Journal of Cyber Law and Information Security
Volume 1, Number 1, 2022

# A Normative Legal Analysis of Social Media Platform Responsibility in Combating Misinformation in Indonesia

**Muhammad Dafa Bagus Efendi**[1*]

[1] Universitas Diponegoro, Semarang, Indonesia

## Abstract

**Article history:**
Received: March 12, 2022
Revised: April 06, 2022
Accepted: May 08, 2022
Published: June 30, 2022

**Keywords:**
Cyber Law, Digital Platform, Indonesia, Misinformation, Platform Responsibility.

**Identifier:**
Zera Open
Page: 57-76
https://zeraopen.com/journal/jclis

This article examines the responsibility of social media platforms in combating misinformation in Indonesia from a cyber law perspective. The discussion is guided by two questions: to what extent Indonesia's existing legal frameworks are effective in regulating platform responsibility, and why it is necessary to strengthen and clarify such responsibility. Using a normative legal approach, the study analyzes the ITE Law, Government Regulation Number 71 of 2019, and Ministerial Regulation Number 5 of 2020, supported by scholarly literature and selected public cases involving election-related and COVID-19 misinformation. The analysis shows that Indonesia's framework provides a legal basis for regulating unlawful electronic information and requiring platform compliance with takedown mechanisms. However, the framework remains partially effective because it does not clearly define preventive duties, transparency obligations, user remedies, or safeguards for freedom of expression. The article argues that clearer platform responsibility is essential to ensure proportional enforcement, legal certainty, public protection, and a more secure digital information environment.

*Corresponding author:
(Muhammad Dafa Bagus Efendi)

## 1. Introduction

The rapid expansion of social media has changed the structure of public communication in Indonesia by allowing information to circulate instantly, interactively, and across territorial boundaries. This transformation has strengthened democratic participation, but it has also created legal and governance problems when digital platforms become channels for misinformation, disinformation, hoaxes, and manipulative political or health narratives. In Indonesia, the problem is not merely technological. It intersects with public order, consumer protection, electoral integrity, public health, and constitutional guarantees of freedom of expression. Lim (2017) shows that algorithmic enclaves and social media polarization can intensify identity-based political conflict, while Mujani and Kuipers (2020) demonstrate that misinformation during the Indonesian election context was believed by significant segments of the electorate. These findings indicate that misinformation is not an isolated communication error, but a socio-legal problem that can affect collective decision-making.

The urgency of regulating platform responsibility became more visible through several public cases. During the election period, Reuters reported that Facebook, Twitter, Instagram, and WhatsApp were central arenas for political misinformation and coordinated online campaigns in Indonesia (Potkin & Da Costa, 2019). After post-election unrest, the government temporarily restricted access to some social media features, arguing that hoaxes had contributed to public disorder (Potkin, 2019). In the health sector, misinformation also became a serious issue during the COVID-19 pandemic. Tempo reported that the Ministry of

Communication and Informatics identified hundreds of coronavirus-related hoaxes circulating through social media (Tempo, 2020). Academic studies support this concern: Yustitia and Ashrianto (2020) found that COVID-19 disinformation circulated intensely through fact-checked claims, while Rahmawati et al. (2021) mapped pandemic-related disinformation and emphasized the need for digital and media literacy as part of the response.

Indonesia has developed several legal instruments to address unlawful online content. Law Number 11 of 2008 on Electronic Information and Transactions, as amended by Law Number 19 of 2016, provides the basic legal framework for electronic information, including provisions related to false and misleading information, hate-based content, and unlawful electronic distribution. Government Regulation Number 71 of 2019 further regulates electronic system operators, while Minister of Communication and Informatics Regulation Number 5 of 2020 on Private Electronic System Operators introduces obligations for private electronic system operators, including platform registration and content takedown mechanisms. These regulations show that Indonesia has moved from a user-centered model of punishment toward a broader governance model that also places responsibility on electronic system operators. However, the central issue is whether these rules are sufficiently effective, clear, proportionate, and accountable when applied to social media platforms.

