Journal of Law and Regulation Governance

Disinformation and Cyber Propaganda in Indonesian Elections: The Urgency of Updating Election Law Regulations

Sulastri[1], Teguh Parsetyo[2], Amin Purnawan[3]
Universitas Islam Sultan Agung, Indonesia[1,3]
Universitas Pelita Harapan, Indonesia[2]
Email: lastri.stihsa@gmail.com, prof.teguh.prasetyo@gmail.com, amin.p@unissula.ac.id

ABSTRACT
The growing prevalence of disinformation and cyber propaganda in Indonesia's electoral processes presents a significant threat to the integrity of democratic elections in the digital age. Disinformation blurs the lines between freedom of expression and political manipulation, challenging the effectiveness of existing legal frameworks. This study examines the effectiveness of Indonesia's electoral laws—specifically the Election Law, the Electronic Information and Transactions Law (ITE Law), and technical regulations issued by the KPU and Bawaslu—in addressing digital disinformation during the 2019 and 2024 general elections. Using a normative legal, comparative, and case study approach, the findings reveal that the current legal framework is sectoral, reactive, and inadequate to address technological developments in disinformation. Institutional fragmentation and the absence of enforceable legal responsibilities for digital platforms exacerbate the challenges of electoral oversight. The study calls for comprehensive legal reforms to establish a cyber election monitoring body, enforce platform transparency, and strengthen legal norms against coordinated disinformation. These reforms are crucial to ensuring that elections remain democratic, transparent, and uphold the dignity of the electoral process.

Keywords: disinformation; electoral law; digital propaganda; legal reform.

INTRODUCTION

Free, honest, and fair elections are the main foundation of constitutional democracy. In the context of modern electoral democracy, elections are not only an arena for the battle of political ideas and visions, but also an increasingly complex terrain because it involves the digital and information dimensions. One of the biggest challenges in the era of digital democracy is the rise of disinformation and cyber propaganda that is spread massively through social media and other digital platforms (Assyahida, 2025; Bachtiar, 2014; Destavino et al., 2023; Novarizal et al., 2025; Utomo & Yulianto, 2018) . Disinformation, which refers to the deliberate spread of false information to mislead the public, as well as coordinated cyber propaganda to influence voters' perceptions and political choices, has become a global phenomenon that threatens the integrity of elections.

In recent years, the spread of disinformation and cyber propaganda has become a serious threat to the integrity of elections in various countries. Digital platforms such as social media, instant messaging apps, and websites are fertile ground for the spread of false narratives, manipulative content, and coordinated influence operations against voters. This phenomenon not

only undermines public trust in democratic institutions, but also challenges the ability of the existing legal framework to ensure free, honest, and fair elections.

Indonesia, as one of the largest democracies in the world with more than 200 million voters, is not immune to this threat (Tahir et al., 2020a, 2020b; Utomo & Yulianto, 2018) . In the 2019 election and continuing in the 2024 election, digital disinformation developed massively, ranging from the spread of hoaxes, hate speech, to identity manipulation and the use of bot accounts in spreading political propaganda. Such activities often blur the line between legitimate political discourse and unlawful cyber actions, and open a loophole to the ineffectiveness of available legal instruments.

This phenomenon is evident in the implementation of the 2019 and 2024 elections, where various forms of misleading information, hate speech, identity-based black campaigns, and visual manipulation with *deepfake technology* and political bots dominate the digital space. This situation creates social polarization, lowers the quality of public discourse, and even weakens trust in election organizing institutions such as the General Election Commission (KPU), the Election Supervisory Agency (Bawaslu), and the Honorary Council of Election Organizers (DKPP). (Tapsell, 2019)

In response to these developments, Indonesia actually has legal tools that can be used as a basis for monitoring and cracking down on disinformation in elections, including Law Number 7 of 2017 concerning General Elections, Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE) and its amendments, as well as various technical regulations from the KPU and Bawaslu related to campaigns and the use of social media (O'Callaghan, 2020; Prasetyo, 2015; (PSHK, 2023) . However, the effectiveness of the legal framework is questionable. Disinformation and cyber propaganda often escape the trappings of the law due to several factors, including weaknesses in normative arrangements, indecisiveness in the formulation of sanctions, and overlapping authority between supervisory agencies. (Undang-Undang Republik Indonesia Nomor 7 Tahun 2017 tentang Pemilihan Umum, 2017).

