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

Rising Cybercrime during the COVID-19 Pandemic: Examining Legal Gaps in Indonesia's Regulatory Framework

Bahtiar Efendi[1*]

[1] Universitas Islam Sultan Agung, Semarang, Indonesia

Abstract

Article history:
Received: March 25, 2022
Revised: April 17, 2022
Accepted: May 29, 2022
Published: June 30, 2022

Keywords:
COVID-19 Pandemic, Cybercrime, Digital Regulation, Information Security, Personal Data Protection.

Identifier:
Zera Open
Page: 77-94
https://zeraopen.com/journal/jclis

This article examines the rise of cybercrime during the COVID-19 pandemic and evaluates whether Indonesia's regulatory framework was effective in responding to pandemic-era cyber threats. Using a normative juridical approach, the study analyzes Law Number 11 of 2008 concerning Electronic Information and Transactions as amended by Law Number 19 of 2016, Government Regulation Number 71 of 2019, relevant scholarly literature, and selected cybercrime cases involving online fraud and alleged data breaches. The findings show that Indonesia's framework provided an important legal basis for recognizing electronic evidence, criminalizing unlawful cyber conduct, and regulating electronic system providers. However, the analysis also reveals significant gaps, including fragmented personal data protection, reactive enforcement, limited breach notification mechanisms, unclear platform accountability, and insufficient victim recovery. The article discusses these gaps through statutory and conceptual analysis. It concludes that Indonesia's cybercrime regulation must shift toward a more integrated, preventive, and victim-oriented model to strengthen legal certainty, cybersecurity governance, and public trust in digital transformation.

*Corresponding author:
(Bahtiar Efendi)

1. Introduction

The COVID-19 pandemic intensified Indonesia's dependence on digital systems. Public health restrictions, remote work, online learning, digital payment, telecommunication platforms, and electronic commerce became central to social and economic activity. This rapid migration to cyberspace also expanded the vulnerability of individuals, businesses, and public institutions to cybercrime. Cyber offenders exploited uncertainty, fear, and increased online interaction through phishing, malware distribution, online fraud, unauthorized access, and misuse of personal information. Amarullah et al. (2021) show that cybercriminals in Indonesia used COVID-19-related situations and public anxiety as entry points for cyberattacks, including attacks directed at specific sectors. This condition indicates that the pandemic did not merely increase internet use but also created a criminogenic digital environment in which legal protection, cybersecurity readiness, and institutional accountability became increasingly urgent.

Cybercrime during the pandemic must be understood as both a technological and legal problem. From a technological perspective, attacks such as phishing, hacking, malware, and data leakage exploit weaknesses in systems and user behavior. From a legal perspective, these acts raise questions about whether Indonesia's regulatory framework is sufficiently effective to prevent, prosecute, and remedy digital harm. Kwarto and Angsito (2018) demonstrate that hacking, phishing, and malware are closely related to cybersecurity compliance in the financial sector, showing that cyber risk is not limited to isolated individual misconduct but also concerns institutional preparedness. In the pandemic context, this issue became

more serious because financial transactions, consumer activities, and administrative services increasingly relied on electronic platforms.

Indonesia's main legal basis for cybercrime enforcement is Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 19 of 2016. This law regulates unlawful access, manipulation of electronic information, electronic fraud, and several forms of prohibited digital conduct. It is also supported by Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, which imposes obligations on electronic system providers. However, the effectiveness of this framework remains debatable. Koto (2021) argues that although cybercrime is regulated under the ITE Law, the development of cybercrime methods creates continuing challenges for legal enforcement. Waluyo et al. (2021) also emphasize the urgency of amending the ITE Law because Indonesia's broader digital legal regime still faces problems of coherence, certainty, and proportionality.

