius, 2021; Helberger & Diakopoulos, 2023). Similarly, several states in the United States, including California and Texas, have enacted election-related deepfake regulations prohibiting deceptive synthetic political media during electoral periods (Kietzmann et al., 2020; Chesney & Citron, 2019). China has also adopted synthetic media labeling obligations requiring AI-generated content to contain identifiable disclosure markers (Roberts et al., 2021). These comparative developments indicate that the regulation of political deepfakes has shifted from a purely technological issue toward an essential component of democratic governance and electoral integrity protection in digital societies.

Despite these international regulatory developments, Indonesia still lacks a comprehensive legal framework specifically addressing AI-generated electoral manipulation. Existing studies concerning Indonesian electoral law primarily focus on conventional cyber misinformation, hate speech, and social media violations without comprehensively examining the emerging risks posed by generative artificial intelligence in electoral contexts. Consequently, there remains limited socio-legal scholarship integrating deepfake technology, electoral integrity, democratic rights, and platform governance within the Indonesian legal system. This article therefore addresses a significant research gap by developing an integrated socio-legal analysis concerning the implications of synthetic political media for democratic resilience and electoral governance in Indonesia's evolving digital democracy.

Existing scholarship concerning deepfake technology generally develops within three dominant perspectives. The first perspective focuses on the technological dimensions of deepfake production and detection systems, particularly machine learning mechanisms, forensic identification, and synthetic media classification (Li et al., 2020; Mahmud & Sharmin, 2021). The second perspective examines the political and communication impacts of deepfakes, including disinformation dissemination, polarization, electoral manipulation, and democratic destabilization (Freelon & Wells, 2020; Hameleers et al., 2022; Pawelec, 2022). The third perspective discusses legal and regulatory issues surrounding artificial intelligence governance, privacy protection, and cyber law enforcement (Armiwulan et al., 2024; Chairani et al., 2024; Laza & Karo, 2023). Several scholars also emphasize that current legal systems remain inadequately prepared to respond to AI-generated disinformation because existing regulations often fail to distinguish between conventional misinformation and synthetic digital manipulation (Citron, 2019; Westerlund, 2021). Although these studies provide important contributions, most discussions remain concentrated on Western political systems or general AI governance debates. Limited studies specifically examine how deepfake technology affects electoral integrity within Indonesia's socio-legal and democratic context.

This article addresses that research gap by analyzing the relationship between deepfake technology, electoral integrity, and democratic rights in Indonesia through a socio-legal perspective. Unlike previous studies that primarily discuss technological detection or general cybercrime regulation, this article focuses on the insufficiency of Indonesian electoral and digital governance frameworks in addressing AI-driven political manipulation during democratic processes. This study argues that deepfake technology creates multidimensional threats to democratic participation, legal certainty, electoral fairness, and public trust because synthetic political content can rapidly influence voters before verification mechanisms function effectively. The article further argues that Indonesia's current legal instruments, including the Law on Electronic Information and Transactions and the Personal Data Protection Law, remain fragmented and

reactive in responding to deepfake-based electoral disinformation. By integrating socio-legal analysis with contemporary debates on digital democracy and AI governance, this article contributes to the development of legal scholarship concerning electoral regulation, cyber governance, and democratic resilience in emerging digital democracies.

This study aims to analyze the socio-legal implications of deepfake technology for electoral integrity in Indonesia and evaluate the adequacy of existing legal frameworks in addressing AI-generated political manipulation. The article also seeks to formulate legal and regulatory approaches capable of strengthening democratic rights protection in the era of artificial intelligence and digital political communication.

This study further employs the theoretical perspectives of digital constitutionalism and democratic resilience to evaluate the relationship between technological disruption and democratic protection within contemporary electoral systems. Digital constitutionalism emphasizes the necessity of adapting constitutional values, civil liberties, and democratic safeguards to increasingly digitized governance environments, while democratic resilience theory highlights institutional capacities required to protect democratic legitimacy against disinformation and technological manipulation. These theoretical approaches provide an analytical foundation for examining how Indonesian electoral law and digital governance mechanisms should evolve in response to emerging artificial intelligence threats (Celeste, 2019; Balkin, 2020; Bennett & Livingston, 2018).

RESEARCH METHOD

This study employs qualitative legal research using a socio-legal approach to examine the implications of deepfake technology for electoral integrity and democratic rights in Indonesia. The socio-legal approach was selected because the research problem involves not only normative legal analysis but also broader social, political, and technological dimensions influencing democratic governance in the digital era. The study focuses on the interaction between artificial intelligence, digital political communication, and Indonesian electoral law during the period surrounding the 2024 Indonesian general election. The material object of this research consists of legal norms, public policy frameworks, and socio-political developments related to deepfake dissemination in electoral contexts. A qualitative approach was considered appropriate because the study seeks to interpret legal gaps, institutional challenges, and democratic risks arising from AI-generated political disinformation rather than quantitatively measuring electoral behavior. The research design refers to qualitative and socio-legal research principles developed by Creswell and Creswell (2018) and Suharsimi Arikunto (2012).

