Jurnal Kecerdasan Buatan dan Teknologi Informasi
Vol. 3, No. 3, September 2024, pp. 156-162
e-ISSN: 2964-2922, p-ISSN: 2963-6191
DOI : https://doi.org/10.69916/jkbti.v3i3.483

THE APPLICATION OF ARTIFICIAL INTELLIGENCE IN ELECTION SUPERVISION: BETWEEN DIGITAL EFFECTIVENESS AND THE PROTECTION OF CITIZENS' POLITICAL RIGHTS

Erfan Wahyudi*[1], Wiredarme[2]

[1,2]Institut Pemerintahan Dalam Negeri, Indonesia
Email: [1]erfan.wahyudie@gmail.com, [2]wiredarme@ipdn.ac.id

(Received: April 16, 2024; Revised: May 15, 2024; Published: September 10, 2024)

Abstract

This study examines the application of artificial intelligence in Indonesian election supervision, focusing on the balance between digital effectiveness and the protection of citizens' political rights. The objective is to analyze how AI can support the monitoring of electoral violations, hoaxes, deepfakes, digital campaigns, and voter-data risks without weakening democratic principles. This research applies a qualitative legal method with normative-juridical, conceptual, and socio-legal approaches. The analysis is based on constitutional principles, election law, campaign regulations, personal data protection law, election supervisory regulations, and recent scholarly debates on AI, disinformation, deepfakes, and electoral integrity. The findings show that AI may strengthen election supervision by improving the speed, scale, and accuracy of digital monitoring. Yet AI may also create constitutional risks, including wrongful content classification, suppression of legitimate political expression, unequal enforcement, excessive surveillance, privacy violations, and wrongful voter-data profiling. This study argues that AI-based election supervision is constitutionally legitimate only when it is governed by legality, proportionality, transparency, accountability, and meaningful human oversight. The contribution of this study lies in framing AI in election supervision as a constitutional issue concerning political rights, democratic accountability, and electoral integrity, rather than merely as a technological tool for detecting violations.

Keywords: artificial intelligence; election supervision; electoral integrity; political rights.

1. INTRODUCTION

Artificial intelligence has begun to reshape the practice of election supervision in democratic states. Election oversight is no longer limited to manual reporting, field monitoring, witness testimony, and institutional coordination among electoral bodies. Digital technologies now enable real-time monitoring of online campaigns, automated detection of disinformation, mapping of coordinated inauthentic behavior, sentiment analysis, voter-data verification, and early warning systems for electoral violations. In this context, AI offers new possibilities for strengthening the effectiveness of election supervision, especially in detecting hoaxes, hate speech, vote manipulation narratives, illegal digital campaigning, and threats to voter-data integrity. Yet AI also creates constitutional risks when electoral supervision relies on automated classification, opaque content moderation, biased datasets, or excessive surveillance of political expression. The Indonesian electoral context makes this issue highly relevant. Indonesia is one of the world's largest democracies, with elections involving national, regional, legislative, and presidential contests across a highly diverse society. Law No. 7 of 2017 on General Elections provides the main legal framework for electoral administration, electoral supervision, campaign regulation, voter rights, violations, and dispute resolution. KPU Regulation No. 15 of 2023 regulates election campaigns, including campaign actors, campaign materials, campaign methods, broadcasting, campaign prohibitions, coordination with state institutions, and political education. Bawaslu Regulation No. 11 of 2023 regulates campaign supervision and confirms the supervisory authority of Bawaslu, provincial Bawaslu, and regency/city Bawaslu in campaign stages. These instruments show that Indonesia already has an electoral supervision framework, but the legal treatment of AI-based supervision remains underdeveloped.

The constitutional problem arises because election supervision is not merely a technical activity. It is directly connected with citizens' political rights, freedom of expression, equal political participation, privacy, and the integrity of democratic competition. AI may help electoral bodies detect digital violations more quickly, but it may also misclassify legitimate political criticism as harmful content, suppress minority political voices, or produce selective enforcement when algorithmic systems are trained on biased data. In the context of voter data, AI may support voter-list cleaning, anomaly detection, and administrative efficiency, but it may also create risks of wrongful deletion, discriminatory profiling, or unauthorized processing of sensitive political information. For this reason, AI in election

supervision must be assessed through the principles of democracy, electoral integrity, proportionality, transparency, accountability, and the protection of political rights.

