The Easta Journal Law and Human Rights
Vol. 3, No. 03, June 2025, pp. 186 - 193
ISSN: 2985-7112, DOI: 10.58812/eslhr.v3i03

Legal Approaches to Combatting Information Warfare in the Age of Social Media and Misinformation in Indonesia

Emmi Rahmiwita Nasution
Universitas Asahan

Article Info

Article history:

Received Jun, 2025
Revised Jun, 2025
Accepted Jun, 2025

Keywords:

Disinformation;
Indonesia;
Information Warfare;
Legal Approaches;
Social Media Regulation

ABSTRACT

The proliferation of social media platforms in Indonesia has intensified the challenges of combating information warfare and disinformation, posing significant risks to public trust, democratic stability, and national security. This study explores legal approaches to addressing these issues, focusing on the strengths, limitations, and enforcement challenges of Indonesia's regulatory framework, particularly the Electronic Information and Transactions Law (UU ITE). Using a qualitative design, data were gathered through in-depth interviews with five key informants, including legal experts, policymakers, digital media analysts, and civil society representatives. The findings reveal that while the UU ITE provides a foundational legal structure, its effectiveness is hindered by ambiguous provisions, resource constraints, and limited collaboration with social media platforms. Recommendations include revising the UU ITE, enhancing capacity building for enforcement agencies, fostering international cooperation, and promoting public digital literacy. These insights contribute to a nuanced understanding of Indonesia's efforts to balance freedom of expression with the need for regulation in the digital era.

Corresponding Author:

Name: Emmi Rahmiwita Nasution
Institution: Universitas Asahan
Email: emminasution0303@gmail.com

1. INTRODUCTION

The rapid growth of social media has revolutionized communication by enabling real-time information sharing and the global spread of ideas, yet this digital transformation has also introduced significant challenges, notably the rise of disinformation and information warfare, which threaten societal stability, influence public opinion, undermine trust in institutions, and disrupt democratic processes. In Indonesia—one of the world's largest and most active social media markets—these issues are particularly pressing due to its diverse sociopolitical landscape and high digital engagement. The country experiences approximately 2,093 hoaxes annually, or about 175 per month, with disinformation often targeting public figures, political matters, and government affairs, primarily through platforms like YouTube, WhatsApp, and Facebook [1]. This has serious implications for democracy, as disinformation erodes public trust, distorts democratic mechanisms, and manipulates electoral outcomes [2]. Furthermore, phenomena like the "disinformation order" and the "algorithmic trap" can polarize political discourse and jeopardize the narrative of the Indonesian nation-state as well as its liberal

democratic values [3]. To address these threats, enhancing digital literacy and promoting transparency of information sources are key strategies [2], supported by initiatives such as the government-run platform https://klinikhoaks.jatimprov.go.id/ that empowers citizens to verify online information [1]. Additionally, international cooperation and the deployment of AI-driven tools are considered vital to protecting democratic integrity [2], [4].

Disinformation campaigns, often driven by political, ideological, or economic motives, thrive in the fast-paced and decentralized environment of social media by exploiting platform vulnerabilities to spread false narratives that incite polarization and conflict; this weaponization of information has evolved into a strategic tool in information warfare, where both state and non-state actors manipulate digital content to advance their objectives. For Indonesia, which holds a strategic geopolitical position and is actively working to strengthen its democratic governance, addressing these challenges is crucial, especially in the lead-up to the 2024 elections, as disinformation campaigns pose serious threats to democratic processes and societal cohesion by leveraging the unregulated dynamics of digital platforms. These campaigns make Indonesia a target for external influence operations, necessitating a multifaceted response that includes policy development, technological interventions, and public education. Research shows that misinformation and disinformation in Indonesia commonly manifest as hoaxes and clickbait, particularly centered on personal and social content [5], and proposes the adoption of the reeve model—comprising laws, standards, and co-regulation through independent institutions—as a regulatory framework to moderate content effectively [5]. Moreover, disinformation is increasingly identified as a hybrid threat, amplified by the extensive use of social media platforms that function as arenas for gray-zone conflicts between peace and war, where both state and non-state actors pursue financial, political, or ideological objectives, making it difficult for the public to differentiate between truth and falsehood [6]. The strategic use of information in political warfare directly affects national security and public perception, thus highlighting the urgency of establishing robust cybersecurity policies, advancing media literacy, and utilizing AI to combat such digital threats [7]. Global cases such as the U.S. 2016 presidential election and the Brexit referendum underscore how disinformation can distort political outcomes, reinforcing the need for systematic studies to detect, understand, and quantify the real-world impacts of these campaigns [8].