This research additionally applies statute, conceptual, and comparative legal approaches to strengthen the socio-legal analysis framework (Celeste, 2019; Balkin, 2020; Bennett & Livingston, 2018). The statute approach was employed to examine Indonesian legal instruments relevant to electoral governance, electronic information regulation, and personal data protection. The conceptual approach was used to analyze theoretical discussions concerning democratic rights, digital constitutionalism, electoral integrity, and artificial intelligence governance. Meanwhile, the comparative approach enabled the study to evaluate regulatory developments concerning deepfake governance in several jurisdictions, including the European Union, the United States, China, and Singapore. These comparative perspectives were incorporated to identify potential regulatory models relevant to Indonesia's evolving digital electoral system.

The study utilizes both primary and secondary data sources. Primary legal materials include Indonesian laws and regulations relevant to digital governance and elections, particularly the Law on Electronic Information and Transactions, the Personal Data Protection Law, and legal provisions concerning electoral campaigns and cyber activities. Secondary data consist of peer-reviewed journal articles, academic books, conference proceedings, and scientific reports discussing deepfake technology, electoral disinformation, democratic integrity, cyber law, and artificial intelligence governance. The study also examines recent scholarly discussions regarding the 2024 Indonesian election and the increasing use of social media in political campaigns. Data collection was conducted through document analysis and literature review techniques by systematically identifying, categorizing, and reviewing relevant legal documents and academic publications connected to the research objectives.

The literature selection process prioritized peer-reviewed international journal articles indexed in Scopus and Web of Science published between 2018 and 2026 to ensure the relevance and contemporary

validity of the discussion concerning artificial intelligence and electoral disinformation. The study also incorporated selected Indonesian legal scholarship and policy documents specifically related to electoral governance, cyber law, and deepfake regulation. Data credibility was strengthened through source triangulation involving legal documents, academic publications, policy reports, and contemporary electoral developments associated with the 2024 Indonesian presidential election (Creswell & Creswell, 2018; Flick, 2018).. This triangulation process enabled the study to critically evaluate the consistency between normative legal frameworks and practical democratic challenges emerging within digital political communication environments.

The collected data were analyzed using thematic analysis to identify recurring patterns, legal challenges, and socio-political implications related to deepfake-based electoral manipulation. The thematic analysis framework follows the analytical principles developed by Braun and Clarke (2006), including data familiarization, coding, theme identification, interpretation, and synthesis. The analysis was further guided by socio-legal perspectives concerning digital democracy, disinformation, and platform governance developed by Bennett and Livingston (2018), Helberger et al. (2018), and Pawelec (2022). These frameworks enabled the study to critically assess how existing Indonesian legal instruments respond to emerging threats posed by synthetic political media and how regulatory limitations affect democratic rights protection. Through this analytical framework, the study evaluates the adequacy of current legal mechanisms while formulating broader legal and policy implications concerning electoral governance in the era of artificial intelligence.

RESULTS AND DISCUSSION

Deepfake Technology and the Transformation of Electoral Disinformation

The development of artificial intelligence has fundamentally transformed the character of political disinformation in contemporary democratic systems. Unlike conventional misinformation, deepfake technology enables the production of highly realistic synthetic audio and visual content capable of imitating public figures, political candidates, journalists, and government institutions with a high degree of accuracy (Westerlund, 2019). Advances in machine learning, generative adversarial networks, and synthetic media production have significantly reduced the technical barriers required to create manipulated political content, allowing deepfake dissemination to become increasingly accessible and scalable (Mahmud & Sharmin, 2021). The emergence of deepfakes therefore represents a transition from text-based digital misinformation toward immersive audiovisual manipulation capable of influencing political perception more effectively than conventional propaganda.

Several studies demonstrate that deepfake content possesses stronger psychological and political effects than traditional forms of fake news because audiovisual materials are often perceived as more credible by audiences (Vaccari & Chadwick, 2020). Experimental studies further indicate that manipulated political videos can influence voter attitudes, increase uncertainty regarding factual information, and reduce trust in democratic institutions (Dobber et al., 2021). Hameleers et al. (2022) found that deepfake political narratives distributed through social media platforms create significant emotional reactions and contribute to political polarization, particularly when disseminated in highly contested electoral contexts. Similarly, Dan (2025) argues that political deepfakes can directly threaten democratic stability because manipulated audiovisual content spreads rapidly before journalistic verification mechanisms are able to counter disinformation narratives effectively.

The increasing sophistication of deepfake technology also intensifies broader concerns regarding post-truth politics and digital disinformation ecosystems. Bennett and Livingston (2018) explain that contemporary disinformation operates through decentralized digital communication structures in which algorithmic amplification, social media engagement, and emotional political narratives weaken public consensus regarding factual truth. Deepfake dissemination therefore does not occur in isolation, but rather functions within a wider digital environment characterized by polarization, political distrust, and viral information circulation. Lazer et al. (2018) similarly emphasize that fake news ecosystems thrive because digital platforms incentivize sensational and emotionally charged content capable of generating engagement regardless of factual accuracy. Consequently, deepfake technology amplifies the structural vulnerabilities already present within digital democracies.

Indonesia demonstrates many of these vulnerabilities due to the rapid expansion of internet penetration and social media dependence in political communication. The transformation of electoral campaigns into digital spaces has increased exposure to online propaganda, misinformation, and AI-generated manipulation. Nugroho and Fahadayna (2025) explain that Indonesia's cyber democracy increasingly relies upon digital political participation, making electoral processes more vulnerable to algorithmic disinformation campaigns and cyber manipulation. During the 2024 presidential election, concerns regarding digital electoral fraud and online political manipulation intensified significantly, particularly concerning misleading political narratives distributed through social media platforms (Alghan et al., 2025). In this context, deepfake technology creates additional risks because manipulated audiovisual materials can rapidly shape voter perception before verification or legal intervention mechanisms become effective.