Recent studies have examined the relationship between AI, disinformation, deepfakes, and electoral integrity. Díaz et al. mapped 557 English-language journal articles on AI for detecting electoral disinformation on social media, showing that this field has grown rapidly but still faces challenges related to models, datasets, evaluation, and socio-political harm [1]. Park et al. explain that generative AI has a dual role in the misinformation ecosystem because it can produce convincing false content while also being used to detect and mitigate misinformation [2]. Momeni shows that political deepfakes can shape citizen perception through persuasive misinformation and may intensify truth decay, political polarization, and electoral manipulation [3]. Łabuz analyzes deepfakes in election campaigns and warns that their greatest danger may lie not only in deception itself, but also in the erosion of public trust in authentic information [4]. Twomey et al. similarly show that deepfake discourse may undermine epistemic trust, especially when citizens become uncertain about whether visual or audio evidence is real [5]. Weikmann and Lecheler add that fact-checking actors face new challenges in responding to deepfakes because synthetic media complicates verification networks and public trust [6]. Pawelec further argues that synthetic audio-visual media may threaten core democratic functions when used for disinformation and hate speech [14]. Ahmed finds that deepfakes interact with citizens' cognitive ability and social media news skepticism, which may influence how voters evaluate political information [15]. Mauk and Grömping also demonstrate that online disinformation may shape inaccurate beliefs about election fairness among both electoral winners and losers [18]. These studies establish that AI-related election risks are not limited to false information; they affect the epistemic foundation of democratic choice and citizens' trust in electoral integrity.

A second group of studies has focused on AI-enabled political campaigns, election regulation, visual disinformation, and the Indonesian case. Rauchfleisch, Jungherr, and Wuttke show that AI-generated political advertising, automated messaging, and photorealistic campaign content have created new regulatory challenges for democratic systems [7]. Kalsnes compares codes of conduct for generative AI use during election campaigns, showing that voluntary and semi-voluntary norms have emerged as responses to deepfakes, synthetic political content, and AI-generated disinformation [8]. Armiwulan et al. argue that the improper use of AI in Indonesian elections threatens democratic election principles and requires a stronger legal framework [9]. Rahman and Anggriawan examine deepfakes as electoral crimes in Indonesia, India, Pakistan, and the United States, highlighting criminal-law gaps in responding to synthetic political manipulation [10]. Paliwang and Swandiani specifically analyze political deepfakes and disinformation in the 2024 Indonesian election and identify weaknesses in the existing regulatory framework [11]. Subekti et al. find that social media played a significant role in spreading disinformation against candidates in the 2024 Indonesian presidential election, especially through platforms that support video and text formats such as Facebook, YouTube, and TikTok [12]. Sibaroni et al. further demonstrate the technical potential of deep-learning models for detecting political hoax news in Indonesian social media, with a hybrid CNN-LSTM model showing strong detection performance [13]. Wahl-Jorgensen and Carlson show that public discourse on deepfakes is often shaped by fear of future manipulation and uncertainty over political authenticity [16]. Dan et al. also emphasize that visual mis- and disinformation on social media has serious implications for democracy because images and videos may influence political perception more strongly than textual claims [17]. These studies are relevant for understanding why AI-based election supervision is increasingly needed, but they also show that technological monitoring must be carefully balanced with democratic rights.

Despite these contributions, existing scholarship still leaves an important gap. Technical studies tend to emphasize the effectiveness of AI for detecting hoaxes, deepfakes, coordinated manipulation, and political misinformation. Legal studies tend to focus on the regulation of AI misuse, campaign violations, criminalization of deepfakes, or platform responsibility. Few studies have examined AI-based election supervision through the constitutional relationship between digital effectiveness, citizens' political rights, democratic principles, and electoral integrity in Indonesia. This article fills that gap by arguing that AI in election supervision must be treated as a constitutional governance issue, not merely as a technological instrument for monitoring violations. Its novelty lies in connecting AI supervision with the protection of political rights, freedom of expression, voter-data integrity, equal participation, and democratic accountability. The objective of this study is to analyze how AI can be applied in Indonesian election supervision without weakening the constitutional foundations of free, fair, honest, and accountable elections.

