Personal Data Protection in E-Commerce: Threats, Risks, Security Strategies, and Regulatory Compliance.

By:

Group 4

Muhammad Fakhri Amir

Rasyad Naufal Ibrahim

Zahwa Aprilia

CLASS 2CS2

FACULTY OF ENGINEERING

CEP-CCIT FTUI

2025

PREFACE

We express our deepest gratitude to Almighty God for His boundless mercy and grace in completing this manuscript, which is part of the Center of Excellence Program (CEP) at the Center for Computing and Information Technology (CCIT), Faculty of Engineering, University of Indonesia. We also extend our appreciation to mentors and colleagues whose support has been invaluable in shaping this work.

The rapid growth of digital technologies has revolutionized data-driven decision-making but also increased risks to personal data privacy (PDP). Cyberattacks, data breaches, and unauthorized access pose significant threats as businesses rely more on data. This manuscript explores PDP challenges, legal frameworks like Indonesia's Personal Data Protection Law (Law No. 27 of 2022), and technological solutions such as machine learning and encryption to enhance data security.

As cyber threats evolve, a proactive approach to PDP is essential. By examining real-world cases and best practices, this work provides valuable insights for researchers, professionals, and organizations. Our goal is to bridge the gap between theory and practice, empowering stakeholders to implement secure and innovative solutions in the digital era.

CEP- CCIT Faculty of Engineering
Universitas indonesia

Table Of Contents

CHAPTER 1 INTRODUCTION

I.1 Background

Numerous facets of human existence have been profoundly impacted by the quick development of information technology, especially in the area of internet access. The emergence of e-commerce, which makes it easier to purchase and sell products and services online, is one of the significant changes brought about by this technological advancement. Platforms like Tokopedia, Lazada, and Akulaku have emerged as major participants in this market in Indonesia, facilitating easy transactions but also presenting serious difficulties for the safety of customer personal information.

Digital transactions provide many financial advantages, but protecting personal information is still a big worry. Cases of cybercrime, data breaches, and illegal access to private customer data have brought up important legal and security concerns. Many customers unintentionally reveal their financial information, transaction history, and personal identification history to possible dangers as a result of Electronic System Providers' (ESP) insufficient security procedures. Privacy hazards are further increased by the growing dependence on big data, as businesses gather and examine enormous volumes of user data.

Evaluating how well e-commerce platforms adhere to regulatory requirements for securing personal data is crucial given the ever-changing nature of data security risks. Gaining customer trust, adhering to regulations, and improving data security procedures all depend on understanding these compliance methods.

I.2 Writing Objective

The primary objective of this study is to analyze the responsibilities of Electronic System Providers (ESP**)** in safeguarding consumer personal data in digital transactions. Specifically, this paper aims to:

- Identifying Data Security Breach Risks for E-Commerce and Individuals.
- Knowing What are the Threats to Personal Data Security in E-Commerce.
- Know the applicable regulations.

I.3 Problem Domain

The study focuses on the risks and challenges associated with personal data protection in e-commerce transactions, particularly on platforms such as Tokopedia, Lazada, and Akulaku. The core research questions addressed in this paper include:

a) How do security threats impact the protection of personal data in e-commerce transactions?
b) To what extent do e-commerce platforms comply with regulatory requirements on personal data protection?
c) What are the key strategies used by Electronic System Providers (ESP) to enhance consumer data security?

I.4 Writing Methodology

This study is based on research that examines the complexities of personal data protection (PDP) in digital transactions. The analysis incorporates legal, ethical, and technological perspectives to provide a comprehensive understanding of data security challenges. The research also evaluates Indonesia’s Personal Data Protection Law (Law No. 27 of 2022) and explores potential solutions, including advancements in

machine learning, encryption, and cybersecurity measures. Through this approach, the study aims to bridge the gap between theoretical knowledge and practical implementation in ensuring effective PDP strategies.

I.5 Writing Framework

CHAPTER I INTRODUCTION

Include Background, Writing Objective, Problem Domain, and Writing Methodology.

CHAPTER II BASIC THEORY

Contains all theories about personal data protection.