The pandemic further exposed the relationship between cybercrime and personal data protection. Large-scale data leakage cases showed that cybercrime does not only involve direct financial loss but also the unlawful circulation of personal information that may later be used for identity abuse, fraud, or other digital crimes. Reuters reported that Tokopedia investigated an alleged data leak involving millions of user accounts, while another Reuters report described government concern after an alleged BPJS Kesehatan data leak. These incidents became important case illustrations because they involved widely used digital or public service platforms, suggesting that regulatory weakness can affect both private and state-managed data

systems. Situmeang (2021) argues that misuse of personal data is a serious form of cybercrime because personal information can become an instrument for further unlawful acts.

The legal gap becomes clearer when Indonesia's framework is examined through a normative approach. The ITE Law provides criminal provisions, yet it does not fully establish a comprehensive cybersecurity governance model. It focuses strongly on prohibited acts and criminal sanctions, while prevention, breach notification, institutional responsibility, victim recovery, and independent supervision remain fragmented across different rules. Aswandi et al. (2020) note that protection of personal data and information in Indonesia requires a stronger and more integrated regulatory system. This is particularly relevant to pandemic-era cybercrime because many incidents emerged from weak data governance, insufficient security standards, and limited accountability of electronic system providers.

Based on this background, the article examines two research questions. First, how effective is Indonesia's cybercrime regulatory framework in responding to the rise of cybercrime during the COVID-19 pandemic? Second, why is it urgent to review this framework in light of legal gaps revealed by pandemic-era cybercrime cases? These questions are important because cybercrime regulation cannot be assessed only from the existence of legal norms. It must also be evaluated based on whether those norms are clear, enforceable, preventive, and capable of protecting victims. This article argues that Indonesia's existing framework has provided an initial foundation for cybercrime enforcement, but its effectiveness remains limited

by fragmented regulation, reactive enforcement, and insufficient integration between cybercrime law, cybersecurity governance, and personal data protection.

2. Research Methods

This study uses a normative juridical approach to examine legal gaps in Indonesia's regulatory framework for addressing the rise of cybercrime during the COVID-19 pandemic. This approach is appropriate because the article does not aim to measure cybercrime statistically, but to analyze the effectiveness, coherence, and adequacy of existing legal norms. The study therefore treats statutory regulations as the primary object of analysis and connects them with scholarly literature and selected cybercrime cases to assess whether the current framework is sufficient to respond to pandemic-related cyber threats.

The primary legal materials consist of Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 19 of 2016, and Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. These instruments are selected because they provide the main legal basis for regulating electronic information, electronic transactions, prohibited cyber conduct, and the obligations of electronic system providers in Indonesia. The analysis also considers related legal principles on consumer protection and personal data protection where relevant, especially when cybercrime involves online fraud, unauthorized access, data leakage, and misuse of personal information.

Secondary materials are drawn from peer-reviewed scholarly sources indexed in Google Scholar and published between 2018 and 2021. These sources discuss cybercrime, cybersecurity governance, electronic transaction law, and personal data protection in Indonesia. Reputable news reports are used only as contextual case illustrations, not as the main basis for legal argumentation. In particular, reports concerning alleged data breaches involving Tokopedia and BPJS Kesehatan are used to illustrate how cybercrime and data exposure occurred in practice and why legal evaluation became increasingly urgent during the pandemic.

The study applies both a statutory approach and a conceptual approach. The statutory approach is used to examine the scope, structure, and limitations of the ITE Law and Government Regulation Number 71 of 2019. The conceptual approach is used to understand cybercrime as a legal issue connected to information security, platform accountability, victim protection, and personal data governance. The collected materials are analyzed qualitatively by comparing regulatory norms with cybercrime patterns identified in the literature and case reports. The analysis is directed toward answering two research questions: first, how effective Indonesia's cybercrime regulatory framework is in responding to the rise of cybercrime during the COVID-19 pandemic; and second, why reviewing this framework is urgent in light of the legal gaps revealed by pandemic-era cybercrime cases.