Existing literature suggests that Indonesia's misinformation regulation still faces normative and practical gaps. Lee (2020) argues that online hoaxes have been framed as existential threats, which can justify securitized state responses such as

internet shutdowns. Prahassacitta (2021) also notes that the criminalization of disinformation must be limited by offense principles so that legal enforcement does not punish content that merely irritates the public without causing legally relevant harm. Prianto et al. (2021) add that the government response to COVID-19 fake news relied on monitoring, clarification, and public communication, but such measures still required coordination with digital platforms and public literacy. This concern is important because vague standards such as disturbing public order or causing public anxiety may create uncertainty for platforms, users, journalists, and civil society. At the same time, weak platform accountability may allow harmful misinformation to circulate rapidly before legal authorities can respond. Therefore, legal analysis must assess not only the existence of regulation, but also its coherence, enforceability, and compatibility with rights-based digital governance.

Based on this background, this article applies a normative legal approach to examine social media platform responsibility in combating misinformation in Indonesia. The study focuses on statutory norms, regulatory obligations, and legal principles governing electronic information and private electronic system operators. The research is guided by two questions: first, to what extent are Indonesia's existing legal frameworks effective in regulating social media platform responsibility in combating misinformation; and second, why is it necessary to strengthen and clarify the legal responsibility of social media platforms in addressing misinformation from a cyber law perspective. By addressing these questions, the article aims to clarify whether the current framework provides adequate legal certainty, public protection, and proportional accountability in the governance of misinformation.

## 2. Research Methods

This study uses a normative legal research method to examine the responsibility of social media platforms in combating misinformation in Indonesia. A normative approach is appropriate because the main focus of the study is not to measure public attitudes or platform behavior empirically, but to analyze legal norms, regulatory obligations, and principles of cyber law that govern electronic information and digital platform accountability. The study evaluates whether the existing legal framework provides sufficient legal certainty, enforceable obligations, and proportional mechanisms for addressing misinformation on social media platforms.

The legal materials used in this study consist of primary, secondary, and supporting materials. Primary legal materials include Law Number 11 of 2008 on Electronic Information and Transactions, as amended by Law Number 19 of 2016, Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions, and Minister of Communication and Informatics Regulation Number 5 of 2020 on Private Electronic System Operators. These instruments are selected because they form the core regulatory framework for electronic information, electronic system operators, unlawful online content, and content moderation obligations in Indonesia. Secondary legal materials include peer-reviewed journal articles discussing misinformation, platform governance, cyber law, disinformation, and digital rights. Reputable news reports are used only as contextual materials to illustrate misinformation-related cases in Indonesia, particularly during election-related unrest and the COVID-19 pandemic.

The analysis is conducted through statutory, conceptual, and analytical approaches. The statutory approach is used to identify the scope of legal obligations imposed on electronic system operators and the extent to which these obligations can be applied to social media platforms. The conceptual approach is used to interpret key concepts such as platform responsibility, misinformation, legal certainty, proportionality, and public interest in cyber law. The analytical approach is applied to assess whether the current framework is effective in responding to misinformation and whether further clarification of platform responsibility is necessary.

Data analysis is performed qualitatively by interpreting the content of legal provisions and comparing them with problems identified in academic literature and public cases. The effectiveness of regulation is assessed through three indicators: clarity of norms, enforceability of obligations, and balance between misinformation control and freedom of expression. The urgency of strengthening platform responsibility is analyzed by considering the risks of regulatory ambiguity, rapid content circulation, public harm, and the need for accountable digital governance. This method enables the study to provide a systematic legal assessment of Indonesia's current framework and its relevance for cyber law development.

## 3. Results and Discussion

### 3.1. To What Extent Are Indonesia's Existing Legal Frameworks Effective in Regulating Social Media Platform Responsibility in Combating Misinformation?

Indonesia's existing legal framework shows a serious attempt to regulate misinformation in the digital sphere, but its effectiveness remains partial. The main legal instruments relevant to this issue are Law Number 11 of 2008 on Electronic Information and Transactions, as amended by Law Number 19 of 2016, Government Regulation Number 71 of 2019, and Minister of Communication and Informatics Regulation Number 5 of 2020 on Private Electronic System Operators. From a normative legal perspective, these regulations provide a foundation for controlling unlawful electronic information, requiring electronic system operators to ensure the reliability and security of their systems, and enabling the government to request the removal of prohibited online content. However, the effectiveness of this framework depends not only on the existence of legal norms, but also on whether the norms clearly define platform responsibility, can be enforced consistently, and protect the balance between public order and freedom of expression.

