

CHAPTER I

INTRODUCTION

1.1 Background

As humans living in a digital society, our personal data is prone to be exposed and extracted by unwanted organizations and individuals. Personal data is confidential information or personally identifiable information (PII)¹About information of an identifiable person.² Identifying an individual could be seen from a name, number, date of birth, and perhaps other attributes, for instance, an IP address or a cookie identifier.³ Therefore, there must be protection to secure our data from any dangerous exposures of privacy violation. By establishing personal data protection, it will preserve individuals' primordial rights and freedoms connected to such data—security of personal data guarantees that people's rights and freedoms are not breached. Hence, regulations and laws have been established to secure the rights of an individual's private information.

The right to privacy is assured under Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which states that "No one

¹ Stevens, Gina (10 April 2012). "[Data Security Breach Notification Laws](#)" (PDF). fas.org. Retrieved 8 June 2017

² Greene, Sari Stern (2014). *Security Program and Policies: Principles and Practices*. Indianapolis, IN, US: Pearson IT Certification. p. 349. ISBN 978-0-7897-5167-6. OCLC 897789345.

³ NIST Special Publication 800-122" (PDF). *nist.gov*.

shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation." Hence, every individual is entitled to be protected by the law against any interference. The ICCPR has a significant role in overcoming flaws in the interconnected systems of international frameworks dealing specifically with data protection.⁴

Other than international treaties, the protection of personal data is also regulated under the Indonesian 1945 Constitution. Constitutionally, the State protects the privacy and data of its citizens. Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia ("UUD 1945") asserts: "Everyone has the right to protection of himself, family, honor, dignity and property under his control, and to the right to feel safe and protection from the threat of fear which reflects an individual's human right." This provision implicitly unfolds the protection of an individual's data. Each individual has the right to privacy over their data, which includes the right to manage, edit, and delete an individual's personal data along with determining when, how, and for what purpose the data is communicated to other parties.

Having personal data stored in various technology devices will increase the chance of a data breach incident. A data breach is a phenomenon that has

⁴ Bygrave, Lee A. *Data Protection according to the Right to Privacy in Human Rights Treaties*, vol. 6, 1998, pp. 247–287.

occurred throughout the years, ever since the Internet has continuously evolved with its advanced developments suited to adjust any era of time. Touching upon the history of a data breach, it was first well-known in 2005.⁵ More than 1 million documents released by a DSW Shoe Warehouse company were exposed for a data breach. Diving more profound to the accident, 1.4 million credit card numbers and names were revealed on those accounts registered in DSW Shoe Warehouse.⁶ The incident was an eye-opening occurrence for businesses and organizations as according to Ayyagari⁷ Data breaches have been one of the biggest corporate challenges, which cost an average of \$7.2 million per data breach case.⁸

Hence, technology expansion gives businesses, governments, and individuals exposed to a data breach's danger and complications. Without a doubt, confidential information can potentially be extracted by unauthorized parties for abysmal intentions. For instance, identity theft, fraud purposes,⁹ Individuals obtain such valuable information for personal gain associated with

⁵ Silverman, David L. "Developments in Data Security Breach Liability." *The Business Lawyer*, vol. 72, no. 1, 2016, pp. 185–194. *JSTOR*, www.jstor.org/stable/26419115. Accessed 7 December 2020.

⁶ "1.4 Million Exposed in Shoe Data Breach." *NBCNews.com*, NBCUniversal News Group, 19 April. 2005, www.nbcnews.com/id/7550562/ns/technology_and_science-security/t/million-exposed-shoe-data-breach/#.XxrQxJMzaEs.

⁷ Ayyagari, R. (2012). An exploratory analysis of data breaches from 2005-2011: Trends and insights. *Journal of Information Privacy and Security*, 8(2), 33-56

⁸ *Ibid.*

⁹ Martin, Nicole. "What Is A Data Breach?" *Forbes*, *Forbes Magazine*, 25 February 2019, www.forbes.com/sites/nicolemartin1/2019/02/25/what-is-a-data-breach/#3e53a21d14bb.

national governments, organized crime, or political means.¹⁰ As mentioned previously, the whole concept of a data breach is a security violation by acquiring classified information of individuals. This crime category can be committed by obtaining financial information such as credit card or bank information, medical records, personal identification information, corporate trade secrets, or intellectual property information.¹¹ Most infringements of data include excessively exposed and insecure unstructured data, including confidential documents and records.¹²

A data breach is certainly a disaster for businesses, organizations, health care sectors, and many more. Many factors cause personal information to be exposed and stolen by unauthorized parties. Some of the major reasons for data breaches entail¹³