3. Results and Discussion

3.1. How effective is Indonesia's cybercrime regulatory framework in responding to the rise of cybercrime during the COVID-19 pandemic?

Indonesia's cybercrime regulatory framework provided an important legal foundation during the COVID-19 pandemic, but its effectiveness remained partial and uneven. The main strength of the framework lies in the existence of the ITE Law, which recognizes electronic information and electronic documents as legal objects and evidence, while also criminalizing several unlawful acts in cyberspace. Through Law Number 11 of 2008 as amended by Law Number 19 of 2016, Indonesian law already provides provisions on unauthorized access, interception, manipulation of electronic information, disruption of electronic systems, and unlawful transmission of electronic content. In principle, these provisions allowed law enforcement institutions to respond to common forms of cybercrime that increased during the pandemic, including phishing, account takeover, online fraud, and data misuse. Koto (2021) notes that the ITE Law has become the main statutory basis for addressing cybercrime in Indonesia, particularly because conventional criminal law was not originally designed to regulate digital conduct.

However, the effectiveness of a cybercrime framework cannot be measured only by the existence of criminal provisions. It must also be assessed based on whether the legal norms are sufficiently clear, adaptive, enforceable, preventive, and capable of protecting victims. During the pandemic, cybercrime patterns became more complex because offenders exploited public dependence on online platforms. Amarullah et al. (2021) show that cybercriminals used COVID-19-related themes,

public fear, and digital dependence to carry out cyberattacks in Indonesia. This indicates that cybercrime was not merely increasing in quantity but also changing in method. The law therefore needed to respond to social engineering, fraudulent digital communication, data theft, and platform-based vulnerabilities. In this context, Indonesia's framework was effective only to the extent that the act could be linked to existing ITE Law provisions, but less effective when the harm involved weak cybersecurity governance, delayed breach response, or unclear responsibility of electronic system providers.

Government Regulation Number 71 of 2019 attempted to strengthen the legal framework by regulating the implementation of electronic systems and transactions. It introduced obligations for electronic system providers, including reliability, security, and responsibility in managing electronic systems. This regulation is significant because cybercrime prevention requires duties not only from individual users but also from digital platforms, public agencies, and private companies that process electronic information. Nevertheless, the regulation remained more administrative than victim-centered. It did not fully provide a comprehensive system for compensation, breach notification, independent supervision, or clear accountability when personal data were exposed through weak electronic systems. This gap became visible in large-scale data breach cases, such as the alleged Tokopedia data leak reported by Potkin (2020) and the alleged BPJS Kesehatan leak reported by Reuters (2021). These cases showed that cybercrime enforcement must be connected with preventive data governance, not merely post-incident punishment.

The weakness of personal data protection further limited regulatory effectiveness. Before the enactment of a comprehensive personal data protection law, Indonesia's rules on personal data were scattered across sectoral regulations. Aswandi et al. (2020) argue that Indonesia required an integrated personal data protection system because fragmented regulation made protection less effective. Nugroho et al. (2020) similarly highlight that personal data protection in Indonesia was still incomplete, especially in areas involving financial technology and digital services. This fragmentation mattered during the pandemic because online transactions and platform-based services increased rapidly, while users often had limited control over how their data were collected, stored, transferred, or protected. When a cybercrime incident involved personal data leakage, victims faced difficulty identifying who was responsible, what remedy was available, and which institution had the authority to supervise the incident.

Another limitation concerns the reactive character of the framework. The ITE Law is primarily structured around prohibited acts and sanctions. This is necessary for criminal enforcement, but it is not sufficient for cybersecurity governance. Cybercrime prevention requires risk assessment, security standards, incident reporting, institutional coordination, digital forensic capacity, and public education. Kwarto and Angsito (2018) demonstrate that cybersecurity compliance is essential in sectors such as finance because cybercrime risks are closely connected to institutional security behavior. In other words, cybercrime regulation must not only punish offenders after an attack occurs but also require organizations to prevent foreseeable risks. During the pandemic, when many services shifted online quickly,

preventive obligations became more important because users and institutions were exposed to unfamiliar digital risks.