The ITE Law is important because it establishes the basic legal basis for addressing harmful online content. It prohibits the distribution of certain forms of unlawful electronic information, including false and misleading information that causes consumer loss, content that violates decency, defamation, threats, and hate-based provocation. In relation to misinformation, the strongest connection is Article 28, which regulates false and misleading information causing consumer loss and

information intended to create hatred or hostility based on ethnicity, religion, race, and intergroup identity. This framework is useful when misinformation produces concrete legal harm, such as fraud, public hostility, or consumer deception. However, misinformation on social media is often more complex than a single unlawful statement. Tandoc et al. (2018) explain that fake news can include fabrication, manipulation, propaganda, advertising, satire, and parody, each with different levels of facticity and intention to deceive. This typology shows why legal treatment of misinformation must be careful. A regulation that treats all false information in the same way may become overbroad, while a regulation that only punishes individual users may fail to address the platform systems that amplify misinformation.

The effectiveness of Indonesia's framework is also limited because the ITE Law was originally designed around electronic information and prohibited acts, not specifically around platform governance. Social media platforms are not passive intermediaries. Their content recommendation systems, community standards, reporting mechanisms, and moderation policies influence what information becomes visible, viral, or suppressed. Gorwa (2019) argues that platform governance involves relationships among platform companies, users, advertisers, governments, and political actors. This concept is relevant for Indonesia because misinformation is not produced only by individual users. It is also shaped by platform architecture, algorithmic amplification, coordinated networks, and moderation decisions. Therefore, a legal framework that focuses mainly on unlawful content may be insufficient if it does not clearly regulate the procedural duties of platforms.

Government Regulation Number 71 of 2019 strengthens the regulatory position by classifying and regulating electronic system operators. It requires electronic system operators to operate reliable, secure, and responsible systems. Normatively, this creates a broader basis for expecting social media platforms to maintain a safe digital environment. However, the regulation still does not provide detailed standards on what platform responsibility means in the context of misinformation. It does not clearly explain whether responsibility includes proactive detection, fact-checking cooperation, transparency reporting, algorithmic risk assessment, user appeal mechanisms, or rapid response during public emergencies. As a result, platform responsibility may depend heavily on government requests or the platform's own private policies. This creates a gap between formal legal authority and practical control over misinformation.

Ministerial Regulation Number 5 of 2020 provides a more specific mechanism by requiring private electronic system operators to register and comply with content governance obligations. It also gives the government authority to order platforms to remove or disable access to prohibited electronic information. This is an important development because it moves Indonesian cyber law closer to a platform responsibility model. Instead of relying only on criminal enforcement against content creators or spreaders, the regulation recognizes that platforms have a role in controlling the circulation of unlawful content. Nevertheless, its effectiveness is still constrained by several normative weaknesses. First, the category of prohibited content may be interpreted broadly, especially when connected to public order or disturbing society. Second, the mechanism emphasizes takedown compliance, but it

does not fully establish transparency obligations for platforms and government agencies. Third, the regulation focuses on content removal after a problem is identified, while misinformation often produces harm through speed, repetition, and virality before formal takedown can occur.

The Indonesian experience shows that misinformation can produce social and political consequences before legal mechanisms respond. Lim (2017) argues that social media can contribute to algorithmic enclaves, where users are repeatedly exposed to identity-based narratives that reinforce polarization. In the electoral context, Mujani and Kuipers (2020) found that misinformation during the 2019 Indonesian election was believed by parts of the electorate, showing that false political information can influence public perception. These findings are consistent with Reuters' reporting that social media platforms became battlegrounds for political misinformation and buzzer activity during the election period (Potkin & Da Costa, 2019). From an effectiveness perspective, this suggests that the existing framework is reactive. It can punish certain unlawful acts or order removal, but it has not fully addressed the structural conditions that allow misinformation to spread quickly through platform systems.