Empirical concerns regarding AI-generated political manipulation became increasingly visible during the 2024 Indonesian presidential election. Several political campaign materials circulated through TikTok, Instagram, and YouTube utilized artificial intelligence-generated visual editing, synthetic voice modification, and digitally manipulated political narratives designed to enhance candidate popularity and emotional voter engagement (Imran et al., 2025; Karim et al., 2025). Public discussions also emerged concerning AI-generated campaign imagery portraying political candidates in idealized or historically reconstructed scenarios intended to strengthen symbolic political legitimacy. Although not all materials constituted fully fabricated malicious deepfakes, these developments demonstrated the increasing normalization of synthetic political communication within Indonesian electoral campaigns.

The Indonesian Ministry of Communication and Information Technology (Kominfo) and electoral supervisory institutions also reported substantial increases in online misinformation, manipulated political narratives, and digital propaganda during the 2024 election period (Alghan et al., 2025; Paskarina et al., 2025). The rapid dissemination of viral political content through algorithmically amplified social media ecosystems complicated fact-checking efforts and institutional monitoring mechanisms. Under these conditions, deepfake technology possesses the potential to accelerate electoral disinformation by producing highly persuasive audiovisual materials capable of shaping political perception before verification procedures can effectively respond (Helberger et al., 2018; Tucker et al., 2018). These empirical developments demonstrate that Indonesia's electoral system has entered a new phase of technological vulnerability associated with artificial intelligence-driven political communication.

The risks associated with political deepfakes are not limited to misinformation alone. Deepfake dissemination may also produce long-term institutional consequences by eroding public trust in democratic procedures and information systems. Persily (2017) argues that digital communication technologies increasingly challenge the ability of democratic institutions to maintain informational integrity during elections. Similarly, Judge and Korhani (2020) emphasize that electoral integrity depends upon equal access to accurate information and the ability of citizens to evaluate political communication without systematic manipulation. When deepfake technology distorts political information environments, voters face increasing difficulty distinguishing authentic political communication from fabricated synthetic content. This condition weakens democratic deliberation and creates uncertainty regarding the legitimacy of electoral outcomes.

Recent studies further indicate that political deepfakes may contribute to the delegitimization of political actors and democratic institutions. Hameleers et al. (2026) found that radical political deepfakes successfully influenced public perception against targeted political figures in experimental settings conducted in the United States and the Netherlands. Similar concerns emerge in Indonesia, where political polarization and identity-based political narratives have intensified digital hostility during electoral contests. Under such conditions, deepfake technology can function as a tool for black campaigns, reputational attacks, and political manipulation designed to influence electoral behavior and weaken public trust in democratic institutions. Karim et al. (2025) explain that black campaign practices conducted through social media have become increasingly difficult to regulate due to the speed and anonymity of digital dissemination mechanisms.

The transformation of electoral disinformation through deepfake technology therefore creates substantial socio-legal challenges for democratic governance. Deepfakes undermine not only individual reputations and privacy rights, but also collective democratic rights associated with fair elections, informed

political participation, and public trust. Pawelec (2022) argues that synthetic audiovisual disinformation threatens several core democratic functions, including public deliberation, electoral accountability, and institutional legitimacy. Consequently, deepfake regulation should not be understood solely as a cybercrime issue, but rather as an essential component of democratic rights protection in the digital era.

Legal Challenges of Deepfake Regulation in Indonesia

The rapid expansion of deepfake technology has exposed significant limitations within Indonesia's legal framework concerning digital governance and electoral protection. Existing Indonesian regulations primarily address conventional cybercrime, electronic information misuse, defamation, and personal data violations rather than AI-generated synthetic political manipulation. Consequently, current legal instruments remain fragmented and insufficient to comprehensively regulate deepfake dissemination during electoral processes. This regulatory gap creates substantial legal uncertainty concerning accountability, criminal liability, evidentiary standards, and institutional enforcement mechanisms in cases involving political deepfakes.

Indonesia currently relies on several legal instruments potentially applicable to deepfake-related offenses, including the Law on Electronic Information and Transactions and the Personal Data Protection Law. However, these regulations were enacted before the widespread emergence of generative artificial intelligence technologies and therefore lack explicit provisions regarding synthetic media manipulation. Arvitto (2025) explains that the Indonesian legal framework remains normatively inadequate because existing regulations focus primarily on unlawful electronic information dissemination without specifically addressing the technical and political dimensions of deepfake production. Similar arguments are presented by Chairani et al. (2024), who emphasize the urgency of establishing explicit legal regulations concerning deepfake misuse due to increasing risks to privacy rights, public trust, and democratic stability.

The absence of specific legal definitions concerning deepfake technology also creates difficulties in criminal law enforcement. Indonesian criminal law traditionally depends upon identifiable elements of intent, causation, and direct unlawful conduct. However, deepfake dissemination often involves anonymous actors, transnational digital infrastructures, and algorithmic amplification processes that complicate legal attribution and evidentiary procedures. Nurkholisah et al. (2025) argue that deepfake-related cybercrime presents serious challenges for Indonesian criminal law because synthetic media manipulation does not fit neatly within conventional legal categories governing fraud, defamation, or electronic misinformation. Consequently, law enforcement institutions face practical limitations in identifying perpetrators, verifying manipulated content, and determining appropriate criminal sanctions.