The ITE Law also faced challenges of legal certainty. Several provisions have been criticized for broad formulation and potential inconsistent interpretation. Although much of this criticism concerns expression-related offenses, the broader issue is relevant to cybercrime governance because unclear norms may weaken predictable enforcement. Waluyo et al. (2021) argue that amendments to the ITE Law are urgent because Indonesia's digital legal regime requires better coherence, certainty, and proportionality. In cybercrime cases, legal certainty is important for determining the boundaries between technical failure, negligence, administrative violation, and criminal responsibility. Without clear distinctions, enforcement may become inconsistent, while victims may still lack meaningful remedies.

Electronic evidence also plays an important role in cybercrime enforcement. Pribadi (2018) explains that electronic evidence has become legally important within the Indonesian criminal justice system, especially as crime increasingly involves digital traces. The recognition of electronic evidence under the ITE Law improves enforcement capacity, but practical problems remain. Cybercrime often involves anonymous actors, encrypted communication, cross-border servers, and rapidly deleted digital traces. Therefore, the legal recognition of electronic evidence must be supported by forensic capability, procedural safeguards, and interinstitutional cooperation. The pandemic increased the urgency of this issue because more criminal conduct occurred through digital communication and electronic platforms.

Overall, Indonesia's cybercrime framework was effective in providing a basic legal foundation, but it was less effective as a comprehensive response to pandemic-era cybercrime. It enabled the criminalization of several cyber offenses and recognized electronic evidence, yet it remained limited by fragmented data protection, reactive enforcement, insufficient preventive obligations, and unclear victim recovery mechanisms. The framework responded better to individual cyber offenses than to systemic cyber risks involving platform accountability and data governance.

3.2. Why is it urgent to review Indonesia's cybercrime regulatory framework in light of legal gaps revealed by pandemic-era cybercrime cases?

Reviewing Indonesia's cybercrime regulatory framework is urgent because the COVID-19 pandemic revealed that digital vulnerability is no longer a marginal legal issue. Cybercrime became closely connected to daily life, public service delivery, economic survival, and institutional trust. When education, employment, commerce, banking, and public administration moved online, cybercrime affected not only individual victims but also the reliability of digital governance. The pandemic therefore changed the legal significance of cybercrime. It was no longer sufficient to treat cybercrime as a specialized offense committed by technically skilled perpetrators. Instead, cybercrime became a mainstream threat to consumer protection, privacy, public administration, and national digital resilience.

The first reason for urgency is the widening gap between cybercrime methods and existing legal norms. Cybercriminals increasingly used social engineering, fake websites, phishing messages, malware, fraudulent online shops, and data

exploitation. Fadhila (2021) shows that e-commerce fraud became a relevant criminal phenomenon during the pandemic, especially as consumers relied more heavily on digital transactions. These crimes often combine deception, identity misuse, electronic communication, and financial loss. Although the ITE Law can be used to address certain aspects of such conduct, complex cases may involve overlapping issues of fraud, consumer protection, electronic evidence, platform responsibility, and personal data misuse. This overlap shows that cybercrime regulation needs stronger coordination across legal fields.

The second reason is the weak integration between cybercrime law and personal data protection. Situmeang (2021) argues that misuse of personal data can be understood as a serious cybercrime because personal information may be used repeatedly for further unlawful acts. Data leakage is therefore not a single completed incident. Once personal data enter illegal circulation, they may support identity theft, financial fraud, account takeover, doxing, blackmail, or targeted scams. Puluhulawa et al. (2020) also emphasize that personal data protection remained legally weak in the industrial revolution 4.0 era, particularly because technological development moved faster than regulatory protection. This weakness became more urgent during the pandemic because public dependence on digital platforms increased the amount of personal data processed by private and public institutions.