2. ESEARCH METHODS

This study uses a qualitative legal research method with normative-juridical, conceptual, and socio-legal approaches. The normative-juridical approach is used to examine the constitutional and statutory framework governing elections, election supervision, political rights, personal data protection, and digital governance in Indonesia. The conceptual approach is applied to construct the relationship between artificial intelligence, electoral integrity, democratic accountability, and the protection of citizens' political rights. The socio-legal approach is used to understand how AI-based election supervision may operate within Indonesia's practical electoral context, especially in monitoring online campaigns, hoaxes, disinformation, deepfakes, digital political advertising, campaign

violations, and voter-data management. This research does not employ a quantitative method, statistical testing, or the development of a specific AI algorithm. It also does not train or evaluate a technical model for detecting electoral violations. Instead, the study is designed as **a** descriptive-analytical legal research that evaluates the constitutional implications of using AI as a supervisory instrument in elections. The central issue is not merely whether AI can detect electoral violations effectively, but whether its use remains consistent with democratic principles, freedom of political expression, equal participation, voter privacy, due process, and the integrity of elections.

The case study of this research is Indonesia's election supervision system, particularly the role of electoral supervisory institutions in responding to digital campaign violations, online disinformation, political hoaxes, AI-generated campaign content, deepfakes, and voter-data risks. Indonesia is selected because it represents a large, complex, and digitally active democracy. Its electoral system involves national and local contests, diverse political actors, large-scale voter administration, and intensive use of social media during campaigns. Law No. 7 of 2017 on General Elections serves as the main legal framework for electoral administration, campaign regulation, voter rights, supervision, violations, and dispute resolution in Indonesia.

The study also analyzes specific electoral regulations relevant to digital campaign supervision. KPU Regulation No. 15 of 2023 regulates election campaigns, including campaign actors, campaign materials, campaign methods, broadcasting, campaign prohibitions, coordination with government institutions, and political education. Bawaslu Regulation No. 11 of 2023 regulates campaign supervision and confirms the authority of Bawaslu, provincial Bawaslu, and regency/city Bawaslu to conduct supervision according to their respective authority and to prepare supervision reports during campaign stages. These regulations are important because AI-based supervision would operate within the existing legal mandate of election supervisory bodies, not outside the statutory framework of election law. Data collection is conducted through documentary research. The primary legal materials consist of the 1945 Constitution of the Republic of Indonesia, Law No. 7 of 2017 on General Elections, Law No. 27 of 2022 on Personal Data Protection, Law No. 11 of 2008 as amended by Law No. 19 of 2016 and Law No. 1 of 2024 on Electronic Information and Transactions, KPU Regulation No. 15 of 2023 on Election Campaigns, Bawaslu Regulation No. 11 of 2023 on Election Campaign Supervision, and relevant regulations concerning digital government, electronic systems, campaign supervision, and voter-data protection. Law No. 27 of 2022 is included because voter data and political-preference-related information may be affected by AI-based processing; the law regulates data-subject rights, obligations of controllers and processors, data transfer, sanctions, institutional arrangements, dispute settlement, and the constitutional protection of personal data subjects.

Secondary data consist of peer-reviewed journal articles published mainly within the last five years on artificial intelligence in elections, electoral disinformation, political deepfakes, automated content detection, AI-generated political campaigns, digital campaign regulation, voter-data protection, democratic integrity, and algorithmic governance. These academic sources are used to build the theoretical foundation and to compare Indonesia's case with broader international debates. The study also uses official government documents, election supervisory materials, policy reports, and institutional publications to understand how digital election supervision is developing in Indonesia.

The data are analyzed using qualitative legal analysis through four stages. First, the study identifies constitutional principles relevant to AI-based election supervision, including political rights, freedom of expression, equality, privacy, legal certainty, democratic participation, and electoral integrity. Second, it maps the possible uses of AI in election supervision, including hoax detection, deepfake identification, campaign-content monitoring, anomaly detection in voter data, sentiment analysis, and early warning systems for digital electoral violations. Third, it examines the legal risks that may arise from AI-based supervision, including over-surveillance, algorithmic bias, wrongful content classification, suppression of legitimate political speech, discriminatory enforcement, and unlawful processing of voter data. Fourth, it formulates a rights-based framework for applying AI in election supervision without weakening democratic rights.