The Indonesian government has introduced several legal frameworks, notably the Electronic Information and Transactions Law (UU ITE), to regulate digital platforms and address issues such as online fraud, cybercrime, and the spread of disinformation; while these measures mark important progress, they have also sparked considerable debate due to ambiguous provisions that critics argue may lead to legal overreach and infringe upon freedom of expression and other fundamental rights. Articles 27(3) and 28(2) of the UU ITE, which criminalize defamation and hate speech, have been particularly contentious for their broad and vague formulations that risk being misused to suppress press freedom and dissent [9], [10], while Article 40(2)(b) permits government censorship, further fueling concerns over the suppression of legitimate expression [11]. These complexities underscore the need for a nuanced and balanced approach to combating information warfare that also safeguards civil liberties. The law's implementation has also faced practical challenges, including difficulties in identifying and prosecuting online perpetrators, limited investigative resources, and the complications of addressing cross-border cybercrimes, all of which hinder its effectiveness despite the presence of a formal legal framework [12]. Furthermore, the rapid pace of technological change and the need for harmonization with other national and international legal instruments add layers of difficulty to enforcement [12], [13]. In response, scholars and policymakers recommend revising the UU ITE to clarify problematic provisions,

narrow the scope of controversial articles, and enhance enforcement mechanisms [10], [11]. A comprehensive solution should also include international cooperation, the advancement of digital literacy, and the development of AI-based tools to support the early detection and prevention of cyber threats [12]. This study aims to examine the legal strategies employed in Indonesia to address the challenges posed by information warfare in the era of social media.

2. LITERATURE REVIEW

2.1 Information Warfare and Disinformation

Information warfare in the digital age has evolved into a sophisticated and non-contact global strategy that leverages the pervasive reach of social media to disseminate disinformation, manipulate public opinion, and achieve political, economic, or strategic objectives; this strategy is characterized by the intentional spread of false information designed to deceive and emotionally influence targeted audiences within echo chambers, exploiting the decentralized nature of digital platforms that enables rapid, unchecked dissemination of content and complicates efforts to verify and counter it. Information warfare systematically manipulates symbolic capital to influence social reality and public perception [14], utilizing tools such as disinformation and cyberattacks to advance its aims. Social media platforms like Facebook, YouTube, and Instagram play a pivotal role in this dynamic, particularly in global conflicts like the Russian-Ukrainian war, where propaganda is spread through bots, trolls, and fake narratives to manipulate mass consciousness [15]. The Brexit referendum similarly demonstrated the power of data-driven microtargeting and hyperpartisan content in conducting influence operations [16] To counter such threats, it is essential to understand the mechanisms of disinformation and apply strategic responses rooted in planning theory, truth theory, and military strategy, including frameworks like the "kill chain" which emphasize the need for systematic, phased countermeasures [17].

2.2 Legal Frameworks for Addressing Disinformation

Governments around the world are increasingly adopting legal measures to combat the spread of disinformation, though the approaches and challenges vary significantly by region. The European Union, for example, implemented the Code of Practice on Disinformation in 2018 as a self-regulatory initiative involving major digital platforms, emphasizing transparency and accountability through collaboration with technology companies; this framework has shown promising results, supported by regular reports from participants like Facebook and Google and its integration into broader legislation such as the Digital Services Act [18], [19]. In contrast, the United States faces significant challenges due to First Amendment protections, which limit the government's ability to regulate speech and thus rely primarily on voluntary actions by technology companies to mitigate disinformation [20]. Meanwhile, Indonesia enforces the Electronic Information and Transactions Law (UU ITE), which criminalizes the dissemination of false information to regulate digital communication; however, this law has been criticized for its overly broad provisions that may lead to selective enforcement and the suppression of free expression [20].

