

The Company's Legal Responsibility for Consumer Personal Data Leaks (Case Study on Tokopedia)

Nanda Putri Andana Kusuma¹⁾ & Satino²⁾

¹⁾ Faculty of Law, Universitas Pembangunan Nasional "Veteran" Jakarta, Indonesia,
E-mail: 2210611435@mahasiswa.upnvj.ac.id

²⁾ Faculty of Law, Universitas Pembangunan Nasional "Veteran" Jakarta, Indonesia,
E-mail: satino@upnvj.ac.id

Abstract. *The personal data leak experienced by Tokopedia in 2020 was one of the biggest incidents in the history of data protection in Indonesia. This incident, which involved more than 91 million user accounts, raised concerns about weak cybersecurity and the lack of law enforcement related to personal data protection. This study aims to analyze the legal responsibility of companies for the leakage of consumer personal data based on applicable laws and regulations, including the Personal Data Protection Law (PDP Law), the Electronic Information and Transaction Law (ITE Law), and their derivative regulations. The research method used is normative legal research through the study of laws and regulations, literature, and case documents. The results of the study show that as an Electronic System Operator (PSE), Tokopedia has an obligation to ensure the security of personal data and is responsible for any violations that occur. Affected users have several legal remedies, including administrative complaints to the Ministry of Communication and Information Technology, civil lawsuits based on unlawful acts, class actions, and criminal reports. This study emphasizes the importance of enforcing the principles of accountability and consumer protection in personal data management to prevent similar incidents from recurring in the future.*

Keywords: Consumer; Data; Personal; Responsibility; Tokopedia.

1. Introduction

Every human being has an identity that distinguishes one individual from another. This identity is recorded in the form of personal data, which can facilitate various administrative and social needs. In today's modern era, personal data plays an increasingly vital role because almost all activities, whether in the economic, educational, health, or public service sectors, require the recording and verification of personal identity. This situation makes personal data not just information, but a vital asset that must be kept confidential. Personal data is an asset or commodity with high economic value (Edmon Makarim, 2003). For companies, personal data is a crucial resource for product design, marketing

strategies, service improvement, and even profit generation. In the digital era, consumer personal data has become a crucial asset, frequently collected, stored, and processed by companies in e-commerce, banking, telecommunications, and other digital services. However, as data processing increases, the risk of personal data breaches also increases, both due to internal negligence and cyberattacks.

One company that requires personal data is a marketplace company. With the advancement of technology, buying and selling transactions can now be conducted online through marketplace platforms. A marketplace is an online platform that provides a platform that connects buyers and sellers to transact with each other (Deni Apriadi, 2025). Conceptually, a marketplace is likened to a virtual traditional market (Rini Yustiani, Rio Yunanto, 2017). There are several marketplaces in Indonesia, such as Tokopedia, Shopee, and Lazada. To make a purchase or sale on a marketplace, each individual is required to register to create an account. The account creation process requires users to provide personal data. One of the largest marketplace companies in Indonesia is Tokopedia. PT Tokopedia is an Indonesian technology-based company founded on February 6, 2009, by William Tanuwijaya and Leontinus Alpha Edison under the auspices of PT Tokopedia. Tokopedia has now been in existence for 14 years. Over the past 14 years, Tokopedia has promoted equality in the digital economy by motivating Indonesians to start selling online. In 2018, PT Tokopedia received funding of \$ 1.1 billion from Alibaba Group and Softbank Vision Fund (www.tokopedia.com).

In 2020, Tokopedia experienced a user data breach involving over 91 million accounts. The leaked data included usernames, email addresses, and passwords. Although Tokopedia stated that user financial data remained secure, the incident highlighted the weaknesses in its cybersecurity system and the company's unpreparedness for a large-scale cyberattack. This case sparked public unrest and prompted the government to expedite the development of legislation that comprehensively regulates personal data protection (CNN Indonesia, 2025). The Tokopedia personal data leak marked a significant milestone in the history of data protection in Indonesia, as it highlighted a legal vacuum before the enactment of Law No. 27 of 2022 concerning Personal Data Protection (PDP Law). Previously, regulations regarding personal data were only contained in a few sectoral regulations, such as Law No. 11 of 2008 concerning Electronic Information and Transactions and its amendments, and Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (Edmon Makarim, 2021).