The analytical framework of this study is built on the concept of rights-based AI election supervision. In this framework, AI may be used to strengthen electoral integrity, but only as a supporting instrument under human institutional responsibility. AI must not become an autonomous authority that determines whether political expression is lawful, whether campaign content is prohibited, or whether voter data are valid without meaningful human review. The framework is operationalized through five indicators: legality, proportionality, transparency, accountability, and human oversight. Legality requires AI use to have a clear legal basis. Proportionality requires that AI monitoring does not excessively restrict political expression or privacy. Transparency requires electoral bodies to explain the role and limits of AI systems. Accountability requires clear institutional responsibility for AI-based supervisory actions. Human oversight requires final supervisory judgment to remain with authorized election officials.

To strengthen validity, this study applies source triangulation and conceptual triangulation. Source triangulation is carried out by comparing constitutional provisions, election laws, electoral regulations, personal data protection law, official policy documents, and recent academic literature. Conceptual triangulation is conducted by combining constitutional law, election law, human rights law, data protection law, and AI governance perspectives. This combination is necessary because AI-based election supervision involves more than technological effectiveness. It

concerns the balance between digital monitoring, political freedom, democratic legitimacy, voter privacy, and institutional accountability.

The limitation of this research is that it does not conduct empirical interviews with election supervisors, political parties, voters, platform operators, or AI developers. It also does not test a specific AI system used for detecting election violations or digital campaign manipulation. The study is limited to normative, conceptual, and policy-based analysis. This limitation is appropriate because the main objective of the article is to construct a constitutional and legal framework for evaluating AI in Indonesian election supervision. Future empirical studies may examine how Bawaslu, KPU, political parties, civil society organizations, and digital platforms use or respond to AI-based tools in election monitoring, campaign supervision, voter-data protection, and disinformation control.

3. RESULTS AND DISCUSSION

3.1. AI-Based Election Supervision as an Instrument for Strengthening Electoral Integrity

The first finding of this study shows that artificial intelligence has significant potential to strengthen election supervision in Indonesia, particularly in monitoring digital campaign activities, detecting hoaxes, identifying deepfake content, mapping coordinated disinformation, and supporting voter-data verification. Indonesia's election supervision system already has a legal foundation through Law No. 7 of 2017 on General Elections, which regulates electoral administration, supervision, campaign provisions, violations, and dispute mechanisms. KPU Regulation No. 15 of 2023 further regulates election campaigns, including campaign actors, materials, methods, prohibitions, and coordination with public institutions. Bawaslu Regulation No. 11 of 2023 also confirms the authority of election supervisors to supervise campaign stages and prepare supervision reports according to their respective authority.

Within this regulatory structure, AI can be positioned as a supporting instrument for election supervisors. AI-based tools may assist Bawaslu and related institutions in processing large volumes of digital campaign content, detecting repeated patterns of disinformation, identifying suspicious accounts, classifying potentially prohibited campaign materials, and generating early warning signals for possible election violations. This is important because digital campaign activities often move faster than manual supervision. Election violations in digital spaces may spread across social media platforms, messaging applications, short videos, livestreams, and political advertising networks before formal supervisory mechanisms can respond effectively.

The findings are consistent with Díaz et al., who show that AI for detecting electoral disinformation has developed rapidly, especially through models that analyze social media data, text classification, network patterns, and misinformation datasets [1]. Sibaroni et al. also demonstrate the technical potential of deep-learning models in detecting Indonesian political hoax news on social media, especially through hybrid CNN-LSTM architecture [13]. These studies confirm that AI can improve the speed and scale of digital election monitoring. In Indonesia, this potential is particularly relevant because the 2024 election showed the intensive use of social media in political communication and disinformation circulation, especially on platforms that support text, video, and visual content [12].

