The Principle of Prudence in the ITE Law on Love Scam Cases

Yuliana Dewi Purnama Sari[1], Arista Candra Irawati[2]
[1,2]Faculty of Economics, Law, and Humanities, Universitas Ngudi Waluyo
Email Correspondence: yulianadewii27@gmail.com

Abstract

This research explores how the prudential principle is applied within Indonesia's Information and Electronic Transactions Law (ITE Law) in responding to romance-scam offenses conducted via social media. The swift expansion of digital communication has enabled the emergence of new cybercrime patterns, particularly deceptive romantic schemes that inflict financial and emotional losses on victims. Employing a normative juridical method, this study evaluates the degree to which the ITE Law integrates the prudence principle as a basis for preventing, identifying, and enforcing actions against online romance fraud. The results indicate that, although the ITE Law outlines a broad regulatory structure for digital conduct, its prudence-related preventive measures remain limited and demand clearer interpretation from law enforcement bodies. Reinforcing the prudential standard in online interactions is crucial to improving public awareness, ensuring legal clarity, and safeguarding individuals from cyber-based romantic manipulation.

Keywords: ITE Law; Love Scam; Prudence Principle

Introduction

The swift expansion of digital communication technologies has given rise to various emerging cybercrimes, including romance scam schemes, where offenders fabricate online intimate relationships to deceitfully obtain financial gain or manipulate victims emotionally (A. Setyowati, 2023). This issue poses significant difficulties for law-enforcement authorities as well as the legal regime governing electronic transactions in Indonesia. Although Law No. 11 of 2008 on Information and Electronic Transactions, as revised by Law No. 19 of 2016, regulates digital activities, the implementation of the prudential principle (asas kehati-hatian) in deterring and addressing these offenses is still not clearly defined.(Law No. 11 of 2008 on Information and Electronic Transactions, n.d.).

To prevent any alleged losses, in legal theory every person must act according to the prudential principle. The use of information technology requires of the prudential principle in electronic transactions, emphasizing the need to take into account and anticipate any risks or losses that may occur. Of the prudential principle represents a preventive legal norm designed to encourage responsible behavior and shield digital users from various forms of exploitation or improper use of information (Law Insider, n.d.). The principle of prudence (asas kehati-hatian) is a foundational concept in both civil and criminal law, referring to a legal duty that obliges individuals or institutions to act cautiously to avoid causing harm to others (Peter Mahmud Marzuki, 2022). In Indonesian law, prudence is reflected in various sectors, such as financial regulation, environmental management, and information technology (L. Widyastuti, 2022). Within the ITE Law, this principle implicitly guides users and service providers to behave responsibly in digital interactions, ensuring that electronic information and transactions are conducted safely and ethically

As love scam crimes proliferate across digital platforms, victims often face difficulties in obtaining justice due to regulatory gaps (R. Siregar, 2024). Hence, this study explores how the prudence principle is integrated within the ITE Law and how it may serve as a normative basis for legal protection against romance-based cyber fraud.

Research Method

This study adopts a normative juridical approach by reviewing written legal norms, statutory regulations, and judicial interpretations concerning prudence and cybercrime. The method is grounded in doctrinal examination of primary legal sources such as the ITE Law and the Indonesian Criminal Code and secondary references, including academic articles, legal commentaries, and international publications. The analysis is conducted qualitatively, emphasizing the alignment between the prudential principle and the state's duty to safeguard individuals engaged in digital transactions.

Result and Discussion

Normative Basis of Prudence in the ITE Law

Article 3 of the ITE Law states that the utilization of information technology must be carried out based on the values of "prudence, justice, and legal certainty." This provision reflects the legislature's intention to ensure that every digital interaction whether involving communication, data exchange, or electronic transactions adheres to responsible and accountable conduct. The inclusion of prudence as a foundational principle signifies that users, service providers, and digital platforms are expected to anticipate potential risks, prevent harmful practices, and act with careful consideration in managing electronic information. At the same time, the principles of justice and legal certainty aim to guarantee fairness in the digital sphere and provide clear guidance for resolving disputes or violations. Together, these principles form an ethical and legal framework that not only regulates online activities but also strengthens public trust in the digital environment, emphasizing the need for a balanced, safe, and transparent use of information technology in Indonesia (Law No. 11 of 2008 on Information and Electronic Transactions, n.d.).