The problem is even more complex when faced with the fact that the existing legal framework is reactive, sectoral, and not integrated, so it is unable to keep up with the development of digital technology and the work patterns of modern disinformation networks that are cross-platform, anonymous, and algorithm-based (Tambini, 2022). In addition, there is still no legal arrangement that explicitly establishes legal responsibility for global digital platforms that are the main medium for the dissemination of disinformation-containing content, such as Facebook, X (Twitter), TikTok, and YouTube. On the institutional side, the limited capacity of digital monitoring technology within the KPU and Bawaslu, as well as the absence of a national coordination system in handling election disinformation, are unresolved problems.

The phenomenon of digital disinformation in elections is a multidimensional challenge that touches the realm of election law, information and technology law, human rights, and digital media governance (Indonesia, 2023; (KPU), 2018; Nugroho, 2020). In Indonesia, although there have

been several laws and regulations that intersect with this issue, the regulatory approach is still sectoral, partial, and not fully adaptive to the development of communication technology.

Based on this background, this paper aims to examine two main things: first, the extent of the effectiveness of the existing legal framework, including the Election Law, the ITE Law, and Bawaslu/KPU technical regulations in tackling disinformation and cyber propaganda during the election process; and second, identifying various normative and institutional weaknesses that lead to weak legal responses to digital disinformation practices in elections. This study is important as a conceptual and normative basis in formulating the direction of updating election law regulations that are adaptive to the digital era, as well as to strengthen the state's capacity to maintain the quality of electoral democracy from the infiltration of misleading information.

Although Indonesia has legal tools to tackle disinformation in elections, such as the Election Law (Law No. 7 of 2017) and the ITE Law (Law No. 11 of 2008), its implementation and effectiveness are still considered to be less than optimal. The existing legal framework is sectoral and reactive, and has not been able to keep pace with the technological developments used to spread disinformation in a structured and coordinated manner. This is exacerbated by the limited institutional capacity to conduct real-time digital monitoring, as well as the lack of coordination between supervisory agencies, such as the General Election Commission (KPU) and the Election Supervisory Agency (Bawaslu).

This research is here to fill the gap in the study of the effectiveness of Indonesian election laws in dealing with digital disinformation, as well as to identify weaknesses in existing regulations. The focus of this research is on the role of election law, information and technology law, and digital surveillance policies against disinformation practices in the context of elections in Indonesia. This study aims to contribute to a more adaptive, proactive, and dignified justice principle-based regulatory reform, which not only protects the integrity of elections, but also ensures that people's voting rights are protected from damaging information manipulation.

The benefit of this research is to provide recommendations that can be used by policymakers in formulating more comprehensive regulations related to the surveillance of disinformation during elections. In addition, this research is expected to strengthen Indonesia's position in facing the challenges of digital disinformation, as well as increase legal capacity in maintaining the quality of electoral democracy in the increasingly growing digital era.

RESEARCH METHODS

This research uses a normative juridical approach with the support of a comparative approach and case studies. Specifically, the research is carried out by analyzing primary and secondary legal materials, including laws and regulations related to elections, electronic information, cyber issues, and freedom of expression, as well as technical regulations from *Bawaslu*, *KPU*, and *Kominfo*. Additionally, the Decisions of the Constitutional Court, the Supreme Court, and other relevant judicial institutions were examined.

A comparative analysis was conducted on the regulation and model of disinformation surveillance in the context of elections in several countries, such as the European Union with the *Code of Practice on Disinformation* and the *Digital Services Act*, then Germany with the *Netzwerkdurchsetzungsgesetz* (*NetzDG*) for social media platforms, as well as the countries of India and the Philippines, which face the challenge of disinformation in elections in the context of the global south. This comparison aims to explore the possibility of adopting legal principles or mechanisms that are relevant to the Indonesian context.

Furthermore, to support the research, a case study was carried out focused on disinformation in the 2019 and 2024 elections in Indonesia, including the dominant disinformation narrative, the pattern of dissemination on digital platforms, the response from legal institutions and election organizers, and the effectiveness of reporting and law enforcement mechanisms. The data were collected through documentary studies on news, election monitoring reports, and reports from civil society organizations engaged in elections and digital rights.

RESULTS AND DISCUSSION

Normatively, Indonesia has a number of legal instruments that can be used as a basis for tackling disinformation and cyber propaganda in the context of elections. Among them are Law Number 7 of 2017 concerning General Elections (Election Law), Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law) and its amendments, as well as various technical regulations from the General Election Commission (KPU) and the Election Supervisory Agency (Bawaslu).

The Election Law regulates the prohibition against the spread of false information, black campaigns, and hate speech in the election campaign process (Articles 280 and 521). Meanwhile, the ITE Law expands the scope of action against disinformation through provisions on the spread of false information that causes hatred based on SARA (Article 28 paragraph (2)) (Sagala & Nasution, 2022). Technically, the KPU and Bawaslu have also issued a number of regulations, such as the obligation to register social media accounts for election participants, the prohibition of off-schedule campaigns, and the supervision of online content.