The legal challenges become more complex within electoral contexts because political deepfakes directly affect democratic rights and electoral fairness. Indonesian electoral law contains provisions concerning black campaigns, misinformation, and electoral violations, yet these provisions were designed primarily to regulate traditional campaign practices and conventional digital content. Pirmansyah et al. (2023) note that electronic electoral law enforcement in Indonesia remains institutionally weak due to limited technological capacity, fragmented regulations, and difficulties monitoring digital political communication. Deepfake dissemination intensifies these institutional weaknesses because manipulated audiovisual content can spread rapidly across multiple digital platforms before electoral supervisory institutions are able to intervene effectively.

The role of social media platforms further complicates legal regulation and accountability mechanisms. Deepfake content often circulates through algorithmically driven platforms prioritizing engagement, virality, and emotional political content. Helberger et al. (2018) explain that online platform governance increasingly requires cooperative regulatory responsibility because digital intermediaries possess substantial influence over information dissemination processes. However, Indonesian legal frameworks still provide limited obligations for digital platforms concerning AI-generated political disinformation detection, removal, or moderation. As a result, platform governance mechanisms remain inconsistent and largely dependent upon voluntary moderation policies rather than enforceable legal standards.

The legal implications of deepfake dissemination also intersect with personal data protection and privacy rights. Deepfake technology frequently utilizes biometric data, facial images, voice recordings, and audiovisual materials without consent from targeted individuals. Jufri and Putra (2021) argue that deepfake technology creates serious risks to personal data protection because synthetic content production often

involves unauthorized data extraction and identity replication. Laza and Karo (2023) similarly explain that Indonesia's Personal Data Protection Law remains limited in addressing AI-generated identity manipulation because the regulation primarily focuses on conventional data processing violations rather than synthetic identity reproduction. Consequently, victims of political deepfakes may encounter substantial legal barriers when seeking remedies for reputational harm, privacy violations, or electoral manipulation.

Comparative international developments further demonstrate that many democratic states remain unprepared to regulate deepfake-related electoral threats effectively. Łabuz and Nehring (2024) explain that recent election campaigns in Europe revealed increasing vulnerabilities associated with synthetic political media and AI-driven disinformation. Soñeca (2026) similarly identifies deepfakes as emerging threats to both national and parliamentary elections due to their capacity to manipulate voter perception and destabilize democratic trust. These international developments indicate that Indonesia's regulatory difficulties reflect broader global challenges concerning artificial intelligence governance, digital democracy, and electoral integrity.

Comparative regulatory developments demonstrate that several jurisdictions have begun recognizing deepfake dissemination as a distinct threat requiring specialized electoral and digital governance mechanisms. The European Union has adopted a risk-based artificial intelligence governance approach through the AI Act, requiring transparency obligations for AI-generated content and imposing stricter responsibilities upon digital platforms operating high-risk AI systems (Veale & Borgesius, 2021; Helberger & Diakopoulos, 2023).. In the United States, multiple state-level regulations prohibit the dissemination of materially deceptive deepfake political advertisements during election periods unless accompanied by explicit disclosure labels (Chesney & Citron, 2019; Kietzmann et al., 2020). China has similarly introduced mandatory synthetic media identification requirements obligating digital platforms and content creators to disclose AI-generated audiovisual materials (Roberts et al., 2021). Singapore has strengthened digital misinformation regulation through platform-centered accountability mechanisms allowing government intervention against online falsehoods capable of threatening public order and democratic stability (Tambini, 2017).

These comparative developments reveal that effective deepfake governance increasingly depends upon integrated regulatory approaches combining electoral law, cyber governance, platform accountability, and artificial intelligence oversight. Indonesia, however, continues relying upon fragmented legal provisions lacking explicit obligations concerning synthetic political media transparency, platform moderation responsibility, and election-period AI governance. Consequently, Indonesian electoral regulation remains comparatively underdeveloped in addressing emerging threats associated with AI-driven electoral disinformation and algorithmic political manipulation.

The current Indonesian legal framework therefore demonstrates three major weaknesses. First, existing regulations lack explicit normative recognition of deepfake technology as a distinct legal category requiring specialized regulation. Second, institutional enforcement mechanisms remain technologically and procedurally inadequate for responding to rapidly evolving AI-generated disinformation. Third, Indonesia lacks integrated governance mechanisms connecting electoral supervision, cyber regulation, artificial intelligence governance, and platform accountability. Without comprehensive regulatory reform, deepfake technology will continue creating significant threats to democratic rights, legal certainty, and electoral legitimacy in Indonesia.

Deepfakes, Democratic Rights, and Electoral Integrity

Electoral integrity constitutes a fundamental element of democratic governance because fair elections depend upon equal political participation, transparent information circulation, and public trust in institutional processes. The emergence of deepfake technology threatens these democratic foundations by creating manipulated political realities capable of distorting voter judgment and influencing electoral outcomes. Deepfakes therefore represent not only a technological problem, but also a direct challenge to democratic rights and constitutional principles associated with political participation, informational access, and electoral fairness.