2.3 Social Media and Governance in Indonesia

Social media in Indonesia plays a pivotal role in shaping communication, information dissemination, and public discourse, offering both opportunities and challenges; while platforms like Facebook, Instagram, and TikTok have become essential tools for improving digital literacy by serving as primary sources of information [21], Indonesia still ranks low globally in literacy levels, underscoring the need for more targeted and effective interventions [21]. The rapid

spread of disinformation on these platforms—driven by algorithms that prioritize sensational content—has significantly impacted political, health, and social spheres, as seen during the COVID-19 pandemic when false context and misleading information were rampant [22]. In response, the Indonesian government has partnered with social media companies to improve content moderation, yet the effectiveness of these initiatives has been inconsistent, highlighting the urgent need for more robust, multifaceted strategies [23]. Encouragingly, media literacy efforts such as targeted online videos have shown measurable success, with a 64% reduction in participants' intention to share misinformation [24]. Moving forward, a comprehensive strategy that integrates legal frameworks, technological safeguards, and educational programs is essential to empower users to critically assess information, combat misinformation effectively, and preserve the democratic potential of social media [23].

2.4 Conceptual Framework for the Study

This study adopts a multidisciplinary approach, drawing on theories from communication studies, legal scholarship, and governance. It examines the interplay between legal instruments, social media dynamics, and societal impacts to identify effective strategies for addressing information warfare in Indonesia. By integrating insights from global best practices and local contexts, the research aims to provide actionable recommendations for policymakers and stakeholders.

3. RESEARCH METHODS

This study employs an exploratory qualitative design to capture the insights and experiences of key informants with deep knowledge of the legal, social, and technological aspects of information warfare in Indonesia. This approach is well-suited for examining complex issues that require interpretive understanding of human behavior, institutional practices, and policy implications. Using purposive sampling, five informants were selected for their expertise: a digital law expert, a policymaker, a representative from a social media platform, a digital media analyst, and a civil society advocate for digital rights. This selection ensured that the data collected would be both relevant and insightful.

Data were gathered through in-depth, semi-structured interviews conducted in person or online, depending on informant availability. The interview guide covered key themes such as the effectiveness of legal frameworks in addressing disinformation, enforcement challenges under the Electronic Information and Transactions Law (UU ITE), the role of social media platforms, balancing freedom of expression with security, and policy recommendations. Each interview lasted 60–90 minutes and was recorded with participant consent, accompanied by field notes. Thematic analysis was used to process the data through familiarization, open coding, theme development, and interpretation, grounded in relevant literature and theoretical frameworks to generate context-specific insights.

4. RESULTS AND DISCUSSION

4.1 Effectiveness of Current Legal Frameworks

The informants unanimously agreed that Indonesia's Electronic Information and Transactions Law (UU ITE) provides a foundational legal framework to address the misuse of digital platforms. They acknowledged its strengths, particularly in criminalizing the deliberate spread of false information, and emphasized its deterrent effect in critical situations such as elections and public health crises. The law was seen as a necessary instrument to counter large-scale disinformation campaigns that undermine public trust and social stability. However, several informants also pointed to significant weaknesses, especially the law's ambiguous language around terms like "false information" and

"public order," which allows for subjective interpretation and the risk of misuse. In some cases, the law has been applied not to combat disinformation, but to suppress dissenting voices, raising serious concerns about freedom of expression. These observations reflect earlier critiques [25], which argue that although the UU ITE addresses real challenges, its current form necessitates revisions to bring it into alignment with international human rights standards.

The critique of the UU ITE intersects with broader discussions on the universality of human rights and the obligation of states to harmonize national laws with international norms. Scholars such as Jack Donnelly argue against cultural relativism and emphasize the universal application of human rights, highlighting the importance of legal consistency across different societal contexts [26]. In this light, the shortcomings of the UU ITE illustrate the need for Indonesia to revise its legislation to uphold international human rights obligations and prevent conflicts between domestic law and global standards [27]. Moreover, effective implementation and monitoring mechanisms are vital to ensure that these standards are upheld in practice ("International human rights", 2022). Strengthening such mechanisms would not only reinforce Indonesia's commitment to human rights but also improve the credibility and fairness of its digital governance framework.