However, the effectiveness of the legal framework in practice is still very limited. Field findings and previous studies show that the majority of digital disinformation cases during the 2019 and 2024 elections have not been adequately handled, both in terms of prevention and enforcement. Law enforcement against disinformation perpetrators tends to be casuistic and targets individual social media users, rather than larger actors such as buzzer networks, hidden political advertisers, or covert digital campaign operators.

In addition, the Election Law and the ITE Law have not explicitly regulated contemporary practices of digital disinformation, such as the use *of deepfakes*, *microtargeting*, the use of political *data analytics*, or structured dissemination through automated bots. There are no legal provisions governing the responsibility of global digital platforms for the political disinformation content they facilitate. This normative weakness also intersects directly with institutional

limitations. There is no single institution that has the full authority and capacity to monitor digital information in real-time during elections. Bawaslu, although it has a supervisory function, is not equipped with adequate cyber units and big data technology. Kominfo has a technical function of blocking, but it is more administrative and not directly involved in the election law enforcement process. This is exacerbated by the absence of an integrated coordination system between the KPU, Bawaslu, Kominfo, and law enforcement officials in tackling political disinformation.

Thus, the existing positive legal framework is reactive, non-prescriptive, and not adaptive enough to the evolution of digital disinformation, especially in the realm of electoral campaigns that are now increasingly digitized.

Further analysis of the institutional dimension shows that Indonesia faces significant structural barriers in building an effective legal response to digital disinformation. There are three main weaknesses that can be identified, namely: (a) fragmentation of authority, (b) limited technological capacity and human resources, and (c) lack of coordination between institutions in a structured manner.

First, in terms of authority, there is not yet a single authority specifically responsible for monitoring election information in the digital realm. Bawaslu has the authority to supervise campaigns, but it is not equipped with adequate cyber monitoring tools. Kominfo has the technical capacity to handle digital content, but its function is more administrative (blocking) and not based on legal proceedings. The police and prosecutor's offices generally only act on complaints, not systemic institutional initiatives.

Second, from the aspect of resources, there is no real-time monitoring system used by the KPU and Bawaslu to detect and analyze the distribution of digital content that has the potential to violate the law. In fact, political disinformation works with a very fast pattern of algorithmic and network-based spread. The limitations of digital forensic technology, low verification capacity, and the absence of big data electoral monitoring are the main weak points in the institutional response to this phenomenon.

Third, normatively, technical regulations from the KPU and Bawaslu emphasize more on conventional campaign rules, and have not regulated in detail how digital political campaigns should be carried out with the principles of transparency and accountability. There is no obligation to report campaign funds used in digital platforms, no public repository for political ads, and no oversight of political buzzer/influencer activity on social media.

This situation is exacerbated by the absence of engagement mechanisms for global digital platforms such as Meta (Facebook, Instagram), Google (YouTube), and ByteDance (TikTok), which have a huge role in shaping public opinion but are not legally bound by national election regulations. In many other countries, such as the European Union and Germany, platforms are required to provide political advertising data, recommendation algorithms, and audit access to election watchdogs.

The normative and institutional conditions described above show that the electoral legal framework in Indonesia has not been designed to deal with the logic of digital disinformation that

is algorithmic, transnational, and non-linear. This means that the current law still relies on the old paradigm that places information as the result of communication between individuals whereas modern disinformation is generated by complex systemic structures, including digital platforms, hidden algorithmic campaigns, and political actors who are not formally registered.

This weakness not only has implications for the effectiveness of the law in the technical context of enforcement, but also touches on the aspect of the legitimacy of the law itself in guaranteeing substantive democracy. If the law is unable to protect voters from information manipulation, then the principle *of informed consent* in general elections loses its meaning. In other words, electability obtained through digital manipulation legalized due to a legal vacuum is essentially a new form of *electoral control* that is neither ethically nor constitutionally legitimate.

This condition confirms that the law is not enough just to be a means of formal enforcement of procedural violations, but must function as a tool to enforce substantive justice in favor of protecting the dignity of citizens as voters. Within the framework of Pancasila legal theory, justice is not only legal-formal, but must be "dignified", namely humanizing human beings and respecting their spiritual existence as God's created beings.

Furthermore, the failure to reorganize the electoral legal framework in the face of digital disinformation also opens up space for the strengthening of an information oligarchy, where political actors with access to capital, buzzer networks, and digital technology are able to control public narratives without adequate supervision. This situation is dangerous because it blurs the line between legal campaigns and destructive propaganda, as well as produces asymmetrical conditions in electoral competitions.