A similar problem appears in the health context. During the COVID-19 pandemic, misinformation was not only a communication issue, but also a public health risk. Yustitia and Ashrianto (2020) show that COVID-19 disinformation in Indonesia involved misleading claims that circulated through digital media, while Rahmawati et al. (2021) found that pandemic-related disinformation was dominated by health hoaxes and required media literacy responses. Prianto et al. (2021) also

explain that the government responded to the infodemic through monitoring, clarification, and public communication. These responses were important, but they also reveal that misinformation governance cannot rely only on state clarification after hoaxes have spread. Because social media platforms control the speed and scale of content circulation, their legal responsibility should be clearer than merely responding to takedown requests.

The current framework is therefore moderately effective in creating a legal basis for action, but less effective in creating a comprehensive platform accountability system. It provides authority for the government to respond to unlawful content and requires private electronic system operators to comply with certain obligations. However, it does not yet provide sufficient clarity on preventive duties, transparency standards, due process protections, and the distinction between harmful misinformation and protected expression. Prahassacitta (2021) warns that disinformation offenses must be limited by proper offense principles so that criminal law does not punish content merely because it is unpopular, annoying, or controversial. This warning is important because excessive content control may weaken digital rights, while weak control may allow harmful misinformation to damage public trust and security. Thus, the effectiveness of the current legal framework remains conditional: it is useful as a basic enforcement instrument, but insufficient as a complete model of social media platform responsibility.

### 3.2. Why Is It Necessary to Strengthen and Clarify the Legal Responsibility of Social Media Platforms in Addressing Misinformation from a Cyber Law Perspective?

The strengthening and clarification of platform responsibility is necessary because misinformation creates harms that are difficult to address through individual liability alone. Traditional legal enforcement tends to focus on the person who creates or spreads unlawful content. This approach remains important, especially when misinformation involves fraud, hate speech, or deliberate provocation. However, social media misinformation does not spread only because one person publishes false information. It spreads because digital platforms provide tools for instant sharing, algorithmic recommendation, group-based distribution, and viral engagement. Juditha (2018) shows that social media is a major channel for hoax circulation in Indonesia and that hoaxes create confusion, doubt, slander, and hatred. If the harm is amplified by platform systems, then cyber law must also address the responsibility of platforms as digital intermediaries.

From a cyber law perspective, platform responsibility is urgent because platforms occupy a strategic position between users, information, and the state. They are not identical to publishers, because they do not produce all content posted by users. However, they are also not fully neutral conduits, because they design the rules, algorithms, and moderation processes that shape information visibility. Gorwa (2019) describes platform governance as a structure involving formal and informal regulation among platforms, governments, users, and other stakeholders. This means that legal responsibility should not be understood only as punishment after

harm occurs. It should also include governance duties, such as having clear reporting channels, responding to lawful notices, explaining moderation decisions, cooperating with trusted fact-checkers, preserving user rights, and publishing transparency reports.

Clarification is also necessary to reduce legal uncertainty. Current Indonesian regulations provide several legal bases for content control, but they do not always distinguish clearly between misinformation, disinformation, malinformation, satire, opinion, error, and unlawful falsehood. Tandoc et al. (2018) emphasize that fake news is not a single category; it includes different forms of false or misleading content with different levels of intent and factual distortion. Without clear definitions, platform responsibility may become inconsistent. Platforms may remove too much content to avoid sanctions, or they may remove too little because legal duties are ambiguous. Both outcomes are problematic. Excessive removal can harm freedom of expression and public debate, while insufficient moderation can endanger public order, public health, and electoral integrity.

The urgency is especially visible in cases where misinformation affects public security. The temporary restriction of social media features after post-election unrest illustrates how the state may use broad intervention when misinformation is considered a threat to public order (Potkin, 2019). Lee (2020) argues that online hoaxes in Indonesia have been framed as existential threats, which can justify securitized measures such as internet shutdowns. Such measures may be effective in slowing the spread of harmful content, but they also affect many lawful users and can limit access to legitimate information. If platform responsibility were clearer, the

state might rely less on broad restrictions and more on targeted, accountable, and proportionate measures. Clear platform duties could support faster content review, better escalation channels, and more transparent cooperation between government and platforms.