With the implementation of the Personal Data Protection Law, companies that manage personal data are required to ensure data security and confidentiality and are responsible for any breaches or leaks resulting from negligence in managing such data. This law establishes the principle of accountability and regulates administrative sanctions and criminal penalties for data controllers who fail to protect users' personal information. A company's legal responsibility is not only

moral or ethical but also has significant legal consequences. Therefore, this study is crucial because it seeks to examine the extent to which companies' legal responsibility for consumer personal data leaks is implemented in Indonesia, using the Tokopedia case as the main focus. This study also aims to identify the extent to which the principles of the Personal Data Protection Law can provide effective protection for consumers and serve as a basis for law enforcement against companies that commit negligence. The results of this research are expected to provide theoretical contributions to the development of cyber law in Indonesia and serve as a guideline for policymakers and industry players in improving the management of personal data protection in the future.

2. Research Methods

This research uses a normative legal research method (normative juridical), focusing on the assessment of positive legal norms or principles applicable in Indonesia. This approach is used to examine the legal liability of companies for the breach of consumer personal data, referring to applicable laws and regulations and relevant legal doctrines. Normative legal research focuses on the analysis of legal materials sourced from literature, regulations, and legal documents related to the issue under study (Soerjono Soekanto, 2015). This study employed several approaches, namely the statute approach, the conceptual approach, and the case approach. The statutory approach was conducted by examining various regulations that serve as the legal basis for personal data protection in Indonesia, including Law No. 27 of 2022 concerning Personal Data Protection (UU PDP), Law No. 11 of 2008 concerning Electronic Information and Transactions and its amendments (UU ITE), Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP PSTE), Regulation of the Minister of Communication and Informatics Number 20 of 2016 concerning Personal Data Protection in Electronic Systems, and Law No. 8 of 1999 concerning Consumer Protection. The conceptual approach was used to examine relevant legal theories and doctrines, such as the theory of legal liability, the principle of due diligence, and the principles of personal data protection (data protection principles) (Peter Mahmud Marzuki, 2019). Meanwhile, a case approach is used to examine the 2020 Tokopedia personal data leak case as a concrete case study to determine the application of the company's legal responsibilities based on applicable legal provisions (Syahrudin Nawi, 2018).

The legal sources used in this study consist of primary legal materials, secondary legal materials, and tertiary legal materials. Primary legal materials include various laws and regulations that directly regulate personal data protection and corporate legal liability. Secondary legal materials include literature, journals, and scientific articles that support and explain the primary legal materials. Tertiary legal materials are used to clarify legal terms or concepts contained in primary and secondary legal materials, such as legal dictionaries and legal encyclopedias (Soejono, 2003). The legal material collection technique was carried out through

library research, namely by exploring various relevant written sources such as laws and regulations, law books, scientific journals, court decisions, and official government and legal institution websites. The collected legal materials were then analyzed using qualitative analysis, namely by describing, interpreting, and connecting applicable legal provisions with relevant legal theories and legal facts contained in the Tokopedia data breach case. This analysis is descriptive-analytical, namely by comprehensively describing the form of the company's legal responsibility for the breach of consumer personal data and the legal remedies that can be taken by the injured party (Mukti Fajar ND, 2017). Through this approach, it is hoped that comprehensive conclusions can be obtained regarding the implementation of corporate legal responsibilities regarding personal data protection in Indonesia.

3. Results and Discussion

3.1. Forms of Legal Responsibility of Companies for Leaks of Consumer Personal Data Based on the Provisions of Laws and Regulations in Force in Indonesia

The chronology of the Tokopedia data leak incident began on March 20, 2020, when a hacking incident allegedly occurred by a hacker under the pseudonym Whysodank. Several weeks later, on Saturday, May 2, 2020, the account uploaded the results of its hack on Raid Forum, an online forum site often used to trade hacked data. On the same day, the account @underthebreach, known as an Israeli data breach monitoring and prevention service, published a tweet on Twitter regarding the alleged Tokopedia user data leak. In its post, the account stated that approximately 15 million Tokopedia user account data had been successfully hacked and was being traded on the forum. The personal data consisted of user IDs, email addresses, full names, dates of birth, genders, mobile phone numbers, and passwords that were still hashed or encrypted. On Sunday, May 3, 2020, a hacker under the pseudonym Whysodank announced that he had sold approximately 91 million Tokopedia user data on a dark web forum called Empire Market. Shortly after the information spread, PT Tokopedia's Vice President of Corporate Communications, Nuraini Razak, issued an official statement confirming the user data leak. However, she emphasized that sensitive data, such as encrypted passwords, as well as financial information such as debit card numbers, credit cards, bank accounts, and OVO balances, remained safe and were not leaked.

