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

Legal Gaps in Indonesia's Personal Data Protection Framework: Lessons from Data Breach Cases (2017-2021)

Irham Alfarid Hidayat[1*]

[1] Universitas Pembangunan Nasional Veteran Yogyakarta, Yogyakarta, Indonesia

Abstract

Article history:
Received: January 21, 2022
Revised: February 26, 2022
Accepted: April 13, 2022
Published: June 30, 2022

Keywords:
Accountability, Data Breach, Information Security, Personal Data Protection, Privacy Rights.

Identifier:
Zera Open
Page: 20-37
https://zeraopen.com/journal/jclis

This article examines legal gaps in Indonesia's personal data protection framework during the 2017-2021 period, focusing on the effectiveness and urgency of existing regulations in responding to data breach cases. Using a normative legal approach, the study analyzes the Electronic Information and Transactions Law, Government Regulation No. 71 of 2019, and Ministerial Regulation No. 20 of 2016 in relation to major breach incidents involving Tokopedia and BPJS Kesehatan. The analysis shows that Indonesia's pre-2022 framework had recognized consent, confidentiality, system reliability, and breach notification, but remained fragmented, sectoral, and weak in enforcement. The article discusses regulatory effectiveness through legal certainty, liability, supervision, sanctions, and data subject remedies, while also examining the urgency of reform in the context of privacy rights, digital transformation, and information security governance. The main finding is that Indonesia required a comprehensive personal data protection regime to ensure stronger accountability, clearer rights, effective remedies, and greater public trust in digital systems.

*Corresponding author:
(Irham Alfarid Hidayat)

1. Introduction

Indonesia's rapid digital transformation has intensified the legal relevance of personal data protection. The expansion of e-commerce, digital finance, online public services, telecommunication platforms, and health information systems has increased the volume of personal data processed by both private electronic system providers and public institutions. In this context, personal data has become an important legal object because it is directly connected to privacy, identity, autonomy, and public trust in digital services. However, before the enactment of a comprehensive personal data protection law, Indonesia's framework remained fragmented across the Electronic Information and Transactions Law, Government Regulation No. 71 of 2019, and Minister of Communication and Informatics Regulation No. 20 of 2016. These instruments recognized consent, confidentiality, system reliability, and written notification in cases of data protection failure, but they did not yet form a unified statutory regime with clear institutional enforcement, strong administrative sanctions, and comprehensive rights of data subjects (Nugroho et al., 2020; Sinaga & Putri, 2020). This condition created a legal gap between the growth of digital data processing and the capacity of existing law to prevent, respond to, and remedy personal data breaches.

The urgency of this issue became visible through major data breach incidents involving large-scale digital platforms and public institutions. In May 2020, Tokopedia investigated claims that data from millions of users had been leaked and offered online, raising public concern over the security responsibilities of large digital platforms (Potkin, 2020). In 2021, Indonesia's Ministry of Communication and

Informatics summoned BPJS Kesehatan after allegations that personal data managed by the state health insurer had been leaked and sold online (Reuters, 2021). These cases were not merely technical cybersecurity incidents, but legal events that exposed uncertainty regarding breach notification, liability, compensation, and the role of regulators in supervising data controllers. They also demonstrated that personal data breaches can affect not only consumer confidence, but also citizens' trust in public administration, especially when sensitive demographic, health, or identification data are involved. Personal data protection is closely related to the constitutional right to privacy, because misuse or leakage of personal information can affect individual autonomy, dignity, and legal security in digital interactions (Kusnadi, 2021). Scholars have therefore argued that Indonesia's sectoral approach was insufficient because personal data protection requires not only consent-based rules, but also enforceable principles of accountability, purpose limitation, security safeguards, and effective remedies (Sitompul, 2019; Mangku et al., 2021).

From a normative legal perspective, the central problem lies in whether the applicable regulations during the 2017-2021 period were adequate to protect data subjects in real breach situations. Ministerial Regulation No. 20 of 2016 required electronic system providers to protect personal data throughout collection, processing, storage, transfer, disclosure, and deletion, while also requiring written notification to data owners in the event of failure. Government Regulation No. 71 of 2019 further regulated electronic system operators and introduced obligations related to reliability, security, and data processing. Nevertheless, these rules still left questions concerning the time limit for notification, the independence of supervisory

authority, the calculation of sanctions, the burden of proof, and the enforceability of individual rights. The absence of a stronger and more centralized supervisory mechanism also made it difficult to ensure consistent compliance across sectors. This normative weakness is important because legal protection becomes ineffective when obligations exist formally but enforcement mechanisms remain limited (Rosmaini et al., 2018; Sinaga & Putri, 2020).