Democratic systems require voters to make political decisions based on reliable and verifiable information. However, deepfake dissemination weakens informational integrity by introducing fabricated audiovisual materials that appear authentic to public audiences. Tandoc et al. (2018) explain that fake news and manipulated information undermine democratic deliberation because citizens become increasingly

unable to distinguish factual communication from false narratives. Deepfake technology intensifies this condition because manipulated audiovisual content often possesses higher persuasive power than text-based misinformation. As a result, synthetic political media can influence public opinion rapidly, particularly during emotionally charged electoral periods characterized by polarization and partisan conflict.

The Indonesian electoral environment demonstrates significant vulnerability to such manipulation due to the dominant role of social media in political communication. Tucker et al. (2018) emphasize that social media ecosystems contribute to political polarization and disinformation amplification because digital algorithms prioritize emotionally engaging content. Similar patterns have emerged in Indonesia, where electoral campaigns increasingly rely on digital mobilization strategies and viral political narratives. Sharma et al. (2022) found that online engagement with political disinformation during election periods tends to intensify through coordinated digital interaction networks, further accelerating the spread of manipulated content. Within this environment, deepfake technology becomes an efficient instrument for political actors seeking to manipulate voter emotions, discredit opponents, or shape public narratives strategically.

The circulation of political deepfakes also affects democratic trust at institutional and societal levels. Pooja Raj (2025) argues that deepfake technology significantly damages democratic trust because repeated exposure to manipulated political content creates public skepticism toward authentic information sources. When voters lose confidence in audiovisual evidence, political communication becomes vulnerable to systematic uncertainty and cynicism. This phenomenon is commonly described as the “liar’s dividend,” in which political actors deny authentic evidence by claiming that damaging materials are fabricated deepfakes (Chesney & Citron, 2019). Consequently, deepfake technology simultaneously enables the spread of false information and weakens public confidence in genuine political accountability mechanisms.

The implications for electoral integrity are particularly serious during highly competitive elections. Ranka et al. (2024) explain that deepfakes threaten election integrity because manipulated political media can influence voter behavior, suppress political participation, and destabilize electoral legitimacy before fact-checking institutions respond effectively. Experimental evidence also demonstrates that political deepfakes influence political attitudes and increase uncertainty regarding electoral information environments (Dobber et al., 2021). In Indonesia, where digital literacy disparities remain significant across regions and demographic groups, these risks become even more substantial. Deepfake dissemination may therefore disproportionately affect vulnerable voters who possess limited capacity to verify manipulated political content independently.

The problem also extends to institutional trust concerning electoral administration systems. Paskarina et al. (2025) explain that public trust constitutes an essential component of electoral legitimacy, particularly within increasingly digitized election systems such as electronic recapitulation processes. When deepfake disinformation targets electoral institutions, election officials, or vote-counting procedures, public confidence in electoral outcomes may decline substantially. Such conditions increase the potential for political instability, social conflict, and delegitimization of democratic institutions after elections.

Indonesia’s democratic framework therefore requires stronger legal and institutional protections capable of addressing emerging AI-driven electoral threats. Chen and Yuan (2023) argue that contemporary rule-of-law systems must adapt to technological transformations by developing intelligent legal governance mechanisms capable of regulating emerging digital risks. This approach is particularly relevant for Indonesia because existing electoral governance structures remain oriented toward conventional campaign violations rather than synthetic political manipulation. Effective regulation should therefore integrate electoral law reform, digital platform accountability, cyber governance, and AI ethics principles into a coherent legal framework.

Several policy approaches may strengthen democratic resilience against deepfake-related electoral manipulation. First, Indonesia requires explicit legal recognition of deepfake-based electoral offenses within electoral legislation and cyber law frameworks. Second, regulatory institutions should establish mandatory obligations for digital platforms to identify, label, and remove manipulated political content during election periods. Third, public digital literacy programs must be strengthened to improve voter capacity in identifying synthetic political media and disinformation narratives. Fourth, cross-sector cooperation among electoral commissions, cybersecurity institutions, civil society organizations, and

technology platforms is necessary to create rapid response mechanisms against AI-driven electoral manipulation.

Ultimately, protecting electoral integrity in the digital era requires balancing technological innovation with democratic accountability and legal certainty. Deepfake technology illustrates how artificial intelligence can simultaneously advance digital communication while threatening fundamental democratic rights. Indonesia therefore faces an urgent need to develop adaptive socio-legal governance mechanisms capable of protecting democratic participation, public trust, and constitutional electoral principles within increasingly complex digital information environments.

Toward an Integrated Electoral AI Governance Framework in Indonesia

The increasing risks associated with deepfake-based electoral manipulation demonstrate the urgent necessity of establishing an integrated electoral artificial intelligence governance framework in Indonesia (Pawelec, 2022; Chen & Yuan, 2023). Existing legal instruments remain fragmented because electoral regulation, cyber governance, personal data protection, and platform accountability operate through separate institutional mechanisms lacking coordinated enforcement structures. Consequently, Indonesia requires a comprehensive regulatory model capable of responding adaptively to emerging forms of AI-driven political disinformation while simultaneously protecting democratic freedoms and constitutional rights.