The health misinformation context further strengthens the argument. Tempo reported that hundreds of coronavirus-related hoaxes were identified by the Ministry of Communication and Informatics, showing the scale of the problem during a public health emergency (Tempo, 2020). Rahmawati et al. (2021) also found that COVID-19 disinformation in Indonesia included many health-related hoaxes, while Yustitia and Ashrianto (2020) analyzed the circulation of COVID-19 disinformation through a disinformation triangle. These studies show that misinformation can directly influence risk perception, health behavior, and trust in official information. In this context, platform responsibility should not be limited to removing unlawful content after a government order. Platforms should also be expected to support public interest measures, such as reducing the visibility of demonstrably false harmful claims, directing users to authoritative information, and cooperating with fact-checking institutions.

Strengthening platform responsibility is also important for legal accountability. Ministerial Regulation Number 5 of 2020 creates a more direct relationship between the government and private electronic system operators, but stronger accountability requires clearer procedural safeguards. The regulation should not only empower the state to request takedowns; it should also require transparency about the number of requests, the legal basis for requests, the time taken to respond,

and whether users have access to appeal or correction mechanisms. Without these safeguards, platform responsibility may become a one-sided compliance obligation rather than an accountable governance system. In democratic cyber law, the legitimacy of content regulation depends on both effectiveness and rights protection.

Another reason for clarification is the cross-border nature of social media platforms. Many dominant platforms operate globally, while Indonesian law applies territorially to harms occurring within Indonesia or services accessed by Indonesian users. This creates enforcement difficulties. Platforms may apply global community standards that do not fully reflect Indonesian legal categories, while Indonesian authorities may issue takedown requests based on national laws. Clearer regulation can reduce conflict between private rules and public law by establishing minimum responsibilities for platforms operating in Indonesia. These responsibilities should be predictable, transparent, and proportionate, so that platforms understand their obligations while users remain protected from arbitrary removal or surveillance.

Finally, strengthening platform responsibility is urgent because misinformation threatens information security in a broad sense. Information security is not only about protecting systems from hacking, data theft, or malware. It also concerns the integrity, reliability, and trustworthiness of the information environment. When misinformation circulates widely, the public may lose confidence in institutions, scientific information, electoral processes, and legal authority. Lim (2017) shows that social media polarization can intensify identity-based divisions, while Mujani and Kuipers (2020) demonstrate that misinformation can shape political belief. These harms are relevant to cyber law because they show

that the digital information ecosystem needs governance that protects both security and rights.

Therefore, the legal responsibility of social media platforms should be strengthened and clarified through a more coherent regulatory model. Such a model should define misinformation-related obligations, distinguish harmful falsehood from lawful expression, require transparent moderation procedures, and create proportionate enforcement mechanisms. It should also encourage cooperation among government, platforms, fact-checkers, civil society, and users. The objective is not to impose unlimited liability on platforms or to transform them into state censors. Rather, the objective is to ensure that platforms with significant control over digital communication take reasonable, accountable, and rights-sensitive measures to reduce harmful misinformation. From a cyber law perspective, this clarification is essential for building legal certainty, protecting public interest, and maintaining a secure digital information environment.

## 4. Conclusion

This study concludes that Indonesia's existing legal framework has provided an important foundation for regulating misinformation on social media, but it has not yet fully established a clear and comprehensive model of platform responsibility. The ITE Law, Government Regulation Number 71 of 2019, and Ministerial Regulation Number 5 of 2020 show that Indonesian cyber law already recognizes the need to regulate unlawful electronic information and impose obligations on electronic system operators. These instruments allow the state to respond to harmful

digital content through enforcement, system governance, and takedown mechanisms. However, their effectiveness remains limited because the current framework still focuses heavily on prohibited content and government-initiated removal, while the preventive and procedural responsibilities of social media platforms remain insufficiently defined.

In relation to the first research question, the effectiveness of existing regulation can be considered partial. The regulations are effective to the extent that they provide a legal basis for controlling unlawful online content and requiring private electronic system operators to comply with state orders. Nevertheless, they are less effective in addressing misinformation as a platform-governance issue. Misinformation spreads through speed, algorithmic amplification, user networks, and coordinated activity, which cannot be handled adequately through individual liability or reactive takedown alone. The current rules also leave several uncertainties, including the definition of harmful misinformation, the scope of platform obligations, transparency requirements, appeal mechanisms, and safeguards for freedom of expression. Therefore, the existing framework is useful but not yet sufficient to ensure consistent, accountable, and rights-sensitive platform responsibility.