Therefore, this article examines legal gaps in Indonesia's personal data protection framework by learning from data breach cases occurring before the comprehensive Personal Data Protection Law was enacted. The study is guided by two research questions: first, how effective were Indonesia's applicable personal data protection regulations in responding to data breach cases during the 2017-2021 period? Second, why is it urgent to examine these legal gaps in the context of Indonesia's digital transformation and information security governance? By addressing these questions, the article contributes to cyber law scholarship by linking doctrinal analysis of regulations with concrete breach phenomena. It argues that the protection of personal data is not only a matter of technological security, but also of legal certainty, institutional accountability, regulatory effectiveness, and enforceable rights in an increasingly data-driven society.

2. Research Methods

This study uses a normative legal research method to examine legal gaps in Indonesia's personal data protection framework before the enactment of the comprehensive Personal Data Protection Law. The normative approach is

appropriate because the article focuses on written legal norms, regulatory consistency, and the effectiveness of legal provisions in responding to data breach cases. The analysis is directed toward assessing whether the existing legal instruments during the 2017-2021 period provided adequate protection for data subjects and sufficient obligations for electronic system providers.

The research applies a statutory approach and a case approach. The statutory approach is used to examine relevant Indonesian regulations, particularly Law No. 11 of 2008 as amended by Law No. 19 of 2016 concerning Electronic Information and Transactions, Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, and Minister of Communication and Informatics Regulation No. 20 of 2016 concerning Personal Data Protection in Electronic Systems. These regulations are analyzed to identify provisions related to consent, confidentiality, data processing obligations, breach notification, administrative sanctions, and the responsibilities of electronic system providers. The case approach is applied by considering major Indonesian data breach incidents reported between 2017 and 2021, especially cases involving Tokopedia and BPJS Kesehatan, as examples of how regulatory gaps appeared in practice.

The data used in this study consist of primary and secondary legal materials. Primary legal materials include Indonesian laws and regulations governing electronic systems, information security, and personal data protection. Secondary legal materials include peer-reviewed journal articles, legal commentaries, and reputable news reports published between 2017 and 2021. Scholarly references were selected

from Google Scholar-indexed publications to ensure academic relevance, while news sources were used only to provide factual context regarding data breach incidents. The inclusion criteria focused on sources discussing Indonesian personal data protection, privacy rights, electronic system regulation, cybersecurity governance, and data breach accountability.

The collected materials are analyzed qualitatively through descriptive and analytical legal reasoning. First, the study describes the regulatory framework applicable during the selected period. Second, it evaluates the effectiveness of these rules by comparing legal obligations with the practical problems revealed in data breach cases. Third, it identifies legal gaps concerning enforcement, supervision, breach notification, liability, and remedies. Through this method, the article aims to provide a systematic legal assessment of why Indonesia's pre-2022 personal data protection framework required stronger and more comprehensive regulation.

3. Results and Discussion

3.1. How effective were Indonesia's applicable personal data protection regulations in responding to data breach cases during the 2017-2021 period?

Indonesia's personal data protection framework during the 2017-2021 period can be considered only partially effective. Normatively, the state had already recognized personal data protection through several legal instruments, particularly Law No. 11 of 2008 as amended by Law No. 19 of 2016 concerning Electronic Information and Transactions, Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, and Minister of

Communication and Informatics Regulation No. 20 of 2016 concerning Personal Data Protection in Electronic Systems. These regulations established basic obligations for electronic system providers, including the duty to maintain system reliability, protect confidential information, process data based on consent, and notify data owners when personal data protection fails. Therefore, Indonesia did not experience a complete legal vacuum. However, the problem was that these rules were dispersed, sectoral, and limited in enforcement capacity, which weakened their practical effectiveness in responding to large-scale data breach incidents (Nugroho et al., 2020; Sinaga & Putri, 2020).

The first weakness concerns the fragmented nature of the regulatory framework. Personal data protection was regulated through electronic transaction law, government regulation, ministerial regulation, consumer protection norms, and sectoral rules. This fragmentation made the legal framework difficult to apply consistently because there was no single comprehensive statute that clearly defined data controller obligations, data subject rights, independent supervision, and proportional sanctions. Rosadi (2018) explains that Indonesia's legal framework for privacy and personal data protection in the digital economy still faced significant challenges because personal data was increasingly treated as an economic asset, while legal protection remained incomplete. Yuniarti (2019) also emphasizes that Indonesia required clearer legal protection for personal data because existing rules were scattered and did not yet provide comprehensive certainty for data owners. From a normative standpoint, legal certainty is essential because individuals must be able to understand their rights, while electronic system providers must be able to

identify their responsibilities. When the rules are scattered across several instruments, legal protection becomes dependent on interpretation rather than on a clear statutory design.

