Journal of Cyber Law and Information Security
Volume 2, Number 1, 2023

An Analysis of the Effectiveness of Electronic System Administration Regulations in Establishing PT Tokopedia's Liability in Cases of User Personal Data Breaches

Tofik Yanuar Chandra[1*]

[1] Universitas Jayabaya, Jakarta, Indonesia

Abstract

Article history:
Received: January 5, 2023
Revised: February 12, 2023
Accepted: April 20, 2023
Published: June 30, 2023

Keywords:
Cyber Law, Data Breach Regulation, Electronic System Operator Liability, Personal Data Protection, Tokopedia.

Identifier:
Zera Open
Page: 62-78
https://zeraopen.com/journal/jclis

Indonesia's digital economic transformation has accelerated the collection of personal data by e-commerce platforms, yet it has also been accompanied by significant information security risks. This study examines the legal liability of Private-Sector Electronic System Operators (*Penyelenggara Sistem Elektronik* or *PSE*) through a case study of the 2020 data breach involving 91 million Tokopedia users. Employing a normative legal research method with statutory and case-based approaches, this article evaluates the effectiveness of Indonesia's positive legal instruments, including the *UU ITE*, *PP PSTE*, and *PP PMSE*. The findings reveal that Article 15 of the *UU ITE*, which adopts the principle of presumption of liability, has not been effectively implemented due to ambiguous security standards and weak administrative sanctions under the *PP PSTE*. A deeper analysis further identifies a legal loophole in exoneration clauses contained in platform privacy policies, which unilaterally shift risk to consumers. A comprehensive review of sectoral regulations is therefore urgently needed to ensure legal certainty and to safeguard the constitutional right to personal protection as guaranteed under Article 28G of the 1945 Constitution (*UUD 1945*). This study recommends strengthening technical oversight

*Corresponding author:
(Tofik Yanuar Chandra)

by regulatory authorities and standardizing security system audits for all *PSE* operating in Indonesia.

1. Introduction

Indonesia's digital economic transformation has brought about a fundamental change in the way people conduct transactions through electronic commerce systems. The marketplace sector now dominates the national market, in line with the significant increase in internet users over the past decade. The internet is no longer used solely as a means of communication, but has also become a major source of income through creative digital economy innovations (Muhammad et al., 2021). This rapid development has led to the large-scale collection of personal data by various technology platforms for business and marketing purposes. However, this phenomenon of massive data control has created significant challenges for the protection of privacy rights and the information security of data subjects in Indonesia.

The most prominent legal phenomenon is the hacking incident involving 91 million Tokopedia user accounts, which came to light in early May 2020 (Sylfia et al., 2021). The breach, allegedly carried out by a hacker operating under the account name "whysodank," had actually occurred as early as March 2020 and was later publicized on the hacker forum Raid Forums. The entire database was reportedly

offered for sale on the dark web marketplace Empire Market for approximately US$5,000, or around IDR 74 million. The leaked information included sensitive data such as full names, email addresses, dates of birth, phone numbers, and even encrypted passwords. This incident serves as concrete evidence that even major e-commerce platforms possess system vulnerabilities that can seriously jeopardize consumer data confidentiality.

The incident highlights a significant gap between the security assurances promised in privacy policies and the actual vulnerabilities of corporate cybersecurity systems. Tokopedia explicitly stated its commitment to protecting user data; however, this massive breach exposed weaknesses in the implementation of the prudential principle in its system operations. As a result, millions of users suffered immaterial losses in the form of anxiety, concern, and a diminished sense of security in the digital space. The leaked data also carries substantial potential for misuse in subsequent cybercrimes, such as phishing and social engineering attacks. The absence of a clear compensation mechanism for victims further worsens the bargaining position of consumers, who already occupy a relatively weak legal standing.

To date, Indonesia's personal data protection legal framework remains sectoral and has not yet been comprehensively integrated. Existing regulations are scattered across various legal instruments, including the Electronic Information and Transactions Law (ITE Law), Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions (GR 71/2019), and Government Regulation No. 80 of 2019 on Trading Through Electronic Systems

(GR 80/2019). The ITE Law establishes the fundamental principle that electronic systems must be reliable, while GR 71/2019 requires written notification to data owners in the event of a protection failure. GR 80/2019 further emphasizes the obligation of business actors to implement adequate security systems to prevent any unlawful processing of personal data. Nevertheless, the absence of a dedicated law has resulted in a regulatory framework that is often considered underdeveloped and insufficiently effective for rigorous enforcement.