An integrated electoral AI governance framework should contain several essential regulatory components. First, Indonesian electoral law should explicitly recognize deepfake-based political manipulation as a distinct category of electoral violation accompanied by clear legal definitions, evidentiary standards, and institutional enforcement procedures. Such recognition is necessary to reduce legal ambiguity and strengthen accountability mechanisms concerning synthetic political media dissemination during electoral periods. Second, digital platforms operating within Indonesia should be subjected to mandatory transparency obligations requiring the identification, labeling, and rapid removal of manipulated political content capable of misleading voters or threatening electoral integrity (Helberger et al., 2018; Westerlund, 2021).

Third, Indonesia requires institutional coordination mechanisms involving the General Elections Commission, the Election Supervisory Board, cybersecurity agencies, digital platform providers, and independent fact-checking organizations. Coordinated governance structures would enable rapid response procedures against viral deepfake dissemination during election periods while strengthening digital forensic verification capacities. Fourth, public digital literacy programs should be expanded systematically to improve societal resilience against AI-generated political disinformation. Digital literacy constitutes an essential democratic safeguard because technological regulation alone cannot fully prevent manipulative political narratives from influencing public perception (Tucker et al., 2018; Lazer et al., 2018).

Finally, regulatory reform concerning deepfake governance should remain consistent with democratic principles, freedom of expression, and constitutional protections. Excessively restrictive regulation may create risks of political censorship or arbitrary state intervention within digital communication spaces. Therefore, Indonesia's future AI governance framework must balance technological accountability with democratic freedoms through transparent, proportionate, and rights-based regulatory mechanisms. Such an approach would strengthen democratic resilience while ensuring that artificial intelligence development remains compatible with electoral integrity and constitutional democracy in the digital era (Balkin, 2020; Celeste, 2019).

CONCLUSION

This study demonstrates that deepfake technology has emerged as a serious socio-legal threat to electoral integrity and democratic rights in Indonesia. The rapid development of artificial intelligence and synthetic media technologies has transformed the nature of political disinformation from conventional text-based misinformation into highly persuasive audiovisual manipulation capable of influencing voter perception, political trust, and democratic participation. The findings reveal that deepfake dissemination during electoral processes creates multidimensional risks affecting informational integrity, public confidence in democratic institutions, electoral fairness, and the legitimacy of political outcomes. In Indonesia's increasingly digital electoral environment, social media platforms and algorithm-driven

communication systems intensify the speed and reach of manipulated political content, making democratic systems more vulnerable to coordinated disinformation campaigns and AI-driven political manipulation. The study further finds that Indonesia's current legal framework remains fragmented and insufficient to respond effectively to these emerging challenges. Existing regulations, including the Law on Electronic Information and Transactions and the Personal Data Protection Law, primarily address conventional digital violations and do not comprehensively regulate synthetic political media, deepfake dissemination, or AI-based electoral interference. As a result, legal enforcement mechanisms continue facing significant difficulties concerning attribution, evidence verification, platform accountability, and institutional coordination.

This article contributes to contemporary socio-legal scholarship by positioning deepfake technology not merely as a technological or cybercrime issue, but as a broader democratic governance problem directly connected to constitutional rights, electoral justice, and digital accountability. The study expands existing discussions concerning artificial intelligence governance by emphasizing the relationship between deepfake regulation and democratic resilience within emerging digital democracies such as Indonesia. The findings indicate that protecting electoral integrity in the era of artificial intelligence requires an integrated regulatory framework combining electoral law reform, cyber governance mechanisms, platform accountability obligations, and personal data protection standards. The study also highlights the importance of adaptive legal institutions capable of responding to rapidly evolving technological developments without undermining democratic freedoms and political participation. From a practical perspective, the article underscores the urgency of strengthening digital literacy, enhancing cooperation between electoral supervisory institutions and technology platforms, and establishing rapid-response mechanisms against AI-generated political disinformation during election periods. These measures are essential for preserving public trust, protecting democratic participation, and ensuring legal certainty within increasingly digitized electoral systems.

Despite its contributions, this study has several limitations. The research primarily relies on qualitative socio-legal analysis and secondary data sources, which limits empirical measurement regarding the direct behavioral effects of political deepfakes on Indonesian voters. Future research should therefore incorporate empirical approaches such as public perception surveys, experimental political communication studies, or comparative analyses involving multiple democratic states affected by AI-driven electoral manipulation. Further interdisciplinary studies integrating law, political communication, cybersecurity, and artificial intelligence governance are also necessary to develop more comprehensive regulatory models capable of addressing future challenges associated with synthetic media technologies. Nevertheless, this study affirms that the regulation of deepfake technology constitutes an urgent democratic necessity for Indonesia in safeguarding electoral integrity and protecting democratic rights in the digital era.

GENERATIVE AI USAGE STATEMENT

The authors used generative artificial intelligence technology solely for limited language assistance and structural editing during the preparation of this manuscript. All academic arguments, legal analysis, interpretations, data presentation, literature review, and conclusions were independently developed, reviewed, and validated by the authors under full human supervision. The use of AI-assisted technology did not involve the generation of research findings, scholarly arguments, citations, or analytical conclusions. The authors retain full responsibility for the originality, accuracy, integrity, and ethical compliance of the manuscript.