The second weakness concerns breach notification. Minister of Communication and Informatics Regulation No. 20 of 2016 required written notification to data owners when a failure of personal data protection occurred. Nevertheless, the regulation did not establish a sufficiently detailed notification model, especially regarding strict notification deadlines, minimum content of notification, public disclosure obligations, coordination with supervisory bodies, and consequences for delayed or incomplete reporting. This weakness became visible in data breach cases involving Tokopedia and BPJS Kesehatan. The Tokopedia case in 2020 raised public concern because user data allegedly circulated in online forums, while the BPJS Kesehatan case in 2021 involved allegations of leakage of sensitive public health-related data (Potkin, 2020; Reuters, 2021). In both cases, the legal issue was not limited to whether leakage occurred, but also whether affected data subjects received timely, clear, and enforceable information regarding the nature of the breach, potential harm, and available remedies.

The third weakness concerns liability and remedies. Existing regulations imposed obligations on electronic system providers, but they did not fully clarify the legal consequences when data subjects suffered harm due to leakage, identity theft, fraud, or unauthorized use of personal data. This created uncertainty regarding compensation, burden of proof, and the procedural route for affected individuals. Nurdiani (2020) explains that digital identity theft can function as a form of cyber-

related crime because personal information can be used for fraud, impersonation, account takeover, and other illegal activities. This shows that data breaches are not abstract administrative failures; they can become the starting point for wider criminal and economic harm. However, during the 2017-2021 period, Indonesian regulations did not yet provide a strong remedial structure that allowed data subjects to easily claim protection or compensation after their data had been compromised.

The fourth weakness relates to institutional supervision. Effective personal data protection requires a supervisory authority capable of monitoring compliance, investigating breaches, imposing sanctions, and guiding public and private actors. During the period examined, Indonesia did not yet have an independent personal data protection authority with comprehensive supervisory power. Regulatory responsibility was mainly associated with the Ministry of Communication and Informatics, but this arrangement created limitations because the same institution had broader policy and administrative functions in the digital sector. Nugroho et al. (2020) argue that the absence of a comprehensive personal data protection law created uncertainty in the protection of data subjects and in the obligations of electronic system providers. Without a specialized and independent supervisory framework, enforcement tends to become reactive rather than preventive. As a result, regulation may exist formally, but its capacity to influence behavior before violations occur remains limited.

The fifth weakness concerns sanctions. Government Regulation No. 71 of 2019 and Ministerial Regulation No. 20 of 2016 allowed administrative responses, but the deterrent effect of these sanctions was limited when compared with the scale

of digital platforms and the economic value of personal data. Large digital platforms process millions of user accounts, meaning that a single breach may affect a vast number of individuals. In this context, weak sanctions may be treated merely as compliance costs rather than as serious legal consequences. Rosadi (2018) shows that privacy protection in the digital economy requires a strong legal framework because personal data has significant commercial value. Therefore, sanctions must be strong enough to ensure that companies internalize the cost of security, accountability, and risk management. If sanctions are vague or weak, electronic system providers may not have sufficient legal incentive to invest in stronger data governance.

Based on these points, the applicable regulations during 2017-2021 were effective only at the level of basic recognition. They acknowledged that personal data deserved legal protection and that electronic system providers had duties to safeguard data. However, they were less effective in providing a complete response to breach cases. The legal framework did not yet adequately regulate clear notification procedures, independent supervision, enforceable remedies, strong sanctions, and standardized accountability obligations. Thus, the effectiveness of the pre-2022 framework was limited because it was more declarative than operational. It provided legal language for protection, but it did not yet provide a comprehensive institutional and procedural mechanism capable of addressing the real consequences of data breach incidents.

3.2. Why is it urgent to examine these legal gaps in the context of Indonesia's digital transformation and information security governance?

The urgency of examining Indonesia's personal data protection gaps lies in the rapid expansion of digital activities and the increasing dependence of citizens on electronic systems. Personal data is now processed in almost every aspect of daily life, including online shopping, digital payment, banking, telecommunication, education, public administration, and health services. This means that data breaches can no longer be understood as isolated technological failures. They represent legal, social, economic, and governance risks. In the Indonesian context, the Tokopedia and BPJS Kesehatan cases demonstrated that both private platforms and public institutions may become sources of vulnerability. When personal data is leaked from a large e-commerce platform, users may face risks of phishing, fraud, and account misuse. When data is leaked from a public health institution, the risks become even more serious because health-related data may expose sensitive personal conditions, family information, and identity records.