AI is also relevant for addressing the growing risk of deepfake-based political manipulation. Studies by Momeni, Łabuz, Twomey et al., and Weikmann and Lecheler show that deepfakes may distort citizen perception, weaken public trust, complicate fact-checking, and create uncertainty about the authenticity of political information [3]–[6]. In the Indonesian context, this risk is no longer theoretical. Bawaslu-linked scholarship has specifically discussed the use of deepfakes in spreading hoax issues during the 2024 election campaign, showing that synthetic media has entered the practical field of election supervision in Indonesia.

The study also finds that AI can assist in protecting voter-data integrity. AI-based anomaly detection may help identify duplicate records, unusual changes in voter lists, inconsistent demographic data, or suspicious data patterns. This function may strengthen administrative accuracy and reduce the risk of voter-list manipulation. Yet this use must be carefully limited because voter data are closely connected with citizens' political rights and personal data protection. If voter-data supervision relies on automated profiling without clear legal safeguards, AI may wrongly flag legitimate voters, intensify administrative exclusion, or create discriminatory effects against vulnerable groups.

Based on these findings, AI in election supervision should be understood as a tool for strengthening electoral integrity, not as a replacement for electoral institutions. AI may assist detection, prioritization, and analysis, but the final determination of campaign violations, unlawful content, voter-data invalidity, or electoral misconduct must remain with authorized human officials. This position aligns with broader AI governance studies arguing that public-sector AI should remain accountable to institutional responsibility, legal standards, and public values [7], [8], [11].

3.2. Constitutional Risks: Political Rights, Freedom of Expression, Privacy, and Algorithmic Bias

The second finding of this study shows that AI-based election supervision may create constitutional risks if it is applied without clear limits. Election supervision is not merely a technical function. It directly affects political rights, freedom of expression, equal participation, privacy, and fair democratic competition. AI systems used to monitor campaigns may detect harmful content, but they may also misclassify legitimate political criticism, satire, minority

opinion, investigative speech, or opposition discourse as prohibited content. In this situation, technological effectiveness may produce democratic harm if AI is used as an excessive surveillance instrument.

The risk of over-classification is particularly important in digital campaign supervision. AI models may identify patterns based on keywords, hashtags, images, network behavior, sentiment, or previous violations. These indicators are useful for detection, but they are not always sufficient to determine illegality. Political speech often contains criticism, emotional language, satire, exaggeration, or symbolic expression. If AI systems are trained on narrow or biased datasets, they may interpret legitimate political speech as disinformation, hate speech, or unlawful campaigning. This creates a risk of chilling effect, where citizens, journalists, activists, and political actors avoid lawful expression because they fear algorithmic surveillance or enforcement. This finding is consistent with Pawelec's argument that synthetic media and AI-driven disinformation may threaten democratic functions, not only through deception, but also through the weakening of public deliberation [14]. Dan et al. also show that visual mis- and disinformation may strongly influence democratic perception because images and videos can affect political judgment more directly than textual claims [17]. These studies support the view that AI-based election supervision must protect the quality of democratic information while avoiding excessive control over political communication.

Another constitutional risk concerns unequal enforcement. AI systems may perform differently across languages, dialects, regions, platforms, and political communities. Indonesia has diverse linguistic, cultural, and regional contexts. Political expression in Bahasa Indonesia, local languages, religious idioms, humor, regional slogans, and symbolic campaign materials may not be equally understood by AI models. A model trained mainly on dominant language patterns may fail to detect harmful content in certain communities while over-detecting content in others. This may create selective enforcement and unequal treatment among political participants. The risk is also visible in the context of voter data. AI-based voter-data monitoring may improve accuracy, but it may also create wrongful exclusion if the system flags voters based on incomplete, outdated, or inconsistent data. Citizens living in remote areas, migrant workers, persons with disabilities, elderly voters, first-time voters, or citizens with changing residence status may be more vulnerable to administrative errors. Since voting is a constitutional political right, AI-based voter-data verification must be subject to strict human review, correction mechanisms, and accessible remedies.