In that context, the legal approach is not enough if it only relies on the principle *of law enforcement*, but must shift towards *law as governance*, where law functions as a social engineering instrument that is able to regulate interactions between states, society, and digital platforms in building a fair and integrity information ecosystem.

In addition, the absence of a legal role in regulating the digital information architecture during elections is also contrary to the principles *of due process* and *electoral justice* which are the foundations of a democratic system. In this context, the law should not only be a formal protector of the right to vote, but also responsible for the quality of the information on which citizens' political decision-making is based.

Countries have shown that firm and proactive legal reforms against digital platforms can improve the effectiveness of election surveillance. The European Union, for example, through *the Digital Services Act*, requires platforms to provide algorithm transparency, open political ad data, and provide access to election supervisory authorities to conduct content audits (Liu et al., 2020). In Germany, the NetzDG (*Network Enforcement Act*) regulates the obligation for social media platforms to remove illegal content within 24 hours and to publish regular content handling reports. The regulation of digital political advertising is also a major focus in the context of digital democracy, as it is often used as a covert disinformation channel that is difficult to track publicly. (Bawaslu, 2020; Commission, 2022; Gunawan E. H., 2020)

There are a number of important implications for national legal policy, especially in the context of election governance in the digital era, including the State must get out of a reactive and formalistic position in dealing with digital disinformation. Elections can no longer be monitored with conventional legal tools as the field of competition has shifted to a digital space controlled by algorithmic logic and network structures. The supervisory function needs to be expanded not only to regulate election participants, but also to include digital media, platform service providers, as well as political agencies that are not formally registered.

In addition, the practical implication of the current weak coordination between institutions is the need to establish an independent body or special unit within the Bawaslu structure that functions as a supervisor of electoral digital content, with cyber forensic capacity, big data analysis, and the authority to intervene in algorithm-based campaigns. These institutions must have direct access to digital platforms and be supported by a clear legal framework. Also, the Government of Indonesia needs to encourage transparency policies for digital platform providers (such as Meta, Google, TikTok, and others) to open political advertising data, content distribution algorithms, and advertiser identities. These provisions are in line with the *Digital Services Act* (EU) approach and can be translated in the form of MoU, sectoral regulations, or legislative revisions.

CONCLUSIONS AND SUGGESTIONS

Disinformation and cyber propaganda in elections are a new form of threat to the quality of electoral democracy that is systemic, transnational, and based on algorithmic technology. This research shows that Indonesia's legal framework, including the *Election Law*, the *ITE Law*, and the technical regulations of election organizers, has not been effective enough in responding to the complexity of this phenomenon. The existing law is still oriented toward a repressive and casuistic approach and has not anticipated modern forms of information manipulation such as *deepfakes*, *microtargeting*, and *bot*-based campaigns. Normative weaknesses are exacerbated by the weak institutional supervision of digital information in elections. The absence of a single mandate, limited monitoring technology, and lack of collaboration between countries and digital platforms result in slow, unintegrated, and less systemic legal responses. This condition risks reducing democracy to a mere formal procedure without a guarantee of equal and rational information quality for all voters. Therefore, a holistic and proactive agenda for updating election law regulations is needed. The state must not be neutral toward the digital information infrastructure, which is now the main determinant of electoral contestation. The law must be present not only as a tool for post-violation enforcement but also as an instrument of fair, transparent, and democratic governance of the digital space. This reform is not only technically normative but is an ethical and constitutional call to maintain the integrity of elections as the main pillar of people's sovereignty.

Digital election law reform must be directed at the restoration of justice that is not only legalistic but also rooted in the values of dignified justice as affirmed in the legal theory of *Pancasila*. In Teguh Prasetyo's view, a just law is a law that is in harmony with human nature,

upholds its dignity and worth, and fights for the values of truth and holistic humanity. To support the effectiveness of legal protection for digital elections, the following is a proposal for reformulation or insertion of new norms in relevant regulations: namely, by revising the *Election Law* to insert the provisions of a new article, such as the insertion of article 280A, with the provision: "Every election participant is prohibited from using digital algorithms, automation technology, anonymous accounts, or other forms intended to spread misleading information, incite hatred, or manipulate public perception in a coordinated manner through digital platforms." Meanwhile, regarding the report on campaign funds, article 286 is inserted with an additional paragraph: "Campaign funds used in the form of digital promotions, including paid political advertisements on digital platforms, must be reported in detail and accessible to the public." In addition to the *Election Law*, it is also necessary to insert new norms in the *ITE Law*, namely, the addition of a special article on the responsibility of digital platforms regarding: "Operators of electronic systems used for political campaigns are required to provide reporting mechanisms, content transparency, and verification access by election supervisory institutions related to digital political activities on their platforms." Another addition concerns the provisions on political disinformation as a form of cybercrime in its own right, with elements of the dissemination of fake content carried out in a structured and massive manner, based on *artificial intelligence* (AI), *bots*, or automation, and content that has a direct impact on voter preferences or participation.