The urgency is also connected to the nature of personal data as part of the right to privacy. Kusnadi (2021) explains that personal data protection is closely related to legal protection of privacy rights. This means that leakage of personal data is not merely a loss of information, but also a violation of individual dignity, autonomy, and control over personal identity. In a digital society, privacy must be protected not only from direct surveillance, but also from irresponsible collection, processing, sharing, and commercialization of personal data. Sitompul (2019) similarly notes that the absence of a coherent personal data protection framework

creates legal difficulties in protecting individuals in digital contexts. Therefore, the urgency of regulation is not only technical, but constitutional and human-rights based.

Another reason why these legal gaps are urgent to examine is the growth of the digital economy. Indonesia's digital economy depends heavily on public trust. Users are more likely to participate in online transactions when they believe that their personal data is protected, that platforms are accountable, and that the state can provide remedies when harm occurs. If breaches repeatedly occur without clear legal consequences, trust in digital services may decline. Rosadi (2018) emphasizes that privacy and personal data protection are essential in the digital economic era because data has become a central element of business models and consumer interactions. In this sense, weak personal data protection can produce broader economic consequences, including reduced consumer confidence and uncertainty for businesses that need clear compliance standards.

The urgency also arises from the imbalance of power between data subjects and electronic system providers. In most digital services, users do not negotiate privacy terms equally. They usually accept standard-form consent mechanisms without fully understanding how their data will be collected, processed, stored, or shared. This makes consent alone insufficient as the main basis of protection. Mangku et al. (2021) argue that internet users require stronger personal data protection because digital interaction exposes them to risks that are difficult to control individually. Normatively, this means the law must not only recognize consent, but also impose accountability, transparency, security, and fairness

obligations on data controllers. Without these principles, consent can become a formal requirement that legitimizes unequal data practices rather than genuinely protecting users.

The examination of legal gaps is also urgent because data breach cases reveal the limitations of reactive governance. A reactive model responds only after leakage occurs, usually through clarification, investigation, or administrative warning. However, personal data protection should operate preventively. Regulations should require risk assessment, data minimization, encryption, internal governance, regular audits, incident response planning, and clear accountability structures. Rosmaini et al. (2018), in the context of educational data, show that personal data protection is relevant across sectors that manage sensitive information. This supports the view that data governance cannot depend solely on general electronic system obligations. Different sectors may process different categories of data, but all require minimum standards of protection and accountability.

The urgency is further strengthened by the cross-border nature of digital data processing. Many platforms operate through cloud services, third-party processors, and international data flows. If domestic law is unclear, it becomes difficult to determine responsibility when personal data is processed outside Indonesia or by multiple actors. This issue is particularly important in cyber law because personal data breaches often involve actors, servers, or data markets located beyond national jurisdiction. A fragmented regulatory framework makes enforcement more difficult because Indonesian authorities may lack clear mechanisms to trace responsibility, require cooperation, or impose sanctions on foreign-linked entities. This shows why

a stronger legal framework is necessary not only for domestic compliance, but also for international digital governance.

Finally, examining these gaps is urgent because it provides lessons for the development of future regulation. The existence of data breach cases before 2022 showed that Indonesia needed a more comprehensive personal data protection regime. The analysis of the 2017-2021 framework demonstrates that legal reform was necessary because the earlier framework lacked several essential components: an integrated definition of personal data, clear rights of data subjects, independent supervision, detailed breach notification, stronger sanctions, and effective remedies. Yuniarti (2019) argues that legal protection of personal data in Indonesia needed to be strengthened because technological development had created new risks that were not fully addressed by existing legal instruments. Therefore, studying the gaps in the pre-2022 framework is important because it allows policymakers, scholars, and practitioners to understand why personal data protection must be designed as a comprehensive legal system rather than as a collection of scattered sectoral rules.

In conclusion, the urgency of examining Indonesia's personal data protection gaps is rooted in the intersection between digital transformation, privacy rights, cybersecurity risks, and public trust. The 2017-2021 framework had already introduced important principles, but it was not yet sufficient to address the scale and complexity of modern data breaches. Data breach cases involving Tokopedia and BPJS Kesehatan revealed that Indonesia needed stronger legal certainty, clearer institutional accountability, and more enforceable rights for data subjects. For this reason, the issue is central to cyber law and information security because effective

personal data protection requires not only secure technology, but also a coherent legal framework capable of preventing harm, assigning responsibility, and protecting individuals in the digital environment.