Based on this case, this article aims to analyze the effectiveness of the regulatory framework through two primary research questions. First, it examines the effectiveness of existing positive legal instruments, particularly Article 15 of the ITE Law and GR 71/2019, in ensuring the legal accountability of PT Tokopedia for its system failure, with a specific focus on the application of the principle of presumption of liability to *PSE* that process the personal data of the public. Second, it analyzes the urgency of reviewing cybersecurity standards within the regulatory framework to close gaps in corporate impunity, thereby ensuring legal certainty and protecting citizens' constitutional rights as guaranteed under Article 28G of the 1945 Constitution of the Republic of Indonesia.

2. Methods

This legal research employs a normative, or doctrinal, legal research method, which focuses on an in-depth examination of library materials. The primary objective of this study is to inventory and harmonize the positive legal norms applicable within the Indonesian legal system. This method is used to develop legal arguments and

formulate new legal concepts as prescriptive solutions to the legal issues under examination. The analysis is centered on statutory provisions and legal doctrines closely related to information security and electronic transactions. Through this normative approach, legal truth is sought based on the logic of legal science from a normative perspective in order to comprehensively address the legal issues at hand.

The approaches employed in this study include an integrated statutory approach and case approach. The statutory approach is carried out by examining all laws and sectoral regulations relevant to issues of personal data protection failure. Meanwhile, the case approach focuses on the legal analysis of the 2020 data breach involving 91 million Tokopedia users. The use of these approaches aims to provide a clear depiction of the legal facts and phenomena existing at the time of the research. In addition, a conceptual approach is also applied to strengthen the theoretical framework concerning the doctrine of corporate liability in cyberspace.

The primary data source for this research consists of secondary data, including both primary and secondary legal materials. The primary legal materials, which are authoritative in nature, include the Electronic Information and Transactions Law (ITE Law), Government Regulation on the Implementation of Electronic Systems and Transactions (GR PSTE), Government Regulation on Trading Through Electronic Systems (GR PMSE), and Minister of Communication and Information Regulation No. 20 of 2016. Secondary legal materials consist of prior research findings, textbooks on telematics law, scholarly papers, and relevant legal journals. Tertiary legal materials, such as legal dictionaries and the Indonesian Dictionary, are also used to provide additional clarification of technical terms. All legal materials

were collected through documentation studies and library research using various online academic databases. The data were analyzed using a qualitative descriptive method, presenting the findings in a narrative, systematic, and comprehensive manner. The analytical process employs deductive reasoning through the method of legal syllogistic logic to draw valid conclusions.

3. Results & Discussion

3.1 Implementation of Article 15 of the ITE Law and Government Regulation No. 71 of 2019 in the Tokopedia Data Breach Case

Article 15(1) of the Electronic Information and Transactions Law (ITE Law) expressly mandates that every Electronic System Operator (ESO) must operate an electronic system in a reliable and secure manner and is responsible for the proper functioning of that system. This provision imposes a clear legal obligation on platforms such as Tokopedia to ensure that all components of their information systems function properly in order to protect user data (Delpiero et al., 2021). From a juridical perspective, this responsibility is based on the principle of presumption of liability, under which an ESO is presumed liable for system failures unless it can prove otherwise. Consequently, in the 2020 data breach incident, Tokopedia bore the legal burden of demonstrating that the 91 million user records had been managed in accordance with applicable security standards. The application of this reversed burden of proof is particularly crucial because data subjects often lack the technical capacity to prove corporate negligence in a highly sophisticated technological environment.

Despite the strong mandate contained in the preceding clause, Article 15(3) of the ITE Law introduces a significant legal loophole for corporations through exemptions from liability. This provision stipulates that an ESO may be exempt from legal responsibility if it can prove that the failure resulted from force majeure, or from the fault or negligence of the user of the electronic system. In cases of large-scale cyberattacks, digital platforms frequently rely on this clause to argue that external cyberattacks constitute unforeseeable events beyond the company's control (Herryani et al., 2022). This defense strategy often shifts the legal debate away from internal systemic vulnerabilities and frames the incident merely as the unavoidable consequence of external threats. Moreover, claims regarding users' negligence in safeguarding their account credentials are often used to mitigate platform liability for broader database breaches. The lack of clear technical parameters for these exemptions creates a risk of corporate impunity, whereby ESOs may evade substantive legal consequences despite the existence of evident security vulnerabilities.

Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (GR 71/2019) provides more detailed obligations for ESOs in the processing of personal data. Under Article 14 of this regulation, ESOs are required to protect personal data against unauthorized access, misuse, and destruction throughout the data lifecycle. However, when a breach affects as many as 91 million accounts, the sanctions provided under Article 100 of GR 71/2019 are widely regarded as weak and disproportionate. The available sanctions are predominantly administrative in nature, ranging from written warnings

and administrative fines to temporary suspension of access or removal from the ESO registry. For a giant entity valued at billions of dollars, such as Tokopedia, written warnings or administrative fines alone are unlikely to create a deterrent effect proportionate to the immaterial losses suffered by millions of users. This weak enforcement mechanism and the lack of progressive sanctions represent a critical weakness in the effectiveness of Indonesia's sectoral data protection framework.

In response to the data protection failure, Tokopedia's CEO, William Tanuwijaya, sent an open letter via email to users in May 2020 as part of the company's effort to fulfill transparency obligations. From a regulatory standpoint, Article 14(5) of GR 71/2019 and Article 28 of Minister of Communication and Information Regulation No. 20 of 2016 require ESOs to provide written notification to data owners in the event of a data protection failure. However, an evaluation of the letter's contents indicates that the information provided was general in nature and lacked specific details regarding the technical causes of the system failure. In fact, the applicable regulations require such notification to include the specific reasons or causes of the failure to protect personal data confidentiality. The lack of transparency concerning the extent of exposed data and the concrete risks faced by data owners constitutes a disregard for consumers' right to transparency.

Government Regulation No. 80 of 2019 concerning Trading Through Electronic Systems (GR 80/2019) also establishes security standards for business actors operating in the digital marketplace. Article 59 emphasizes that parties storing personal data must maintain adequate preventive systems to anticipate any unlawful processing of such data. These standards of reasonableness and adequacy should be

aligned with international guidelines, such as the APEC Privacy Framework or standards equivalent to the GDPR (Dhianty, 2022). In Tokopedia's case, the fact that tens of millions of user records could be extracted and sold on platforms such as Raid Forums constitutes a strong indication of non-compliance with these standards. There is a clear inconsistency between the platform's promises of robust security in its Privacy Policy and the actual vulnerabilities exploited by hackers. This gap demonstrates that Indonesia's cyber regulatory framework still requires more uniform technical parameters to ensure legal certainty and strengthen consumer bargaining power.

Several legal scholars have suggested that liability for ESOs in data breach cases should be grounded in the doctrine of strict liability (Sabadina, 2021). Unlike fault-based liability, strict liability requires business actors to bear responsibility for losses without the need to prove fault in detail. This doctrine is particularly relevant in the e-commerce ecosystem, where consumers have virtually no technical control over how platform servers manage their data. Tokopedia's failure to prevent the mass extraction of user data satisfies the criteria for harmful interaction, thereby giving rise to an immediate obligation to provide compensation. However, existing positive law, including the ITE Law, still predominantly applies the principle of presumption of liability, which continues to leave room for ESOs to avoid accountability. A judicial shift toward the application of strict liability is therefore necessary to provide more concrete protection of citizens' fundamental rights in the digital sphere.

Privacy policies on marketplace platforms often function as standard-form contracts, commonly known as click-wrap agreements, which users must accept without any opportunity for negotiation. These documents frequently contain exoneration clauses designed to transfer risk or limit the platform's liability in the event of hacking incidents. For example, Tokopedia explicitly states that it cannot guarantee absolute security and that the risks associated with transmitting information are borne by users themselves. Such clauses are considered inconsistent with Article 18 of the Consumer Protection Law, which prohibits businesses from unilaterally transferring responsibility to consumers. Although platforms may argue that the breach was caused by third parties, their position as controllers of consumer data imposes a duty of protection without exceptions that unfairly disadvantage consumers. The presence of clauses limiting consumers' right to seek legal remedies underscores the urgent need for regulatory audits and the prohibition of unfair contractual terms.

The Tokopedia mass data breach was not merely a technical failure; it constituted a violation of human dignity and fundamental rights. Article 28G of the 1945 Constitution guarantees every citizen the right to personal protection and a sense of security. Victims of the Tokopedia breach suffered real immaterial harm in the form of anxiety, fear, and the loss of security resulting from the widespread exposure of their identities. The metadata leaked onto the dark web provides valuable resources for criminals to carry out subsequent attacks, including phishing and social engineering schemes. Despite the broad impact of such breaches, legal mechanisms for claiming compensation for immaterial damages in Indonesian

courts remain complex and insufficiently victim-oriented. Ensuring firm accountability for ESOs is therefore essential to safeguarding individual informational sovereignty amid the rapid growth of the national digital economy.