4.2 *Challenges in Enforcement*

Enforcement was identified by informants as a critical challenge in addressing information warfare in Indonesia. A key issue is the lack of resources within law enforcement agencies, including insufficient technical expertise and inadequate tools to effectively trace and combat complex disinformation campaigns. These limitations hinder the ability of authorities to respond swiftly and accurately to digital threats, leaving gaps in the national response to online manipulation.

Another major obstacle is the cross-border nature of disinformation, as many campaigns are orchestrated by foreign actors beyond Indonesia's legal jurisdiction. This global dynamic complicates enforcement efforts and underscores the need for international cooperation. Additionally, informants highlighted the ongoing struggle to balance regulatory efforts with the protection of civil liberties. Policymakers and law enforcement are frequently criticized—especially by civil society groups—for measures perceived as infringing on freedom of expression, making this balance a recurring and contentious issue in the broader conversation around digital governance.

4.3 *Role of Social Media Platforms*

Informants emphasized the critical role of social media platforms such as Facebook, Twitter, and TikTok in combating disinformation through various measures including content moderation, fact-checking initiatives, and algorithmic detection of false information. Despite these efforts, several limitations were noted. Inconsistent enforcement of content policies often leads to perceptions of bias or favoritism, undermining public trust in the platforms' neutrality. Additionally, the lack of transparency regarding how algorithms function and how decisions are made about content removal contributes to skepticism and reduces accountability.

Another key concern raised was the insufficient level of collaboration between social media companies and the Indonesian government. Although partnerships exist, informants pointed out that these are often limited in scope, particularly in terms of data sharing and coordinated responses to disinformation. This lack of robust engagement weakens the overall effectiveness of counter-disinformation efforts. As such, the findings highlight the urgent need to build stronger, more transparent

partnerships between government institutions and digital platforms to create a more resilient and coordinated approach to addressing the spread of false information.

4.4 Recommendations for Strengthening Legal Responses

Based on the insights provided by the informants, several recommendations emerged to improve Indonesia's legal and policy responses:

1. Revising the UU ITE:
   Clearer definitions and guidelines should be incorporated to reduce ambiguities and prevent misuse. Revisions should also include provisions to address new forms of digital threats.
2. Capacity Building:
   Investments in training and resources for law enforcement and judicial officials are necessary to enhance their ability to address complex cases involving digital platforms.
3. Public Awareness Campaigns:
   Informants emphasized the need for nationwide digital literacy programs to empower citizens to identify and counter disinformation.
4. International Cooperation:
   Strengthening collaborations with international organizations and neighboring countries could help Indonesia tackle cross-border disinformation campaigns more effectively.

4.5 Broader Implications

The findings of this study contribute to the broader understanding of legal strategies for combating information warfare in the digital age. They highlight the need for multidimensional approaches that integrate legal, technological, and societal interventions. Furthermore, the Indonesian experience offers valuable lessons for other countries grappling with similar challenges, particularly in balancing security concerns with democratic principles.

4.6 Discussion

The findings of this study align with global trends identified in the literature, where challenges such as ambiguous legal language and enforcement gaps are common across countries attempting to regulate digital platforms. In Indonesia, these challenges are compounded by a unique cultural and political context. For instance, the Ministry of Communication and Information Regulation No. 10 of 2021 (MR 10/2021) exemplifies the tension between asserting digital sovereignty and achieving effective governance. This regulation equates digital platforms with traditional businesses, aiming to assert state control; however, its implementation has revealed a disconnect between regulatory objectives and practical outcomes, highlighting the need for more context-sensitive legal instruments [28]. Similar issues are evident in the Personal Data Protection (PDP) Law, where vague definitions hinder enforcement [9], and a lack of independent oversight has led to repeated data breaches in major companies [29].