Privacy is another major concern. Election supervision may require monitoring campaign activity, digital advertising, political networks, and online disinformation patterns. Yet such monitoring must not become mass political surveillance. Law No. 27 of 2022 on Personal Data Protection is relevant because AI-based supervision may process personal data, digital identifiers, political behavior, communication patterns, or voter-related information. Personal data protection law recognizes rights and obligations relating to data processing, data-subject protection, sanctions, and dispute settlement. AI-based election supervision must therefore be designed according to necessity, proportionality, data minimization, purpose limitation, and institutional accountability. The findings also align with Park et al., who explain that generative AI plays a dual role in misinformation because it can produce false content while also being used to detect and mitigate misinformation [2]. This dual role is important for election supervision. The same technology that helps supervisors identify harmful content may also be used by political actors to generate persuasive disinformation, deepfake speeches, synthetic endorsements, manipulated images, or automated propaganda. For this reason, AI-based supervision must be accompanied by legal standards on campaign transparency, AI-generated content disclosure, political advertising accountability, platform cooperation, and public education.

3.3. Rights-Based Model for AI in Indonesian Election Supervision

The third finding of this study is that Indonesia needs a rights-based model for AI-based election supervision. AI should be used to strengthen electoral integrity, but its use must remain subordinate to constitutional democracy. The model proposed in this study consists of five principles: legality, proportionality, transparency, accountability, and human oversight. First, legality requires a clear legal basis for the use of AI in election supervision. Electoral institutions should not deploy AI systems merely on the basis of administrative convenience or technological experimentation. The scope, purpose, authority, data sources, and limits of AI-based supervision must be regulated. Law No. 7 of 2017, KPU Regulation No. 15 of 2023, and Bawaslu Regulation No. 11 of 2023 already provide a basis for election supervision and campaign regulation, but they do not yet provide detailed rules on AI-based monitoring, deepfake detection, automated content classification, or algorithmic voter-data analysis. This regulatory gap must be addressed so that AI supervision does not operate without democratic and legal control. Second, proportionality requires that AI-based monitoring be limited to legitimate electoral purposes. AI should be used to detect and analyze potential violations, not to monitor all political expression indiscriminately. The intensity of AI supervision must correspond to the seriousness of the risk. For example, detecting coordinated deepfake disinformation that may manipulate voters is more justifiable than broad surveillance of ordinary political conversations. This principle is important because electoral integrity must be protected without weakening freedom of expression and political participation.

Third, transparency requires electoral bodies to explain whether AI is used, what type of content or data is monitored, what the system can and cannot do, and how citizens or political actors may challenge supervisory actions influenced by AI. Transparency is essential because citizens must be able to distinguish between lawful supervision

and opaque algorithmic control. This finding is supported by studies on AI governance showing that public trust depends on perceived legitimacy, explainability, and institutional accountability [7], [13]. In the electoral context, transparency is also necessary to prevent allegations that AI supervision is used selectively for partisan purposes. Fourth, accountability requires clear institutional responsibility. AI systems do not possess electoral authority. They cannot independently declare a campaign violation, invalidate voter data, remove political content, or impose sanctions. Such actions must remain within the authority of electoral institutions and must be reviewable through existing legal mechanisms. This is consistent with Kalsnes's observation that the rise of generative AI in election campaigns has encouraged codes of conduct and regulatory responses, but voluntary norms are not sufficient when democratic rights are at stake [8]. Indonesia needs binding accountability rules for electoral bodies, platforms, campaign teams, AI vendors, and political actors using AI-generated campaign materials.

Fifth, human oversight must be meaningful. AI may generate alerts, classifications, risk scores, or recommendations, but human election supervisors must review context, intent, legal elements, evidence quality, and possible rights implications. Human review is especially important for political speech, since legality cannot be determined only through automated pattern recognition. Rauchfleisch, Jungherr, and Wuttke show that AI-generated political advertising and campaign content create regulatory challenges because citizens and institutions may respond differently to AI-mediated political communication [7]. Human oversight is therefore necessary to ensure that election supervision remains legally grounded and democratically legitimate. This rights-based model also responds to the Indonesian literature on AI and elections. Armiwulan et al. argue that improper AI use may threaten democratic election principles in Indonesia and requires stronger legal regulation [9]. Rahman and Anggriawan identify criminal-law gaps in responding to deepfake-related electoral crimes across several jurisdictions, including Indonesia [10]. Paliwang and Swandiani further show that Indonesia's 2024 election experience exposed weaknesses in the legal framework for political deepfakes and disinformation [11]. These studies support the argument that Indonesia should not rely only on reactive enforcement. It needs preventive, supervisory, and remedial mechanisms that integrate AI governance with electoral law and constitutional rights. Based on the analysis, this study formulates the following proposition: AI-based election supervision is constitutionally legitimate only when it strengthens electoral integrity without weakening citizens' political rights, freedom of expression, voter privacy, equal participation, and democratic accountability**.** AI can help election supervisors respond to hoaxes, deepfakes, campaign manipulation, and voter-data risks, but it must be used as a supervised instrument, not as an autonomous authority. The Indonesian framework should therefore develop specific rules on AI use in election supervision, including algorithmic impact assessment, disclosure of AI-generated campaign content, human review of AI-based findings, voter-data safeguards, platform cooperation, complaint mechanisms, and independent oversight.