Then on Tuesday, May 5, 2020, Tokopedia CEO William Tanuwijaya sent a mass email (email blast) to all Tokopedia users. In the email, he acknowledged the data theft by an unauthorized third party and explained that the company was conducting an internal investigation to ensure the security of user accounts and smooth transactions. William also stated that Tokopedia was working with authorities and the cybersecurity team to follow up on the incident and strengthen the data protection system in the future. Following up on the series of data leak events, on May 6, 2020, the Indonesian Consumer Community (KKI), chaired by

David Tobing, officially filed a lawsuit against two parties, namely the Minister of Communication and Information Technology (as Defendant I) and PT Tokopedia (as Defendant II). This lawsuit was registered through the e-court system at the Central Jakarta District Court with Case Number 235/PDT.G/2020/PN.JKT.PST, and began trial on June 10, 2020. KKI filed the lawsuit after receiving several reports from Tokopedia users who felt their personal data had been controlled and accessed without permission. The personal data in question included user IDs, email addresses, dates of birth, gender, and telephone numbers. The reporters expressed concerns about the potential misuse of their personal data for future unlawful acts that could result in material and immaterial losses.

In its petitum, KKI conveyed demands, including a request for the Minister of Communication and Information to revoke the Electronic System Provider Registration Certificate in the name of Tokopedia, to punish Tokopedia by paying an administrative fine of IDR 100 billion to be deposited into the state treasury no later than 30 calendar days after the case decision has permanent legal force, and to ask Tokopedia to issue an apology and statement of responsibility published in three Indonesian print media, namely *Bisnis Indonesia*, *Kompas*, and the *Jakarta Post* (tekno.kompas.com, 2025). In addition, KKI also asked the court to order Defendant II (PT. Tokopedia) to notify Tokopedia account owners in writing regarding the details of personal data that has been controlled by a third party without the consent of the account owners. Following the incident, on May 12, 2020, Tokopedia CEO William Tanuwijaya sent an open letter via email to all Tokopedia users.

A company's legal liability can be divided into three forms: administrative, civil, and criminal. Administrative liability includes sanctions in the form of written warnings, temporary suspension of activities, deletion of personal data, and administrative fines (R. Subekti, 2014). In the realm of civil law, the principle of liability based on fault is the basis for determining a company's responsibility. If a data breach is proven to have occurred due to negligence or a lack of security measures on the part of the company, the company is obligated to compensate the data owner. This aligns with Article 1365 of the Civil Code (KUH Perdata) concerning unlawful acts. From a criminal law perspective, Articles 67 to 70 of the PDP Law provide the basis for imposing criminal sanctions on perpetrators of data breaches. According to Article 46 paragraph (1) of the PDP Law, every personal data controller is required to notify the data owner in writing within a maximum of 3 x 24 hours after the leak occurs. This obligation demonstrates a company's moral and legal responsibility to be transparent with the public. If a company ignores this notification obligation, it may face administrative and even criminal sanctions.

PT Tokopedia's obligation as a PSE is to implement the principles of Personal Data Protection as regulated in Article 14 of the Government Regulation on PSTE in 2019. The PMSE PP also regulates the obligations of Electronic System Organizers,

namely to store personal data in accordance with personal data protection standards or prevailing business practices. The personal data breach incident that occurred at Tokopedia falls within the scope of Electronic System Management activities. Based on the provisions of Article 3 of Government Regulation Number 71 of 2019 concerning the Management of Electronic Systems and Transactions (PP PSTE), every Electronic System Operator (PSE) is required to manage its system reliably and securely and is responsible for the functioning of the system in accordance with applicable regulations. The PSE is legally responsible for the Management of the Electronic System. In this case, PT Tokopedia was deemed to have failed to comply with its obligation to implement the principle of prudence in ensuring the security and protection of its users' personal data. The duty of prudence is a fundamental principle in the use of Information Technology and Electronic Transactions, meaning that prudence requires attention to all aspects that could potentially cause harm, both to oneself and to others, in the use of Information Technology and Electronic Transactions.

3.2. Legal measures that can be taken by Tokopedia users regarding the leak of their personal data against the Tokopedia Company

Personal data protection in Indonesia is regulated by several legal instruments, including Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law) and its amendments, and Regulation of the Minister of Communication and Informatics Number 20 of 2016 concerning Personal Data Protection in Electronic Systems. Based on Article 46 of the PDP Law, any personal data subject who suffers a loss due to a data protection violation has the right to file a lawsuit for compensation against the data controller or responsible party. In this case, Tokopedia users are positioned as personal data subjects, while Tokopedia acts as the controller and manager of user data, which has a legal obligation to maintain the confidentiality and security of said data. The first legal remedy a user can take is to file an administrative complaint with the Ministry of Communication and Informatics (Kominfo), the supervisory authority for personal data protection. Kominfo has the authority to conduct investigations, issue warnings, and even impose administrative sanctions on companies found to have failed to fulfill their obligations as a PSE.