The third reason is the need to clarify the responsibility of electronic system providers. Pandemic-era cases such as alleged large-scale data leaks showed that cybercrime cannot be addressed only by pursuing the direct perpetrator. The law must also ask whether the platform or institution had adequate security systems,

whether it responded promptly, whether users were notified, and whether victims received effective remedies. Government Regulation Number 71 of 2019 already recognizes certain responsibilities of electronic system providers, but the framework still needed more detailed standards on breach notification, accountability, sanctions, and victim-oriented recovery. Without clear obligations, institutions may treat cybersecurity as an internal technical matter rather than a legal duty owed to users.

The fourth reason is the importance of public trust in digital transformation. Indonesia's digital economy depends on user confidence in online platforms, payment systems, e-commerce, and public digital services. If cybercrime continues to increase while legal remedies remain unclear, users may lose trust in electronic transactions. This is especially significant because the pandemic accelerated digital adoption among users who may not have strong cybersecurity literacy. Habibi and Liviani (2020) argue that cybercrime prevention in Indonesia requires a legal system that can respond to technological development and provide adequate protection. Legal reform is therefore not only a matter of criminal law but also a condition for sustainable digital transformation.

The fifth reason is the cross-border nature of cybercrime. Many cybercrimes involve servers, perpetrators, victims, or financial flows located in different jurisdictions. This creates challenges for investigation, evidence collection, asset recovery, and enforcement. Domestic legislation must therefore be supported by clear procedures for cooperation, digital forensic standards, and institutional coordination. The ITE Law provides a national legal basis, but its effectiveness depends on enforcement capacity and compatibility with international cybercrime

cooperation. During the pandemic, when cyberattacks increased globally, Indonesia's regulatory framework needed to be evaluated against transnational cybercrime realities.

The sixth reason is victim protection. Existing cybercrime enforcement tends to focus on identifying and punishing perpetrators. While this remains important, victims of cybercrime often need rapid response, account recovery, financial remedy, identity protection, and assurance that their data will not be further misused. In data breach cases, victims may suffer long-term risks even when no immediate financial loss is visible. A victim-centered approach would require clearer notification duties, complaint mechanisms, and remedies. Without these mechanisms, legal enforcement may produce punishment without fully restoring the harm experienced by victims.

For these reasons, reviewing Indonesia's regulatory framework is urgent. The pandemic revealed that cybercrime regulation must move beyond a sanction-oriented model toward an integrated model combining criminal enforcement, cybersecurity governance, personal data protection, platform accountability, and victim recovery. The ITE Law and Government Regulation Number 71 of 2019 remain important foundations, but they need to be supported by clearer, more coherent, and more preventive legal instruments. A normative review is therefore necessary to identify whether existing laws are capable of addressing cybercrime as it actually occurs in contemporary digital society.

4. Conclusion

This article shows that the rise of cybercrime during the COVID-19 pandemic exposed important weaknesses in Indonesia's regulatory framework for cyber law and information security. The rapid shift toward online transactions, remote communication, digital public services, and platform-based economic activity created wider opportunities for phishing, online fraud, unauthorized access, data leakage, and misuse of personal information. Indonesia already had a legal foundation through Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 19 of 2016, and Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. These instruments are important because they recognize electronic information, electronic documents, and electronic evidence, while also regulating prohibited conduct and certain obligations of electronic system providers.

However, the analysis indicates that the effectiveness of the existing framework remains limited. The ITE Law is useful as a criminal law instrument, but it is still largely reactive because it focuses on prohibited acts and sanctions after cyber harm has occurred. It does not yet provide a fully integrated model of cybersecurity governance, especially in relation to prevention, risk-based security duties, breach notification, platform accountability, victim recovery, and coordination among relevant institutions. Government Regulation Number 71 of 2019 strengthens the administrative responsibilities of electronic system providers, yet it does not completely solve the problem of fragmented regulation. As a result, pandemic-era cybercrime cases involving online fraud and alleged large-scale data

breaches revealed that legal enforcement alone is insufficient when not supported by strong data protection and institutional accountability mechanisms.