Indonesia's cultural and political complexity further complicates digital governance. With a highly diverse population, integrating local customs and values into national legal frameworks is crucial to ensure social acceptance and legal effectiveness [30]. Politically, the strong emphasis on digital sovereignty, as seen in MR 10/2021, reflects a state-centric approach that prioritizes territorial control over collaborative governance models [28]. To address these multilayered challenges, several recommendations have emerged: adopting sector-specific regulations tailored to the unique dynamics of digital platforms [28], and enhancing public engagement through education and awareness initiatives to foster stronger support for digital rights and privacy laws [9], [29]. These strategies underscore the need for a more nuanced and

participatory approach to digital regulation in Indonesia.

5. CONCLUSION

This study highlights the critical role of legal frameworks in addressing the growing threats of information warfare and disinformation in Indonesia. The UU ITE serves as a cornerstone in the country's regulatory efforts but requires significant revisions to address its ambiguities and adapt to evolving digital threats. Effective enforcement remains a challenge due to resource limitations, jurisdictional complexities, and the tension between regulation and freedom of expression.

The findings underscore the importance of a holistic approach, integrating robust legal measures, capacity-building initiatives, and public awareness campaigns to foster digital literacy. Enhanced collaboration with social media platforms and international entities is vital to combating cross-border disinformation and ensuring the efficacy of regulatory measures.

By implementing these recommendations, Indonesia can strengthen its resilience against information warfare, protect its democratic values, and serve as a model for other nations facing similar challenges in the digital era.

REFERENCES

[1] P. A. R. Dewi, A. Dharmawan, G. G. Aji, M. D. Winata, and J. Wahyuni, "Mapping Hoaxes, Disinformation, and Hate Speeches in Indonesia," *Tech. Soc. Sci. J.*, vol. 50, p. 559, 2023.

[2] T. Warin, "Disinformation in the Digital Age: Impacts on Democracy and Strategies for Mitigation," *Available SSRN 4995571*, 2024.

[3] N. Ahmad, "Disinformation Order and Social Media Algorithmic Trap: New Challenges for Sustainability of the Indonesia's United Nation-State Narrative and Liberal Democratic Norms," *Polit. Indones. Indones. Polit. Sci. Rev.*, vol. 7, no. 2, pp. 134–149, 2022.

[4] M. I. Wahab, "Weaponization of Social Media: Challenges and Responses".

[5] A. A. Rosyidah, F. Fajriyah, E. A. Galuh, and D. S. Ulfa, "Exploring Misinformation and Disinformation Towards 2024 Election: Patterns and Policy Recommendations," *Profetik J. Komun.*, vol. 17, no. 2, pp. 269–290.

[6] R. Ivančík and P. Nečas, "On disinformation as a hybrid threat spread through social networks," *Entrep. Sustain. Issues*, vol. 10, no. 1, p. 344, 2022.

[7] A. Anwer, "Cybersecurity and Political Warfare: The Weaponization of Information in the Digital Age," *Interdiscip. J. Humanit. Media, Polit. Sci.*, vol. 1, Dec. 2024, doi: 10.56830/IJHMPS12202402.

[8] R. Sliwa, "Disinformation campaigns in social media," 2020, *University of Stuttgart*.

[9] L. Judijanto, N. Solapari, and I. Putra, "An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia," *Easta J. Law Hum. Rights*, vol. 3, no. 01, pp. 20–29, 2024.

[10] "Juridical Analysis of Law Number 11 of 2008 on Electronic Information and Transactions (ITE) and its Impact on Creative Economy Development in Indonesia." doi: 10.58812/wslhr.v2i04.1366.

[11] T. T. P. Waluyo, E. Calista, D. P. Ratu, T. S. Ramli, and A. M. Ramli, "The Indonesian Electronic Information and Transactions within Indonesia's Broader Legal Regime: Urgency for Amendment?," *J. HAM*, vol. 12, p. 533, 2021.

[12] M. A. F. Syahril and A. Aris, "Strategies and Dynamics of Online Fraud in Indonesia: Tracing the Effectiveness of the Implementation of the Electronic and Transaction Information Act," *J. Law Justice*, vol. 2, no. 3, pp. 198–205, 2024.

[13] M. Lubis and F. A. Maulana, "Information and electronic transaction law effectiveness (UU-ITE) in Indonesia," in *Proceeding of the 3rd International Conference on Information and Communication Technology for the Moslem World (ICT4M) 2010*, IEEE, 2010, pp. C–13.