BIBLIOGRAPHY

Assyahida, T. N. (2025). Disinformasi Pemilu Digital sebagai Ancaman Transnasional: Implikasi terhadap Kedaulatan Demokrasi Indonesia. *Sosial Simbiosis: Jurnal Integrasi Ilmu Sosial dan Politik*, *2*(3), 97–106.

Bachtiar, F. R. (2014). Pemilu Indonesia: kiblat negara demokrasi dari berbagai refresentasi. *Jurnal Politik Profetik*, *2*(1).

Bawaslu, R. I. (2020). *Laporan Pengawasan Pemilu 2019*. Bawaslu Republik Indonesia.

Commission, E. (2022). Digital Services Act – Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022. *Official Journal of the European Union*, *L 277*.

Destavino, I., Habibi, M., & Syamsuri, M. R. (2023). Navigating Digital Deception: Unmasking Propaganda and Disinformation in the 2024 Elections. *TheJournalish: Social and Government*, *4*(4), 380–388.

Gunawan E. H., A. and S. (2020). Cyber propaganda and electoral democracy in Indonesia: A study on the 2019 presidential election. *Journal of ASEAN Studies*, *8*(2), 123–141.

Indonesia, K. K. dan I. R. (2023). *Laporan Tahunan Penanganan Konten Hoaks dan Disinformasi Tahun 2023*. Kominfo RI.

(KPU), K. P. U. (2018). *Peraturan Komisi Pemilihan Umum (PKPU) No. 23 Tahun 2018 tentang Kampanye Pemilu*. KPU RI.

Liu, G., Zhang, C., Zhao, M., Guo, W., & Luo, Q. (2020). Comparison of nanomaterials with other unconventional materials used as additives for soil improvement in the context of sustainable development: a review. *Nanomaterials*, *11*(1), 15.

Novarizal, R., Siregar, R. A., & Shiddiqy, M. A. A. (2025). Hate Crime Pasca Pemilihan Umum Presiden Tahun 2024 Di Indonesia. *Jurnal Kajian Pemerintah: Journal of Government, Social and Politics*, *11*(1), 66–82.

Nugroho, Y. (2020). Pemilu digital dan tantangan disinformasi di Indonesia: Tinjauan hukum dan tata kelola. *Jurnal Hukum dan Teknologi*, *4*(1), 45–62.

O'Callaghan, P. (2020). The regulation of political advertising in the digital age: International approaches and normative justifications. *International Journal of Law and Information Technology*, *28*(2), 153–178. https://doi.org/10.1093/ijlit/eaaa005

Prasetyo, T. (2015). *Keadilan Bermartabat: Perspektif Teori Hukum Pancasila* (Cet. ke-3). Genta Publishing.

(PSHK), P. S. H. dan K. I. (2023). *Laporan Evaluasi Regulasi Pemilu di Era Digital*. PSHK.

Sagala, C. S. T., & Nasution, M. (2022). Implementasi Pancasila di Tahun Politik. *Jurnal Adhyasta Pemilu*, *5*(2), 113–126.

Tahir, R., Kusmanto, H., & Amin, M. (2020a). *Propaganda Politik Hoaks dalam Pemilihan Presiden Tahun*. Perpektif.

Tahir, R., Kusmanto, H., & Amin, M. (2020b). Propaganda Politik Hoaks dalam Pemilihan Presiden Tahun 2019. *Perspektif*, *9*(2), 236–251.

Tambini, D. (2022). *Media freedom and regulation in the age of disinformation*. Palgrave Macmillan.

Tapsell, R. (2019). Deepening the crisis of democracy in Indonesia: Fake news and elections in a digital era. *Journal of Contemporary Asia*, *49*(4), 574–583. https://doi.org/10.1080/00472336.2019.1587900

Undang-Undang Republik Indonesia Nomor 7 Tahun 2017 tentang Pemilihan Umum, 182 (2017).

Utomo, N. A. S. H., & Yulianto, M. (2018). Analisis Isi: Propaganda dalam Pemberitaan VOA-ISLAM Terhadap Kepemimpinan Jokowi. *Interaksi Online*, *6*(4), 82–90.