However, the law does not provide a clear explanation of how the principle of prudence should function in practical terms. In the absence of detailed operational guidance, various digital actors such as platform providers, electronic intermediaries, and individual users frequently fail to recognize or fulfill their responsibility to anticipate risks and prevent potential harm in online interactions. This lack of clarity weakens the preventive function of the ITE Law, particularly in addressing forms of digital deception that continue to evolve, including romance scam schemes. If the principle of prudence were formulated with more explicit standards or operational indicators, it could serve as a stronger legal basis for early detection, proactive supervision, and timely intervention by both platforms and law-enforcement authorities. A more precise legal articulation would not only enhance the accountability of digital actors but also reinforce the state's capacity to prevent fraudulent online behavior before it escalates, thereby offering greater protection to potential victims of cyber-based romantic fraud (L.S. Nasution, 2024).

The Legal Gap in Regulating Love Scams

Although romance scams clearly exhibit elements of fraudulent conduct, they continue to fall within a legal gray zone under Indonesia's current cybercrime framework. The absence of a specific statutory provision addressing online romantic deception forces prosecutors to rely on a combination of cyber-related and conventional fraud articles to pursue such cases.

In practice, authorities often use Article 28(1) of the ITE Law, which stipulates that:

"Any person who knowingly and without authority disseminates false and misleading information that causes consumer losses in an electronic transaction shall be subject to criminal liability."

This provision is then paired with Article 378 of the Indonesian Criminal Code, which provides:(Indonesian Penal Code (KUHP), n.d.)

"Any person who, with the intent of unlawfully benefiting themselves or another person, induces someone to surrender property, extend credit, or cancel a debt through the use of a false name, false status, deceit, or a series of lies, shall be punished for fraud with imprisonment of up to four years."

The combined application of these provisions illustrates the legal system's difficulty in fitting technologically driven manipulative behaviors into traditional criminal categories. This blending of norms also produces varying interpretations among investigators and judges, resulting in inconsistent law enforcement. Consequently, despite the clearly deceptive and exploitative nature of love scams, their classification remains ambiguous, highlighting the urgent need for more explicit regulatory guidance within Indonesia's cyber law regime.

Yet these provisions do not explicitly capture emotional manipulation or digital romance fraud. While the statutory language addresses false information and material deception, it remains silent on deceptive practices that exploit victims' emotions, trust, and psychological vulnerability in online relationships. Romance scam schemes often involve prolonged interactions, constructed identities, and persuasive emotional tactics that fall outside the narrow definitions of misleading information or traditional fraud elements. As a result, many forms of digital romantic deception evade precise legal categorization, creating significant challenges for investigators and prosecutors who must interpret outdated concepts within a rapidly evolving technological context.

The lack of explicit recognition of emotional exploitation in the existing legal framework also limits the state's ability to provide adequate protection and redress for victims, whose losses are not only financial but also psychological. This gap underscores the need for a clearer and more

comprehensive regulatory approach that acknowledges the complex nature of online romantic manipulation as a distinct and serious form of cybercrime (L.S. Nasution, 2024). The absence of a clear prudential clause leads to inconsistent legal interpretations.

Strengthening Prudence as a Preventive Legal Value

To enhance protection, the prudence principle should be explicitly operationalized in cyber regulations. Embedding this principle into concrete regulatory standards would provide clearer guidance for digital platforms, service providers, and users regarding their duty to anticipate and mitigate risks in online interactions. Rather than functioning merely as an abstract legal value, prudence could be translated into specific obligations such as verifying user identities, implementing risk-based monitoring systems, educating the public about digital deception, and establishing mechanisms for early detection of suspicious behavior.