3.2 The Urgency of Reviewing Security Standards and Privacy Policies to Ensure Legal Certainty for Consumers in Digital Transactions

Privacy policies on digital platforms often function as standard electronic contracts (e-contracts) utilizing click-wrap agreements, under which users have no opportunity to negotiate and must accept all terms in order to access the service (Vickya et al., 2021). In practice, the privacy policies of platforms such as Tokopedia and Bhinneka frequently contain exoneration clauses stating that the company is not liable for losses or data breaches caused by third parties. The inclusion of such clauses clearly violates Article 18(1)(a) of Law No. 8 of 1999 on Consumer Protection, which prohibits business actors from unilaterally transferring their responsibilities. Such non-compliance renders these clauses void by operation of law, as they conflict with principles of fairness and reasonableness. This phenomenon further illustrates the weak bargaining position of consumers, who are effectively forced to bear cybersecurity risks independently amid systemic vulnerabilities. A re-evaluation of the legality of these standard clauses is urgently needed to prevent platforms from using inadequate internet security measures as an excuse to evade their responsibilities as data controllers.

Ambiguity in regulatory nomenclature also poses a serious obstacle to legal certainty, particularly with respect to the use of the term "Business Actor" in Government Regulation No. 80 of 2019 (GR 80/2019). Conceptually, marketplace

platforms often position themselves merely as intermediary service providers, even though they exercise full control as data controllers by collecting and processing consumers' personal information. This terminological confusion can be exploited by digital platforms as a loophole to avoid specific responsibilities for maintaining data confidentiality, responsibilities that should properly attach to providers of commercial services. As of 2022, the absence of a clear legal distinction between the roles of data controllers and data processors under Indonesian law has created fragmented accountability in cases of large-scale data breaches. This stands in sharp contrast to jurisdictions such as Singapore, where these roles are clearly delineated in the regulatory framework. Harmonizing this nomenclature is essential to ensure that every failure of data protection has a clearly identifiable legal subject that bears full responsibility (Nafi'ah et al., 2020).

The rapid growth of cross-border digital transactions requires Indonesia to promptly align its national data protection standards with international principles. International instruments such as the OECD Guidelines on the Protection of Privacy establish crucial principles, including collection limitation and security safeguards, which should be incorporated into domestic law. In addition, the General Data Protection Regulation (GDPR) has become the global benchmark, emphasizing integrity, confidentiality, and a high standard of accountability for personal data processors. Indonesia's current cyber regulatory framework remains fragmented and has yet to meet the high level of protection adopted in more than one hundred countries worldwide. Without harmonization with global standards, Indonesia's digital economy ecosystem will struggle to ensure the security of

international data flows and the integrity of electronic commerce. Digital platforms in Indonesia must therefore be required to align their privacy policies with internationally recognized standards of transparency and data minimization.

A personal data breach is not merely a technical failure of a company's servers; it constitutes a direct violation of citizens' constitutional rights. Article 28G(1) of the 1945 Constitution explicitly guarantees the protection of personal integrity, honor, dignity, and the right to security against threats and fear. Any failure to preserve the confidentiality of account holders' personal information represents an affront to the dignity of individuals as data subjects. In the digital era, privacy must be understood as the individual's freedom to control personal information without unlawful interference or surveillance. The absence of comprehensive legal protection to date indicates the state's inadequate preparedness in fulfilling its constitutional obligation to protect its citizens in cyberspace. Protection of personal information is now an indispensable prerequisite for the continuation of human civilization, which has become increasingly dependent on information technology (Alfreda et al., 2021).

The urgency for stronger regulation is also driven by the rapid evolution of cybercrime, which has become increasingly complex and destructive. The data leaked in the Tokopedia incident, such as email addresses and phone numbers, has become valuable material for criminals to conduct follow-up attacks, including phishing and social engineering (Naufal, 2020). Furthermore, emerging threats such as ransomware no longer target only corporate infrastructure but also threaten the destruction or misuse of the personal data of millions of consumers. Existing regulations, particularly the ITE Law, remain overly focused on civil remedies, which

are often difficult for ordinary citizens to access. More progressive criminal law policies are needed to address corporate negligence and to create a genuine deterrent effect through substantial fines and severe criminal sanctions.