CHAPTER III PROBLEM ANALYSIS

Includes analysis of case study examples.

CHAPTER IV CONCLUSION AND SUGGESTION

Conclusions and suggestions include material and analysis.

CHAPTER II BASIC THEORY

II.1 What is Personal Data and Data Protection?

According to Law Number 27 of 2022 Article 1, Personal Data is data about an individual person who is identified or can be identified by alone or in combination with other information either directly or indirectly through electronic or non-electronic systems.

Personal Data Protection is the overall effort to protect Personal Data in a series of processing of Personal Data to ensure the constitutional rights of Personal Data subjects.

II.2 What are the Threats to Personal Data Security in E-Commerce

Information that can be used to directly or indirectly identify an individual is known as personal data. Personal data might be threatened in many different ways and from many different sources.

a. Phishing

   The goal of this assault is to obtain private data, like credit card numbers or passwords, by pretending to be a reliable source.

b. Malware and Ransomware

   Malware is software that is intended to steal, corrupt, or access data without authorization.The victim's data is encrypted by ransomware, which then demands a fee to unlock it.

c. Social Engineering

The victim is coerced by the assailant into willingly divulging personal information. Social engineering methods like implantation or other forms of manipulation are one example.

d. Theft of Identity

The fraudster opens a bank account or obtains credit on the victim's behalf using the victim's personal information.

II.3 Risks of Personal Data Security Breach

Breach of personal data security can put people and businesses at danger in a number of ways. These hazards include monetary losses, harm to one's reputation, legal troubles, and interruptions in business operations.

A. Risk to Individuals:

- Financial Loss: Personal information may be abused to get access to bank accounts, submit loan applications, or make unlawful purchases.
- Reputational harm: Fraudsters can propagate false information using personal information, harming a person's reputation.
- Emotional and Psychological Losses: Privacy violations can cause emotional and psychological stress, which can result in feelings of uneasiness, anxiety, and fear.
- Identity Theft: Victims may have their personal information, including addresses, dates of birth, and ID numbers, stolen and used to open bank accounts, commit fraud, or apply for loans.
- Extortion: Online blackmail, especially sexual extortion, can be carried out through social media account hacking.
- Illegal internet Loans: Victims of illegal internet loan schemes may be intimidated for reimbursements once their personal information is abused.

B. Risks to the Company:

- Reputational Loss: Over time, data breaches can have a detrimental effect on a company's reputation and customer trust.
- Financial Losses: Net income may decline as a result of business losses, penalties, indemnity payments, and legal fees. A business lost billions of dollars as a result of leaking personal information.
- Regulatory and Legal Losses: Businesses who break the Personal Data Protection Law (PDP) risk severe legal repercussions.
- Operational Disruption: Business operations may be affected by a data breach.

II.4 Regulation and Legal Protection

Personal Data Protection Law Number 27 of 2022 (PDP Law). This bill marks a significant turning point in the nation's attempts to safeguard its citizens' personal information in the quickly changing digital age. With the advancement of ever-more-advanced information technology, safeguarding personal information has become crucial to upholding both digital information security and individual privacy rights.

By developing a code of conduct, electronic system operators can protect the personal information of their customers. through internal policy, or self-regulation. One of the most likely solutions to customers' data protection issues is self-regulation for businesses involved in electronic commerce in the form of a privacy policy. This is a must.

"Every Organizer Electronic systems must formulate rules internal protection of Personal Data as a precautionary measure for the occurrence of failures in protection of Personal Data it manages," states Article 5 paragraph (2) of Kominfo Regulation 20/2016.

CHAPTER III PROBLEM ANALYSIS

III.1 Examples of personal data theft cases

In March of 2020, there was a huge hack of Tokopedia, in which there was a leak of around 91 million users' and 7 million merchants' accounts. The hacker "ShinyHunters" was in a position to get access to the database of Tokopedia and retrieve users' personal information, i.e., user ID, email, full name, birth date, gender, phone number, and password in encrypted hash form. Although financial information such as bank account information and credit card information is not leaked, leaked information is risky enough in that it is possible to use it to execute phishing attacks and identity thefts. The leak shows that there is a huge security loophole in Tokopedia's system, otherwise capable of keeping users' details more stringently secure.