4. Conclusion

This article concludes that Indonesia's personal data protection framework during the 2017–2021 period was only partially effective in responding to data breach cases. The existing regulations, particularly the Electronic Information and Transactions Law, Government Regulation No. 71 of 2019, and Minister of Communication and Informatics Regulation No. 20 of 2016, had already recognized several important principles, such as consent, confidentiality, system reliability, and written notification in the event of data protection failure. However, these provisions were still fragmented and sectoral, so they did not yet provide a comprehensive legal structure for protecting data subjects. The absence of a single integrated law created uncertainty regarding the scope of personal data protection, the obligations of electronic system providers, the rights of data owners, and the mechanisms available when breaches occurred.

The analysis also shows that data breach cases involving Tokopedia and BPJS Kesehatan revealed important weaknesses in Indonesia's pre-2022 framework. These cases demonstrated that the problem was not merely technical, but also legal and institutional. The applicable regulations did not provide sufficiently detailed rules on breach notification, liability, compensation, burden of proof, supervisory authority, and proportional sanctions. As a result, affected individuals had limited

certainty regarding what remedies they could pursue and how electronic system providers should be held accountable. In this sense, Indonesia's earlier personal data protection framework was more declarative than operational: it acknowledged the importance of data protection, but did not yet establish strong enforcement instruments to ensure effective protection in practice.

The urgency of examining these legal gaps is closely related to Indonesia's broader digital transformation. As personal data becomes increasingly central to e-commerce, financial technology, public administration, health services, and other digital activities, weak protection can threaten individual privacy, public trust, and information security governance. Personal data breaches may lead to identity theft, fraud, discrimination, reputational harm, and loss of confidence in digital platforms. Therefore, personal data protection should not be viewed only as a technical cybersecurity issue, but also as a matter of legal certainty, constitutional privacy rights, institutional accountability, and consumer protection.

Overall, the findings indicate that Indonesia needed a stronger and more comprehensive personal data protection regime to respond to the risks of a data-driven society. Lessons from the 2017–2021 breach cases show that future regulation must contain clearer rights for data subjects, stronger obligations for data controllers, independent supervision, detailed breach notification standards, effective sanctions, and accessible remedies. A coherent legal framework is essential not only to prevent and respond to data breaches, but also to strengthen trust in Indonesia's digital ecosystem and support the development of cyber law and information security governance.

References

Kusnadi, S. A. (2021). Perlindungan hukum data pribadi sebagai hak privasi. *AL WASATH Jurnal Ilmu Hukum, 2*(1), 9-16.

Mangku, D. G. S., Yuliartini, N. P. R., Suastika, I. N., & Sudiatmaka, K. (2021). The personal data protection of internet users in Indonesia. *Journal of Southwest Jiaotong University, 56*(1), 202-209.

Nugroho, A.A., Winanti, A., & Surahmad, S. (2020). Personal Data Protection in Indonesia: Legal Perspective. *International Journal of Multicultural and Multireligious Understanding, 7*(7), 183-189.

Nurdiani, I. P. (2020). Pencurian identitas digital sebagai bentuk cyber related crime. *Jurnal Kriminologi Indonesia, 16*(2), 1-10.

Potkin, F. (2020, May 2). Indonesia's Tokopedia probes alleged data leak of 91 million users. *Reuters.* Retrieved Feb 2, 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 2, 2022 from https://www.reuters.com/technology/indonesia-summons-state-health-insurer-over-alleged-data-leak-2021-05-21/

Rosadi, S. D. (2018). Protecting privacy on personal data in digital economic era: Legal framework in Indonesia. *Brawijaya Law Journal, 5*(1), 143-157.

Rosmaini, E., Kusumasari, T. F., Lubis, M., & Lubis, A. R. (2018). Study to the current protection of personal data in the educational sector in Indonesia. *Journal of Physics: Conference Series, 978*(1), 1-7.

Sinaga, E. M. C., & Putri, M. C. (2020). Formulasi Legislasi Perlindungan Data Pribadi dalam Revolusi Industri 4.0. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional, 9*(2), 237.

Sitompul, J. (2019). Developing a legal framework of personal data protection in the Indonesian criminal procedure law. *Indonesia Law Review, 9*(3), 351-377.

Yuniarti, S. (2019). Perlindungan hukum data pribadi di Indonesia. *Business Economic, Communication, and Social Sciences Journal, 1*(1), 147-154.