REFERENCES

- Alghan, A. S., Hafiedh, F., Louis, M., & Pratama, V. B. U. (2025). Kecurangan Pemilihan Presiden di Indonesia pada tahun 2024: Analisis Kasus dan Dampaknya terhadap Demokrasi. *Jurnal Ilmiah Mimbar Demokrasi*, 24(2), 514-520. <https://doi.org/10.21009/jimd.v24i2.53161>
- Appel, M., & Prietzel, F. (2022). The detection of political deepfakes. *Journal of Computer-Mediated Communication*, 27(4), zmac008. <https://doi.org/10.1093/jcmc/zmac008>

- Armiwulan, H., Rahman, R. A., Prabowo, V. N., & HajdÄº, J. (2024). Artificial intelligence and its challenges to elections in Indonesia: A legal analysis. *Jambura Law Review*, 6(2), 264-285. <https://doi.org/10.33756/jlr.v6i2.24243>
- Arvitto, R. S. (2025). Implikasi hukum deepfake: Telaah terhadap UU ITE dan UU PDP. *Jurnal Ilmiah Hukum dan Hak Asasi Manusia*, 4(2), 73-82. <https://doi.org/10.35912/jihham.v4i2.3937>
- Bennett, W. L., & Livingston, S. (2018). The disinformation order: Disruptive communication and the decline of democratic institutions. *European Journal of Communication*, 33(2), 122–139. <https://doi.org/10.1177/0267323118760317>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp0630a>
- Chairani, M. A., Yitawati, K., & Pradhana, A. P. (2024). Urgensi pengaturan hukum bagi penyalahgunaan aplikasi deepfake. *Jurnal Rechtsens*, 13(1), 81-96. <https://doi.org/10.56013/rechtsens.v13i1.2668>
- Chen, Z., & Yuan, J. (2023). From the Traditional Rule of Law to the Intelligent Rule of Law: The Approach to the Rule of Law from the New Technology Revolution Perspective. *Chinese Studies*, 12(01), 59–74. <https://doi.org/10.4236/chnstd.2023.121006>
- Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(6), 1753–1820. <https://doi.org/10.15779/Z38RV0D15J>
- Citron, D. K. (2019). Deepfakes and the new disinformation war: The coming age of post-truth geopolitics. *Foreign Affairs*, 98(1), 147–155.
- Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.
- Dan, V. (2025). Deepfakes as a democratic threat: Experimental evidence shows noxious effects that are reducible through journalistic fact checks. *The International Journal of Press/Politics*. <https://doi.org/10.1177/19401612251317766>
- Dobber, T., Metoui, N., Trilling, D., Helberger, N., & de Vreese, C. (2021). Do (microtargeted) deepfakes have real effects on political attitudes? *The International Journal of Press/Politics*, 26(1), 69–91. <https://doi.org/10.1177/1940161220944364>
- Freelon, D., & Wells, C. (2020). Disinformation as political communication. *Political Communication*, 37(2), 145–156. <https://doi.org/10.1080/10584609.2020.1723755>
- Hameleers, M., van der Meer, T. G. L. A., & Dobber, T. (2022). You won't believe what they just said! The effects of political deepfakes embedded as vox populi on social media. *Social Media + Society*, 8(3). <https://doi.org/10.1177/20563051221116346>
- Hameleers, M., van der Meer, T. G. L. A., Tulin, M., & Dobber, T. (2026). Radical right-wing political deepfakes can successfully delegitimize targeted political actors: Evidence from three-wave experiments in the US and The Netherlands. *Communication Research*. 00936502261421437. <https://doi.org/10.1177/00936502261421437>
- Helberger, N., Pierson, J., & Poell, T. (2018). Governing online platforms: From contested to cooperative responsibility. *The Information Society*, 34(1), 1–14. <https://doi.org/10.1080/01972243.2017.1391913>
- Imran, A., Ali, M. I., & Rehman, A. (2025). The Role of Generative AI in Undermining Electoral Integrity: A Study on AI-Driven Election Interference. *Global Political Review*, 10(1), 89-106. [https://doi.org/10.31703/gpr.2025\(x-i\).08](https://doi.org/10.31703/gpr.2025(x-i).08)
- Judge, E. F., & Korhani, A. M. (2020). Disinformation, digital information equality, and electoral integrity. *Election Law Journal: Rules, Politics, and Policy*, 19(2), 240-261. <https://doi.org/10.1089/elj.2019.056>
- Jufri, M. A. A., & Putra, A. K. (2021). Aspek hukum internasional dalam pemanfaatan deepfake technology terhadap perlindungan data pribadi. *Uti Possidetis: Journal of International Law*, 2(1), 31-57. <https://doi.org/10.22437/up.v2i1.11093>
- Karim, A., Zeinudin, M., & Suhartono, S. (2025). Pertanggungjawaban Hukum Perbuatan Kampanye Hitam (Black Campaign) dalam Pemilu Melalui Media Sosial. *JURNAL HUKUM PELITA*, 6(1), 109-121.
- Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). Deepfakes: Trick or treat? *Business Horizons*, 63(2), 135–146. <https://doi.org/10.1016/j.bushor.2019.11.006>