On May 3, 2020, the account of @underthebreach posted news of a leak of Tokopedia account details on hacker forums. The initial estimate was that around 15 million of its account holders were compromised, though a more careful analysis found that it was a maximum of 91 million. One day after that, on May 4, 2020, hackers sold all of that data on the dark web on Empire Market for a price of USD 5,000 or around Rp 74 million. Once that leak was discovered, that information was leaked widely throughout multiple online forums, making it more probable that users would become a victim of other cyberattacks, such as credential stuffing, in which hackers use a set of leaked passwords and emails to take over other accounts of their victims across multiple platforms.

In response to this incident, Tokopedia confirmed that there was a hacking attempt and clarified that it has strengthened its security systems to prevent such in the future. The company also clarified that passwords of users are still secure in that they are in encrypted hashes form. Cyber security experts warn, however, that password hashes can be compromised via brute force attacks, more so when weak or default passwords

are used. Tokopedia then urges all users to reset their passwords immediately and to be security-aware of their personal data in the digital realm. With everything that has been done, this leak serves to remind that security in the cyber realm needs to be beefed up even more to prevent hacking of user data in the future.

III.2 Risks for Tokopedia and Users

a. Risks to Tokopedia

- Decline in Public Trust and Reputation

  Data leak cases decrease users' trust in security in Tokopedia, causing a likely decrease in the number of subscribers. Users would be able to switch to other e-commerce sites that appear more secure.

- Economic Risk

  Tokopedia invested a great amount of money in strengthening security in order to contend with this incident. Corporations also risk getting sued and issued fines by regulators.

- Enhanced Cyber Attack Vulnerability

  The success of such a hack would embolden other hackers to seek security gaps that have yet to be plugged. Unless acted on immediately, Tokopedia is open to successive instances of leaks of data.

- Legal Sanctions and Controls

  Tokopedia can be sanctioned if it is found to be in violation of rules of protection of data that apply in Indonesia. This incident also expedited the drafting of the Personal Data Protection Law (PDP Law).

b. Risks to Users

- Misuse of Personal Information for Cybercrime

The leaked information can be utilized to enable identity fraud, online fraud, or financial fraud. The users risk loss of money in case their details get misused.

- Social Engineering and Phishing Scams

  The leaked information can be utilized to send spam emails or messages that instruct users to give sensitive information. Scammed users risk loss of their account privileges or exposure to money fraud.

- Illicit Information Disclosure to Third Parties

  The leaked information can be sold in the dark web and utilized by other players to enable illicit marketing or mental manipulation. The users can start receiving excessive spam or suspicious phone calls.

- Illicit Access to Other Accounts

  Where users use one password to many platforms, other accounts like emails or mobile banking get compromised. This subjects them to chain hacking of their personal accounts.

- Financial Security Risks

  The stolen information can be utilized to obtain users' e-wallet or card account details. Once a hacker is in, money in a user's account can be stolen without their knowledge.

III.3 Handling Actions by Tokopedia

After the leak of 91 million users in 2020, various measures were undertaken by Tokopedia in response to it. The company's response was embraced in diverse ways across different segments of society, i.e., security professionals and regulators. The measures undertaken by Tokopedia in dealing with leaks of information and evaluating the effectiveness of such efforts are discussed herebelow:

1. An enhanced encryption and data security system

Tokopedia adds firewalls and intrusion detection systems, upgrades data encryption, and enhances password hashing techniques to fortify its security system. To improve user account security, they also employ two-factor authentication (2FA).

2. Encourage Users to Update Their Passwords

   Through in-app reminders, SMS, and email, Tokopedia encourages users to change their passwords right away. Additionally, they provide education on the value of creating distinct passwords in order to stop unwanted access to accounts with identical credentials.

3. Working together with the government and cybersecurity authorities

   Tokopedia is enhancing its security measures in compliance with GDPR and ISO 27001 while closely collaborating with BSSN and authorities to look into the breach. The goal of this action is to stop future occurrences of the same kind.