4. CONCLUSION

This study concludes that the application of artificial intelligence in Indonesian election supervision must be understood as a constitutional governance issue, not merely as a technological strategy for improving monitoring capacity. AI has clear potential to support election supervisors in detecting hoaxes, deepfakes, coordinated disinformation, illegal digital campaigns, suspicious online behavior, and anomalies in voter data. In a large and digitally active democracy such as Indonesia, these functions may strengthen the effectiveness of Bawaslu and related electoral institutions in protecting electoral integrity. The main finding of this study shows that AI-based election supervision creates a dual implication. On one side, AI can improve the speed, scale, and analytical capacity of electoral monitoring. On the other side, AI may threaten political rights when it is used without clear legal limits, transparency, human review, and accountability. Algorithmic systems may misclassify legitimate political criticism as harmful content, produce unequal enforcement across languages and regions, intensify political surveillance, or create risks of wrongful voter-data classification. These risks are constitutionally significant because election supervision is directly connected with freedom of expression, equal political participation, voter privacy, legal certainty, and democratic accountability. The novelty of this study lies in connecting AI-based election supervision with citizens' political rights and democratic constitutional principles. Previous studies have discussed AI, deepfakes, disinformation, and electoral manipulation mainly from the perspectives of technological detection, campaign regulation, or criminal-law responses. This article contributes to that debate by arguing that AI in election supervision must be evaluated through a rights-based constitutional framework. The central issue is not only whether AI can detect violations effectively, but whether its use remains consistent with free, fair, honest, transparent, and accountable elections. This study proposes five principles for rights-based AI election supervision in Indonesia: legality, proportionality, transparency, accountability, and meaningful human oversight. Legality requires a clear legal basis for AI-based monitoring. Proportionality requires that AI supervision be limited to legitimate electoral purposes and must not become mass political surveillance. Transparency requires electoral institutions to explain the role and limits of AI systems. Accountability requires clear institutional responsibility for AI-assisted supervisory actions. Human oversight requires final legal judgment to remain with authorized election officials, not automated systems. The limitation of this study is that it does not conduct empirical testing of a specific AI tool used by Indonesian electoral institutions. It also does not examine direct interviews with Bawaslu, KPU, political parties, civil society groups,

platform operators, or voters. Future research should examine concrete AI practices in election supervision, including digital campaign monitoring, deepfake detection, voter-data verification, social media surveillance, political advertising transparency, and platform cooperation. Comparative studies with other democratic countries would also be useful to formulate a more operational model for AI-based election supervision that protects both electoral integrity and citizens' political rights.

REFERENCES

[1] F. Díaz, N. Cerna, R. Liza, and B. Motta, "Artificial Intelligence for Detecting Electoral Disinformation on Social Media: Models, Datasets, and Evaluation," *Information*, vol. 17, no. 3, 292, 2026, doi: 10.3390/info17030292.

[2] S. Park, J. Casas, and A. G. Paz, "Generative AI and misinformation: A scoping review of the role of generative AI in the generation, detection, mitigation, and impact of misinformation," *AI & Society*, 2025, doi: 10.1007/s00146-025-02620-3.

[3] M. Momeni, "Artificial Intelligence and Political Deepfakes: Shaping Citizen Perceptions Through Misinformation," *Journal of Creative Communications*, 2025, doi: 10.1177/09732586241277335.