In addition to administrative complaints, Tokopedia users can also pursue civil legal action based on unlawful acts (PMH) as stipulated in Article 1365 of the Civil Code. The elements of PMH—namely, the existence of an act, fault, loss, and a causal relationship between the act and the loss—can be met if the company is proven to have been negligent in maintaining its security system, resulting in losses for users. These civil lawsuits can be filed individually or as a class action. In the context of the Tokopedia data breach, which involved millions of users, the class action mechanism is relevant because it is efficient and represents the interests of many parties who have suffered similar losses. Class actions are also

recognized in Indonesian civil procedure law and are regulated by Supreme Court Regulation No. 1 of 2002.

In civil cases, the types of compensation that can be sought include material and immaterial damages. Material damages cover economic losses arising from the unauthorized use or misuse of personal data, while immaterial damages relate to non-financial losses such as psychological distress, fear, and reputational damage experienced due to the distribution of personal data in the digital space. In addition to civil proceedings, users also have the right to pursue criminal proceedings if the data leak case contains elements of a criminal act. Based on the provisions of Articles 30 and 32 of the Electronic Information and Transactions Law (UU ITE), anyone who intentionally and without authority accesses or changes the electronic system of another party can be subject to criminal sanctions. In this context, although hackers are primarily responsible, Tokopedia's negligence in maintaining the security of its electronic system can be considered a factor that aggravates the company's legal liability (Law Number 27 of 2022).

The Personal Data Protection Law (PDP Law) also serves as the legal basis for imposing criminal sanctions on data controllers who intentionally or negligently cause personal data leaks. For example, Article 67 of the PDP Law stipulates that personal data controllers who fail to comply with data security provisions may be subject to criminal penalties including imprisonment and significant fines (Law Number 8 of 1999). Additionally, users have the option to pursue dispute resolution mechanisms outside the courts, such as mediation or arbitration, if such provisions are outlined in the Tokopedia platform's terms and conditions. This alternative is generally chosen because it is considered more efficient and can resolve disputes in a shorter timeframe than litigation (Nindyo Pramono, 2021). Essentially, the legal liability stipulated in the ITE Law and its implementing regulations adheres to the principle of presumption of liability, which assumes responsibility rests with the electronic system provider. Therefore, Tokopedia is obligated to prove that the data breach incident occurred not due to its negligence, but rather due to the actions of a third party or factors beyond its control (Sinta Dewi, 2020).

From a consumer protection perspective, Tokopedia users also have the right to pursue legal action under Law No. 8 of 1999 concerning Consumer Protection (UUPK). Article 19 of the UUPK stipulates that business actors are obligated to provide compensation for losses suffered by consumers due to the use of their goods or services, including losses arising from breaches of personal data (Ahmad M. Ramli, 2019). In practice, the National Consumer Protection Commission, along with the Non-Governmental Consumer Protection Institution (LPKSM), can act as legal counsel or representatives for Tokopedia users who have suffered losses. These institutions play a crucial role in strengthening users' positions when seeking justice for violations of their personal data. Users also have the right to demand a public apology and restoration of their good name, as is generally the

case in cases of privacy violations. This public apology serves as a manifestation of the company's moral responsibility and serves as a preventative measure that serves as a deterrent for other businesses to be more careful in managing consumers' personal data.

4. Conclusion

Legally, corporate responsibility for personal data breaches is regulated by various legal instruments, such as the PDP Law, the ITE Law and its amendments, Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP PSTE), and Law No. 8 of 1999 concerning Consumer Protection (UUPK). Based on these regulations, companies as Electronic System Providers (PSE) are required to ensure system security and are responsible for any violations arising from negligence in data management. Tokopedia's failure to prevent data leaks can be categorized as a violation of the principles of prudence and accountability regulated by Indonesian positive law. For consumers who have suffered losses, there are several legal remedies available to obtain protection and justice. These include administrative complaints to the Ministry of Communication and Informatics (Kominfo), civil lawsuits based on Article 1365 of the Civil Code concerning unlawful acts, and the possibility of criminal law enforcement if criminal elements are found in data breaches. Furthermore, consumers can also pursue dispute resolution mechanisms through non-litigation channels such as mediation or arbitration, and seek compensation, both material and immaterial, for losses arising from the misuse of personal data. With the Tokopedia data breach, it is crucial for every digital company to strengthen its cybersecurity system and consistently implement personal data protection principles. Personal data protection is not only a moral obligation but also a legal responsibility that must be carried out by every business actor in maintaining consumer trust. Going forward, it is hoped that the implementation of the Personal Data Protection Law will be an effective instrument in realizing legal certainty, increasing corporate accountability, and building a safe and ethical digital ecosystem in Indonesia.