4. Public Communication and Transparency

   In response to this occurrence, Tokopedia released a formal declaration guaranteeing the security of transaction and financial data. To preserve confidence in their platform, they also provided clarification to the user base and the media.

III.4 Regulations Imposed on Tokopedia

Electronic system operators (PSEs) that failed to secure users' personal data were not subject to severe penalties under applicable legislation, such as the ITE Law, PP PSTE No. 71 of 2019, and Permenkominfo No. 20 of 2016, at the time of the 2020 data breach of 91 million Tokopedia accounts. Tokopedia is therefore immune from penalties and legal repercussions. The Personal Data Protection Law (PDP Law) No. 27 of 2022, which stipulates penalties for PSEs that fail to protect user data, including

fines of up to 2% of annual revenue and criminal penalties of up to 5 years or a fine of Rp 50 billion, was ratified more quickly as a result of this incident.

CHAPTER IV CONCLUSION AND SUGGESTIONS

IV.1 Conclusion

The story of the Tokopedia data breach emphasizes how crucial it is for e-commerce to protect personal information. This episode demonstrates the data protection system's shortcomings, both in terms of businesses and the legislation that were insufficiently strict at the time. A benefit of this occurrence, nevertheless, is that it has sped up the ratification of the 2022 PDP Law, which improves the protection of Indonesian citizens' personal information.

Both e-commerce businesses and customers need to be more proactive in protecting user data and be on the lookout for online dangers like identity theft and phishing. The future danger of data leaking can be reduced with the correct precautions.

IV.2 Suggestion

To strengthen personal data protection in e-commerce, platforms like Tokopedia must design their security infrastructure using multiple-layered encryption, advanced firewalls, intrusion detection systems, and multi-factor authentication (MFA) to restrict unauthorized entry. Education of users is also a crucial point, such as password security, phishing attacks, and settings of privacy. Law No. 27 of 2022 (PDP Law) demands strict regulation of data, regular security audits, punctual notification of breaches, and adherence to principles of minimization of data.

In cases of breaches of data, open crisis management is a necessity, such as instant disclosure, punctual updates, and potential redress to injured users. Aside from that, government-industry cooperation is also crucial, such that e-commerce platforms synchronize efforts with institutions of cybersecurity such as BSSN and Kominfo while adopting international security frameworks such as GDPR and ISO 27001. By adopting

such strategies, e-commerce companies can earn user trust, be compliant to regulation, and boost their cybersecurity resilience in the digital era.

BIBILIOGRAPHY

[1] Beer, S. (2024, September 12). *Top Strategies for Data Privacy and Protection in eCommerce*. CLARITY. https://www.clarity-ventures.com/ecommerce/strategies-data-privacy-protection-ecommerce

[2] CNNIndonesia. (2020, May 3). Kronologi Lengkap 91 Juta Akun Tokopedia Bocor dan Dijual. *Teknologi*. https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual

[3] Maharani, R., & Prakoso, A. L. (2024). Perlindungan data pribadi konsumen oleh penyelenggara sistem elektronik dalam transaksi digital. *JURNAL USM LAW REVIEW*, *7*(1), 333. https://doi.org/10.26623/julr.v7i1.8705

[4] Poeja Kehista, A. (2023, May 1). Analisis Keamanan Data Pribadi pada Pengguna E-Commerce: Ancaman, risiko, Strategi Kemanan (Literature Review). *Jurnal Ilmu Manajemen Terapan*. https://dinastirev.org/JIMT

[5] Rexy, & Rexy. (2023, December 30). Risiko Pelanggaran Privasi dan Cara Mitigasinya dengan ISO 27701 - IT Proxsis Group. *IT Proxsis Group - Just another WordPress site*. https://it.proxsisgroup.com/risiko-pelanggaran-privasi-dan-cara-mitigasinya-dengan-iso-27701/

[6] *UU No. 27 Tahun 2022*. (2022, October 17). Database Peraturan | JDIH BPK. https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022