[4] M. Łabuz, "On the way to deep fake democracy? Deep fakes in election campaigns in 2023," *European Political Science*, 2024, doi: 10.1057/s41304-024-00482-3.

[5] J. Twomey, D. Ching, M. P. Aylett, M. Quayle, C. Linehan, and G. Murphy, "Do deepfake videos undermine our epistemic trust? A thematic analysis of tweets that discuss deepfakes in the Russian invasion of Ukraine," *PLOS ONE*, vol. 18, no. 10, e0291668, 2023, doi: 10.1371/journal.pone.0291668.

[6] T. Weikmann and S. Lecheler, "Cutting through the hype: Understanding the implications of deepfakes for the fact-checking actor-network," *Digital Journalism*, 2023, doi: 10.1080/21670811.2023.2194665.

[7] A. Rauchfleisch, A. Jungherr, and A. Wuttke, "Explaining public preferences for regulating Artificial Intelligence in election campaigns: Evidence from the U.S. and Taiwan," *Telecommunications Policy*, 2025, doi: 10.1016/j.telpol.2025.103072.

[8] B. Kalsnes, "Comparing codes of conduct for generative AI use during election campaigns," *Information, Communication & Society*, 2026, doi: 10.1080/1369118X.2026.2647362.

[9] H. Armiwulan, R. A. Rahman, V. N. Prabowo, and J. Hajdú, "Artificial Intelligence and Its Challenges to Elections in Indonesia: A Legal Analysis," *Jambura Law Review*, vol. 6, no. 2, 2024, doi: 10.33756/jlr.v6i2.24243.

[10] R. A. Rahman and R. Anggriawan, "Deepfake and Electoral Crimes: Criminal Law Perspectives from Indonesia, India, Pakistan, and the U.S.," *Indonesian Comparative Law Review*, vol. 7, no. 2, 2025, doi: 10.18196/iclr.v7i2.26337.

[11] A. N. A. A. Paliwang and N. L. P. E. Swandiani, "Artificial Intelligence Regulation in the Protection of Democracy: A Legal Analysis of Political Deepfakes and Disinformation in the 2024 Election," *Hakim: Jurnal Ilmu Hukum dan Sosial*, vol. 3, no. 4, pp. 1433–1455, 2025, doi: 10.51903/rx25ap29.

[12] D. S. Subekti, M. Yusuf, M. Saadah, and M. Wahid, "Social media and disinformation for candidates: The evidence in the 2024 Indonesian presidential election," *Frontiers in Political Science*, vol. 7, 1625535, 2025, doi: 10.3389/fpos.2025.1625535.

[13] Y. Sibaroni, S. B. Mahadzir, S. S. Prasetiyowati, and A. F. Ihsan, "Combating Misinformation: Leveraging Deep Learning for Hoax Detection in Indonesian Political Social Media," *Jurnal Infotel*, vol. 16, no. 2, pp. 413–426, 2024, doi: 10.20895/INFOTEL.V16I2.1139.

[14] M. Pawelec, "Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions," *Digital Society*, vol. 1, no. 2, 19, 2022, doi: 10.1007/s44206-022-00010-6.

[15] S. Ahmed, "Navigating the maze: Deepfakes, cognitive ability, and social media news skepticism," *New Media & Society*, vol. 25, no. 5, pp. 1108–1129, 2023, doi: 10.1177/14614448211019198.

[16] K. Wahl-Jorgensen and M. Carlson, "Conjecturing fearful futures: Journalistic discourses on deepfakes," *Journalism Practice*, vol. 15, no. 6, pp. 803–820, 2021, doi: 10.1080/17512786.2021.1908838.

[17] V. Dan, B. Paris, J. Donovan, M. Hameleers, J. Roozenbeek, S. van der Linden, and B. von Sikorski, "Visual mis- and disinformation, social media, and democracy," *Journalism & Mass Communication Quarterly*, vol. 98, no. 3, pp. 641–664, 2021, doi: 10.1177/10776990211035395.

[18] M. Mauk and M. Grömping, "Online disinformation predicts inaccurate beliefs about election fairness among both winners and losers," *Comparative Political Studies*, vol. 57, no. 6, pp. 965–998, 2024, doi: 10.1177/00104140231193008.