In relation to the second research question, strengthening and clarifying platform responsibility is necessary because social media platforms occupy a central position in Indonesia's digital information ecosystem. Platforms are not merely neutral intermediaries, since their design, moderation systems, reporting channels, and recommendation mechanisms influence the visibility and circulation of

information. When misinformation affects elections, public health, social harmony, or public trust, weak platform accountability may create broader risks for cyber law and information security. At the same time, unclear regulation may encourage excessive content removal or broad state intervention, which can threaten freedom of expression and access to information. For this reason, platform responsibility should be clarified through proportionate legal standards that distinguish harmful falsehood from lawful opinion, satire, criticism, or ordinary error.

Overall, the study argues that Indonesia needs a more coherent model of platform responsibility in combating misinformation. Such a model should include clearer definitions, preventive duties, transparent takedown procedures, user remedy mechanisms, cooperation with fact-checking institutions, and regular transparency reporting. Legal reform should not aim to transform platforms into state censors or impose unlimited liability for all user-generated content. Instead, it should require platforms to take reasonable, accountable, and rights-based measures against demonstrably harmful misinformation. By strengthening this framework, Indonesian cyber law can better protect public interest, legal certainty, democratic communication, and the integrity of the digital information environment.

## References

Gorwa, R. (2019). What is platform governance? *Information, Communication & Society, 22*(6), 854–871.

Juditha, C. (2018). Hoax communication interactivity in social media and anticipation (Interaksi komunikasi hoax di media sosial serta antisipasinya). *Jurnal Pekommas, 3*(1), 31–44

Lee, A. (2020). Online hoaxes, existential threat, and internet shutdown: A case study of securitization dynamics in Indonesia. *Journal of Indonesian Social Sciences and Humanities, 10*(1), 17–34.

Lim, M. (2017). Freedom to hate: Social media, algorithmic enclaves, and the rise of tribal nationalism in Indonesia. *Critical Asian Studies, 49*(3), 411–427.

Mujani, S., & Kuipers, N. (2020). Who believed misinformation during the 2019 Indonesian election? *Asian Survey, 60*(6), 1029–1043.

Potkin, F. (2019, May 22). Indonesia curbs social media, blaming hoaxes for inflaming unrest. *Reuters*. Retrieved Jan 21, 2022 from https://www.reuters.com/article/world/indonesia-curbs-social-media-blaming-hoaxes-for-inflaming-unrest-idUSKCN1SS1LV/

Potkin, F., & Da Costa, A. B. (2019, March 12). In Indonesia, Facebook and Twitter are "buzzer" battlegrounds as elections loom. *Reuters*. Retrieved Feb 14, 2022 from https://www.reuters.com/article/world/in-indonesia-facebook-and-twitter-are-buzzer-battlegrounds-as-elections-loom-idUSKBN1QU0AQ/

Prahassacitta, V. (2021). Offences principles and a limitation for disinformation via the internet in Indonesia. *Indonesian Law Journal, 14*(1), 37–51.

Prianto, A. L., Abdillah, A., Syukri, S., Muhammad, F., & Yama, A. (2021). Combating infodemic Covid-19: Government response against fake news on social media. *Profetik: Jurnal Komunikasi, 14*(2), 255–275.

Rahmawati, D., Mulyana, D., Lumakto, G., Viendyasari, M., & Anindhita, W. (2021). Mapping disinformation during the COVID-19 in Indonesia: Qualitative content analysis. *Jurnal ASPIKOM, 6*(2), 222–234.

Tandoc, E. C., Lim, Z. W., & Ling, R. (2018). Defining "Fake News": A typology of scholarly definitions. *Digital Journalism, 6*(2), 137–153.

Tempo. (2020, March 18). Govt finds 242 hoaxes and disinformation on coronavirus. *Tempo.co English*. Retrieved Feb 14, 2022 from https://en.tempo.co/read/1320779/govt-finds-242-hoaxes-and-disinformation-on-coronavirus

Yustitia, S., & Ashrianto, P. D. (2020). An analysis on COVID-19 disinformation triangle in Indonesia. *Komunikator, 12*(2), 116–128.