The urgency of reviewing Indonesia's cybercrime framework therefore lies in the changing nature of digital harm. Cybercrime during the pandemic was not limited to individual criminal acts but also reflected structural weaknesses in digital governance. Data leakage, phishing, and e-commerce fraud show that cybercrime often involves overlapping issues of consumer protection, personal data protection, cybersecurity compliance, electronic evidence, and platform responsibility. For this reason, Indonesia's regulatory framework needs to move from a sanction-oriented model toward a more preventive and integrated model. Such a model should combine clear criminal provisions with stronger duties for electronic system providers, effective data protection rules, timely breach response, accessible remedies for victims, and stronger institutional coordination.

In conclusion, Indonesia's existing regulations have provided a necessary starting point for addressing cybercrime, but they are not yet sufficient to respond to the complexity of pandemic-era cyber threats. A normative review is important because it helps identify whether the current legal framework is coherent, enforceable, and responsive to contemporary digital risks. Strengthening cybercrime regulation is therefore essential not only for law enforcement, but also for protecting personal data, maintaining public trust in digital services, and supporting a safer digital transformation in Indonesia.

References

Amarullah, A. H., Runturambi, A. J. S., & Widiawan, B. (2021). Analyzing cyber crimes during COVID-19 time in Indonesia. In *2021 3rd International Conference on Computer Communication and the Internet (ICCCI)* (pp. 78–83). IEEE.

Aswandi, R., Muchsin, P. R. N., & Sultan, M. (2020). Perlindungan data dan informasi pribadi melalui Indonesian Data Protection System (IDPS). *Legislatif, 3*(2), 167–190.

Fadhila, A. P. (2021). Tinjauan kriminologi dalam tindakan penipuan e-commerce berdasar peraturan perundang-undangan pada masa pandemi COVID-19 di Indonesia. *Jurnal Suara Hukum, 3*(2), 274–299.

Habibi, M. R., & Liviani, I. (2020). Kejahatan teknologi informasi (cyber crime) dan penanggulangannya dalam sistem hukum Indonesia. *Al-Qanun: Jurnal Pemikiran dan Pembaharuan Hukum Islam, 23*(2), 400–426.

Koto, I. (2021). Cyber crime according to the ITE Law. *International Journal Reglement & Society, 2*(2), 103–110.

Kwarto, F., & Angsito, M. (2018). Pengaruh cyber crime terhadap cyber security compliance di sektor keuangan. *Jurnal Akuntansi Bisnis, 11*(2), 99–110.

Nugroho, A. A., Winanti, A., & Surahmad. (2020). Personal data protection in Indonesia: Legal perspective. *International Journal of Multicultural and Multireligious Understanding, 7*(7), 183–189.

Potkin, F. (2020, May 2). Indonesia's Tokopedia probes alleged data leak of 91 million users. *Reuters*. Retrieved Feb 17, 2022 from

https://www.reuters.com/article/technology/indonesias-tokopedia-probes-alleged-data-leak-of-91-million-users-idUSKBN22E0P9/

Reuters. (2021, May 21). Indonesia summons state health insurer over alleged data leak. *Reuters*. Retrieved Feb 18, 2021 from https://www.reuters.com/technology/indonesia-summons-state-health-insurer-over-alleged-data-leak-2021-05-21/

Situmeang, S. M. T. (2021). Penyalahgunaan data pribadi sebagai bentuk kejahatan sempurna dalam perspektif hukum siber. *SASI, 27*(1), 38–52.

Waluyo, T. T. P., Calista, E., Ratu, D. P., Ramli, T. S., & Ramli, A. M. (2021). The Indonesian Electronic Information and Transactions within Indonesia's broader legal regime: Urgency for amendment? *Jurnal HAM, 12*(3), 533–552.