By giving the prudential principle a tangible operational form, the regulatory framework would better support preventive measures, reduce interpretive ambiguities, and strengthen law-enforcement efforts in addressing complex cybercrimes such as romance scams. A more detailed articulation of prudence would also contribute to greater legal certainty and accountability, ensuring that digital actors play an active role in safeguarding users from exploitation in the increasingly dynamic and interconnected online environment (F.A Putri, 2024).

This could include obligations for social media platforms to verify user identities, public awareness campaigns on online fraud, and digital literacy programs emphasizing ethical interaction. In practice, such measures would require digital service providers to adopt more robust verification systems to reduce the presence of fake accounts, which are frequently used as tools for romance scams and other forms of online deception. Public awareness initiatives could further educate users about common fraud indicators, manipulative communication patterns, and the psychological strategies scammers often employ to gain trust. Equally important, digital literacy programs that highlight responsible and ethical online behavior would empower individuals to navigate digital spaces more safely and critically. These combined efforts would not only strengthen preventive mechanisms at the platform level but also enhance societal resilience by equipping users with the knowledge and skills needed to recognize and avoid potential risks. Ultimately, integrating such obligations into cyber regulations would contribute to a more secure, transparent, and ethically grounded digital environment (S.M. Pratama, 2023).

From a policy perspective, prudence bridges the gap between preventive ethics and legal enforcement, promoting a safer digital environment. As a guiding principle, prudence encourages individuals, institutions, and digital platforms to act with foresight and responsibility, anticipating potential harms before they materialize. When incorporated into regulatory frameworks, this principle provides a normative foundation that supports proactive interventions rather than relying solely on punitive measures after violations occur. It enables policymakers to design rules that prioritize risk mitigation, user protection, and ethical online conduct, ensuring that safety considerations are embedded into the architecture of digital governance. Furthermore, prudence fosters collaboration between government agencies, technology companies, and civil society by emphasizing shared responsibility in preventing cybercrime. In this way, the principle serves not only as a moral compass but also as a strategic regulatory tool that strengthens the coherence between ethical expectations and formal enforcement mechanisms, ultimately contributing to a more trustworthy and resilient digital ecosystem (R.H. Dewi, 2025).

Conclusion

The study concludes that the principle of prudence under Indonesia's ITE Law remains a latent value rather than an enforceable standard. While it is acknowledged in the law's preamble and objectives, its absence in procedural and enforcement provisions limits its effectiveness in combating love scam crimes. Strengthening prudence through statutory amendment, regulatory guidelines, and user education is crucial for developing a comprehensive legal protection framework in cyberspace. Future reforms should integrate prudence as both an ethical and legal obligation ensuring that digital interactions are grounded in caution, responsibility, and respect for the rights of others.

References

A. Setyowati. (2023). Cyber Romance Fraud in Indonesia: Legal Perspective on Online Deception. *Jurnal Hukum Dan Teknologi Informasi*, *5*(2), 112.

F.A Putri. (2024). Prudence as a Preventive Legal Principle in Cyber Regulation. *Journal of Law*

and Technology, *5*(2), 60.
Indonesian Penal Code (KUHP).
L. Widyastuti. (2022). Prinsip Kehati-hatian dalam Regulasi Hukum Indonesia. *Jurnal Legislasi Indonesia*, *19*(3), 45.
L.S. Nasution. (2024). Ethical Dimensions of Prudence in Digital Regulation. *Journal of Cyber Ethics and Law*, *2*(1), 22.
Law Insider. (n.d.). *Definition of Principle of Prudence*. https://www.lawinsider.com/dictionary/principle-of-prudence
Peter Mahmud Marzuki. (2022). *Pengantar Ilmu Hukum*. Kencana.
R. Siregar. (2024). Challenges in Prosecuting Online Fraud under Indonesia's ITE Law. *Indonesian Journal of Cyber Law*, *4*(1), 77.
R.H. Dewi. (2025). Shared Responsibillity in Preventing Cyber Love Scams. *Indonesian Law Review*, *7*(1), 40.
Law No. 11 of 2008 on Information and Electronic Transactions.
S.M. Pratama. (2023). State Responsibillity in Building a Safe Digital Ecosystem. *Jurnal Kebijakan Dan Teknologi Informasi*, *6*(1), 90.