5. References

Books:

- Dewi, S. (2020). *Perlindungan Data Pribadi Dalam Era Digital*. Bandung: Refika Aditama.
- Fajar, M., & Achmad, Y. (2017). *Dualisme Penelitian Hukum Normatif & Empiris*. Yogyakarta: Pustaka Pelajar.
- Makarim, E. (2003). *Kompilasi Hukum Telematika*. Jakarta: Raja Grafindo Persada.
- Makarim, E. (2021). *Perlindungan Data Pribadi Dalam Era Digital*. Jakarta: Rajawali Pers.
- Marzuki, P. M. (2019). *Penelitian Hukum*. Jakarta: Kencana Prenada Media Group.
- Nawi, S. (2018). *Penelitian Hukum Normatif Versus Penelitian Hukum Empiris*. Makassar: Pt Umitoha Ukhuwah Grafika.

- Pramono, N. (2021). *Hukum Perlindungan Konsumen Di Indonesia*. Yogyakarta: Ugm Press.
- Ramli, A. M. (2019). *Cyberlaw Dan Perlindungan Privasi Di Indonesia*. Jakarta: Kominfo Press.
- Soejono, & Abdurrahman, H. (2003). *Metode Penelitian Hukum*. Jakarta: Rineka Cipta.
- Soekanto, S., & Mamudji, S. (2015). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: Raja Grafindo Persada.
- Subekti, R. (2014). *Pokok-Pokok Hukum Perdata*. Jakarta: Intermasa.

Journals:

- Apriadi, D., & Saputra, A. Y. (2025). E-Commerce Berbasis Marketplace Dalam Upaya Mempersingkat Distribusi Hasil Pertanian. *Jurnal Resti*. Retrieved October 27, 2025, From <Http://Jurnal.laii.Or.Id/Index.Php/Resti/Article/View/36/20>
- Yustiani, R., & Yunanto, R. (2017). Peran Marketplace Sebagai Alternatif Bisnis Di Era Teknologi Informasi. *Jurnal Ilmiah Komputer Dan Informatika (Komputa)*, 6(2), 44. Universitas Komputer Indonesia.

Regulation:

- Civil Code (KUHPerdata).
- Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions.
- Government Regulation Number 80 of 2019 concerning Trade Through Electronic Systems.
- Law No. 11 of 2008 concerning Electronic Information and Transactions and its amendments.
- Law No. 27 of 2022 concerning Personal Data Protection.
- Law No. 8 of 1999 concerning Consumer Protection.
- Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems.

Internet:

- CNN Indonesia. (2020, May 3). Kronologi lengkap 91 juta akun Tokopedia bocor dan dijual. CNN Indonesia. Retrieved November 9, 2025, from <https://www.cnnindonesia.com/teknologi/20200503153210-185-499553>
- CNN Indonesia. (2020, May 6). Kebocoran data Tokopedia dorong regulasi perlindungan data pribadi. CNN Indonesia. Retrieved November 6, 2025, from <https://www.cnnindonesia.com/teknologi/20200506104028-185-501931>
- Hitekno.com. (2020, May 13). Akui data pelanggan Tokopedia dicuri, ini surat terbuka William Tanuwijaya. Hitekno.com. Retrieved November 10, 2025, from <https://www.hitekno.com/internet/2020/05/13/123324>

- Hukumonline.com. (2020). Kasus bocornya data pribadi konsumen Tokopedia berujung ke meja hijau. Hukumonline. Retrieved November 9, 2025, from <https://www.hukumonline.com/berita/a/kasus-bocornya-data-pribadi-konsumen-tokopedia-berujung-ke-meja-hijau-lt5eb331b39427b>
- Kompas Tekno. (2020, June 10). Sidang perdana kasus kebocoran data Tokopedia digelar hari ini. Kompas.com. Retrieved November 9, 2025, from <https://tekno.kompas.com/read/2020/06/10/09144017>
- Tokopedia. (2025). Our story. Retrieved November 6, 2025, from <https://www.tokopedia.com/about/our-story>