[14] Y. L. Bankovskaya, "Information warfare of the modern world," *Vestn. Samara State Tech. Univ. Ser. Philos.*, vol. 4, no. 3, pp. 75–80, 2022.

[15] I. Shmalenko and O. Mitina, "Social networks as an instrument of information warfare," 2024.

[16] M. Bastos, "Information Warfare," in *Brexit, Tweeted*, Bristol University Press, 2024, pp. 91–103.

[17] A. Dowse and S. D. Bachmann, "Information warfare: methods to counter disinformation," *Def. Secur. Anal.*, vol. 38, no. 4, pp. 453–469, 2022.

[18] C. E. Berdud, "The EU Code of Practice on Disinformation: An Example of the Self-Regulatory Trend in International and European Law," *Vis. Rev. Int. Vis. Cult. Rev. Int. Cult. Vis.*, vol. 16, no. 2, p. 10, 2024.

[19] A. M. Prokopovic and M. Vujović, "The European approach to regulating disinformation," *Facta Univ. Ser. Law Polit.*, pp. 175–183, 2021.

[20] J. Huang, "Information Warfare in the Digital Age: Legal Responses to the Spread of False Information under Public International Law," *J. Educ. Humanit. Soc. Sci.*, vol. 28, pp. 176–184, 2024, doi: 10.54097/46jmtq31.

[21] B. F. Aulia, S. S. Subarjah, and Y. Rahma, "Media Sosial Sebagai Sarana Peningkatan Literasi Digital Masyarakat," *J. Bima Pus. Publ. Ilmu Pendidik. Bhs. dan Sastra*, vol. 2, no. 2, pp. 86–93, 2024, [Online]. Available:

https://journal.aripi.or.id/index.php/Bima/article/view/806

[22] S. Yustitia and P. D. Asharianto, "Misinformation and disinformation of COVID-19 on social media in Indonesia," in *Proceeding of LPPM UPN "VETERAN" Yogyakarta Conference Series 2020–Political and Social Science Series*, 2020, pp. 51–65.

[23] W. M. Miarta, "Voter Behavior and Social Media Influence: A Case Study of Indonesia's 2024 General Election," *Riwayat Educ. J. Hist. Humanit.*, vol. 7, no. 4, pp. 2592–2600, 2024.

[24] T. W. Ford, M. Yankoski, M. Facciani, and T. Weninger, "Online Media Literacy Intervention in Indonesia Reduces Misinformation Sharing Intention.," *J. Media Lit. Educ.*, vol. 15, no. 2, pp. 99–123, 2023.

[25] E. W. E Aspinall, D. Fossati, B. Muhtadi, "Elites, masses, and democratic decline in Indonesia," *Democratization*, vol. 27, no. 4, pp. 505–526, 2019.

[26] T. Taufiqurokhman, E. Satispi, A. Andriansyah, M. Murod, and E. Sulastri, "The impact of e-service quality on public trust and public satisfaction in e-government public services," *Int. J. Data Netw. Sci.*, vol. 8, no. 2, pp. 765–772, 2024, doi: 10.5267/j.ijdns.2024.1.002.

[27] S. Strungaru, "International Human Rights Law: Frameworks and Responses," in *The Hidden Child Brides of the Syrian Civil War: Vulnerable and Voiceless in Human Rights Law and Practice*, Springer, 2024, pp. 51–66.

[28] M. R. Gumati, "Digital Sovereignty and State Power: Indonesia's Approach to Digital Platforms Regulation," *JISPO J. Ilmu Sos. dan Ilmu Polit.*, vol. 14, no. 1, pp. 99–126, 2024.

[29] A. S. Kriswandaru, B. Pratiwi, and S. Suwardi, "Efektivitas Kebijakan Perlindungan Data Pribadi di Indonesia: Analisis Hukum Perdata dengan Pendekatan Studi Kasus," *Hakim J. Ilmu Huk. dan Sos.*, vol. 2, no. 4, pp. 740–756, 2024.

[30] F. P. Disantara, "Innovative legal approaches for contemporary challenges in Indonesia," *Indones. J. Innov. Stud.*, vol. 25, no. 4, pp. 10–21070, 2024.