4. Conclusion

Indonesia's current positive cyber law instruments, particularly the Electronic Information and Transactions Law (ITE Law) and Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions (GR 71/2019), are considered insufficiently effective in imposing full liability on PT Tokopedia for the massive data breach incident. Although the principle of presumption of liability is juridically recognized under Article 15 of the ITE Law, the reversed burden of proof often fails to provide substantive justice for consumers amid the complexities of cyber technology. A fundamental weakness lies in the administrative sanctions provided under GR 71/2019, which are largely limited to written warnings or temporary suspension of access. Such sanctions are clearly disproportionate to the scale of harm suffered by 91 million users. Furthermore, the exemptions from liability contained in Article 15(3) of the ITE Law such as force majeure or user negligence create opportunities for Electronic System Operators (ESOs) to evade substantive legal responsibility. As a result, the fulfillment of compensation rights for affected data subjects is often hindered by the lack of clear parameters for determining system fault.

The findings of this study also demonstrate an urgent legal need to reassess national electronic system security standards in order to ensure legal certainty for

consumers in the aftermath of the Tokopedia case. A comprehensive evaluation of sectoral regulations is imperative, particularly to explicitly prohibit the use of exoneration clauses in privacy policies that disclaim platform liability for breaches caused by third parties. Such standard contractual clauses are clearly inconsistent with Article 18 of the Consumer Protection Law and significantly undermine both the dignity and bargaining position of individuals in the digital sphere. The harmonization of technical oversight standards and electronic system audit mechanisms must be integrated to close loopholes that enable corporate impunity and to ensure the protection of the fundamental right to security. Personal data protection must be recognized as part of the fulfillment of the constitutional mandate under Article 28G of the 1945 Constitution, thereby safeguarding the informational sovereignty of every citizen.

As a corrective measure, the role of the Ministry of Communication and Information Technology should be strengthened to enable more proactive and rigorous technical oversight of data processing by private-sector ESOs. The government should require periodic security audits conducted by independent institutions to ensure ESO compliance with high-level data protection standards. Beyond regulatory reinforcement, improving data literacy among the general public is equally crucial so that consumers can make informed decisions when granting access to their personal information and better understand their legal rights in the event of system failures. Dispute resolution mechanisms, including mediation panels and formal complaint channels, must also be optimized to ensure that data owners can obtain timely and transparent remedies. Ultimately, synergy between robust state

oversight and strong accountability on the part of digital platforms is essential to restoring public trust in Indonesia's digital economy ecosystem.

References

Alfreda, I. J., Permata, R. R., & Ramli, T. S. (2021). *Pelindungan dan tanggung jawab kebocoran informasi pada penyedia platform digital berdasarkan perspektif rahasia dagang*. Jurnal Sains Sosio Humaniora, 5(1), 1–16.

Delpiero, M., Reynaldi, F. A., Ningdiah, I. U., & Muthmainnah, N. (2021). *Analisis yuridis kebijakan privasi dan pertanggungjawaban online marketplace dalam perlindungan data pribadi pengguna pada kasus kebocoran data*. Padjadjaran Law Review, 9(1).

Dhianty, R. (2022). *Kebijakan privasi (privacy policy) dan peraturan perundang-undangan sektoral platform digital vis a vis kebocoran data pribadi*. Scripta: Jurnal Kebijakan Publik dan Hukum, 2(1), 186–199.

Herryani, M. R. T. R., & Njoto, H. (2022). *Perlindungan hukum terhadap kebocoran data pribadi konsumen online marketplace*. Transparansi Hukum, 5(1).

Muhammad, M. O., & Nugroho, L. D. (2021). *Perlindungan hukum terhadap pengguna aplikasi e-commerce yang terdampak kebocoran data pribadi*. Jurnal Pamator: Jurnal Ilmiah Universitas Trunojoyo, 14(2), 165–174.

Nafi'ah, R. (2020). *Pelanggaran data dan pencurian identitas pada e-commerce*. Cyber Security dan Forensik Digital, 3(1), 7–13.

Naufal, R. A. (2020). *Tanggung jawab PT Tokopedia dalam kasus kebocoran data pribadi pengguna*.

Sabadina, U. (2021). *Politik hukum pidana penanggulangan kejahatan teknologi informasi terkait kebocoran data pribadi oleh korporasi berbasis online*. Lex Renaissance, 6(4), 799–814.

Sylfia, A., Amrullah, M. F., & Djaja, H. (2021). *Tanggungjawab yuridis PT. Tokopedia atas kebocoran data pribadi dan privasi konsumen dalam transaksi online*. Bhirawa Law Journal, 2(1), 21–27.

Vickya, A., & Kusumadewi, R. (2021). *Kewajiban data controller dan data processor dalam data breach terkait pelindungan data pribadi berdasarkan hukum Indonesia dan hukum Singapura: Studi kasus data breach Tokopedia*. Padjadjaran Law Review, 9(1).