- Łabuz, M., & Nehring, C. (2024). On the way to deep fake democracy? Deep fakes in election campaigns in 2023. *European Political Science*, 23(4), 454–473. <https://doi.org/10.1057/s41304-024-00482-9>
- Laza, J. M., & Karo, R. K. (2023). Perlindungan Hukum Terhadap Artificial Intelligence Dalam Aspek Penyalahgunaan Deepfake Technology Pada Perspektif UU PDP dan GDPR [Legal Protection of Artificial Intelligence in Misusage of Deepfake Technology in the Perspective of PDP Law and GDPR]. *Lex Prospicit*, 1(2), 136-150. <https://doi.org/10.19166/lp.v1i2.7386>
- Lazer, D. M. J., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., Metzger, M. J., Nyhan, B., Pennycook, G., Rothschild, D., Schudson, M., Sloman, S. A., Sunstein, C. R., Thorson, E. A., Watts, D. J., & Zittrain, J. L. (2018). The science of fake news. *Science*, 359(6380), 1094–1096. <https://doi.org/10.1126/science.aao2998>
- Li, Y., Yang, X., Sun, P., Qi, H., & Lyu, S. (2020). Celeb-DF: A large-scale challenging dataset for deepfake forensics. *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 3207–3216. <https://doi.org/10.1109/CVPR42600.2020.00327>
- Mahmud, B. U., & Sharmin, A. (2021). Deep insights of deepfake technology: A review. *arXiv*. <https://arxiv.org/abs/2105.00192>
- Meliana, Y. (2025). Urgensi formulasi perlindungan hukum dan kepastian pidana terhadap pengaturan tindak pidana deepfake dalam sistem hukum pidana nasional. *Jurnal Hukum Lex Generalis*, 6(7). <https://doi.org/10.56370/jhlhg.v6i7.1087>
- Nugroho, M. W., & Fahadayna, A. C. (2025). *Demokrasi siber dan resiliensi siber di Indonesia: Studi tentang kualitas demokrasi Indonesia dalam Pemilu 2014–2023/4*. *Jurnal Pendidikan Indonesia*, 6(1). <https://doi.org/10.59141/japendi.v6i1.7090>
- Nurkholisah, S., Rismana, D., Nugroho, A. E., Munjiyah, A., & Ayunisa, Q. (2025). Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan Kriminalisasi Dalam Hukum Pidana Indonesia. *JURNAL USM LAW REVIEW*, 8(3), 2421-2445. <https://doi.org/10.26623/julr.v8i3.13060>
- Paskarina, C., Ummah Mustofa, M., Hermawati, R., Nurmanto, E., & Wardana, R. (2025). Guarding the people's vote: why ethics dimension matters for public trust to E-recapitulation in the Indonesia 2024 election. *Cogent Social Sciences*, 11(1), 2586372. <https://doi.org/10.1080/23311886.2025.2586372>
- Pawelec, M. (2022). Deepfakes and democracy (theory): How synthetic audio-visual media for disinformation and hate speech threaten core democratic functions. *Digital Society*, 1(19). <https://doi.org/10.1007/s44206-022-00010-6>
- Persily, N. (2017). The 2016 U.S. election: Can democracy survive the internet? *Journal of Democracy*, 28(2), 63–76. <https://doi.org/10.1353/jod.2017.0025>
- Pirmansyah, R., Junaidi, J., & Merta, M. (2023). PENEGAKAN HUKUM PIDANA PEMILU/PILKADA ELEKTRONIK PADA PEMILU/PILKADA SERENTAK 2024. *VARIA HUKUM*, 5(2), 141–152. <https://doi.org/10.15575/vh.v5i2.28130>
- Pooja Raj. (2025). The Impact of Deepfake Technology on Elections and Democratic Trust. *Indian Journal of Law*, 3(6), 56–64. <https://doi.org/10.36676/ijl.v3.i6.137>
- Ranka, H., Surana, M., Kothari, N., Pariawala, V., Banerjee, P., Surve, A., ... & Mehta, S. (2024). Examining the Implications of Deepfakes for Election Integrity. *arXiv preprint arXiv:2406.14290*. <https://arxiv.org/abs/2406.14290>
- Sharma, K., Ferrara, E., & Liu, Y. (2022, May). Characterizing online engagement with disinformation and conspiracies in the 2020 US presidential election. In *Proceedings of the international AAAI conference on web and social media* (Vol. 16, pp. 908-919). <https://arxiv.org/abs/2107.08319>
- Soñeca, V. (2026). Risks and Challenges of Deepfakes in National and European Parliament Elections. In *Combatting Misinformation and Global Nation's False Narratives Through Education* (pp. 149-172). IGI Global Scientific Publishing.
- Suharsimi Arikunto, 2012, *Prosedur Penelitian suatu Pendekatan Praktek*, Jakarta, Rineka Cipta.
- Tandoc, E. C., Lim, Z. W., & Ling, R. (2018). Defining “fake news”. *Digital Journalism*, 6(2), 137–153. <https://doi.org/10.1080/21670811.2017.1360143>
- Topo Santoso, 2019, *Pemilu di Indonesia*, Jakarta : Sinar Grafika.

- Tucker, J. A., Guess, A., Barberá, P., Vaccari, C., Siegel, A., Sanovich, S., Stukal, D., & Nyhan, B. (2018). Social media, political polarization, and political disinformation: A review of the scientific literature. *Political Polarization and Disinformation Review*. <https://doi.org/10.2139/ssrn.3144139>
- Vaccari, C., & Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. *Social media+ society*, 6(1), 2056305120903408. <https://doi.org/10.1177/2056305120903408>
- Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review*, 9(11), 39–52. <https://doi.org/10.22215/timreview/1282>
- Westerlund, M. (2021). AI and deepfake technologies in election manipulation. *Journal of Information Warfare*, 20(3), 1–15.