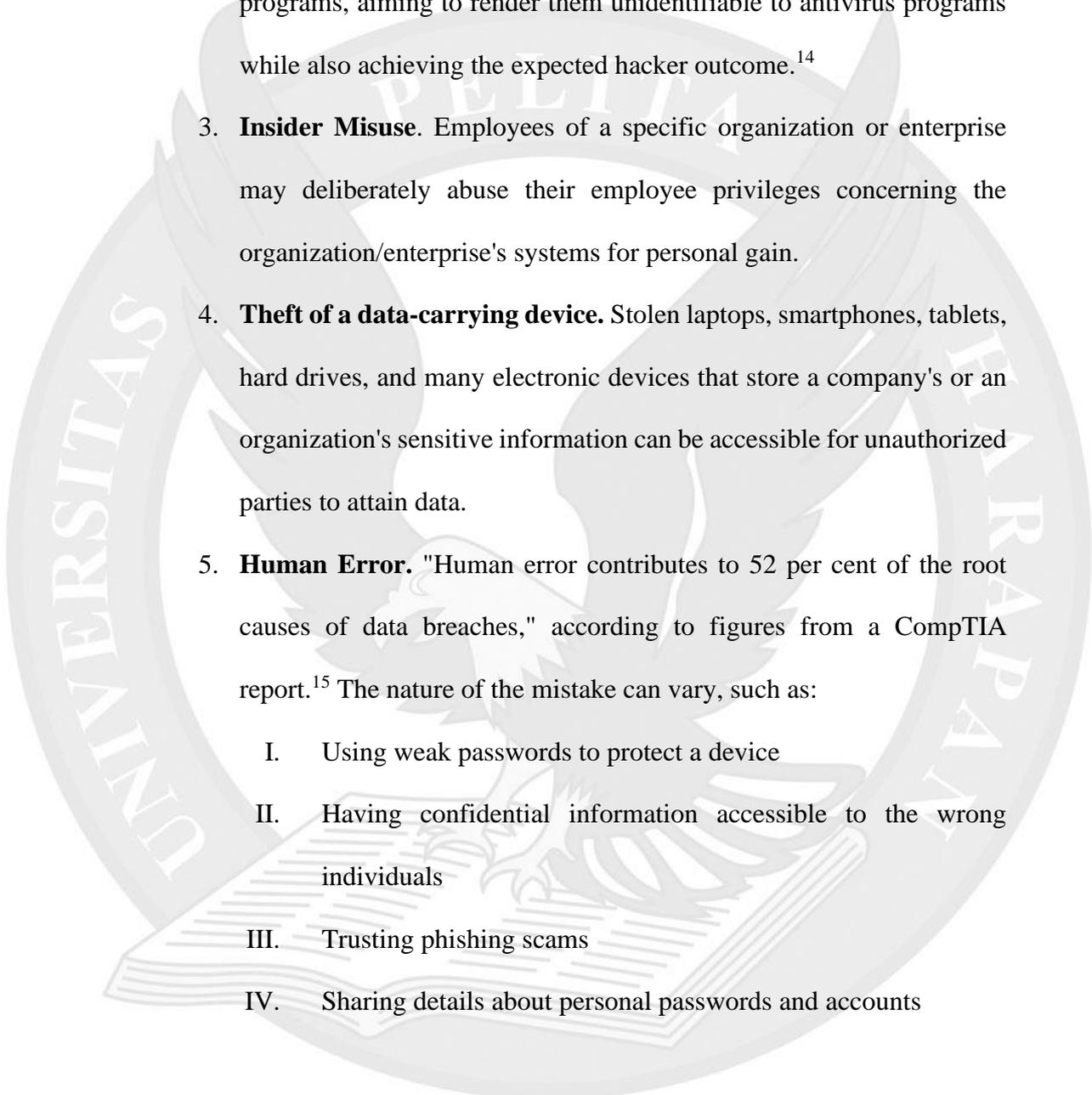
1. **Old and Unfixed Security Vulnerabilities.** Unpatched security may cause exploited vulnerabilities of a company/organization system. Thus, old securities vulnerabilities allow hackers to access a company or an organization's confidential information.

¹⁰ Skowronski, Lukasz, et al. "Internet Security: How Widespread Are Bad Development Habits?" *Security Boulevard*, 4 March. 2020, securityboulevard.com/2019/08/internet-security-how-widespread-are-bad-development-habits/.

¹¹ Kaspersky. "How Data Breaches Happen: What They Are and Why It Matters." *Www.kaspersky.com*, 16 July 2020, www.kaspersky.com/resource-center/definitions/data-breach.

¹² "Panama Papers Leak: The New Normal?". *Xconomy*. 2016-04-26.

¹³ WHOA.com. "Data Breach 101: Top 5 Reasons It Happens." *WHOA.com*, 26 Oct. 2018, www.whoa.com/data-breach-101-top-5-reasons-it-happens/.

- 
2. **Malware.** Hackers can make slight adjustments to existing malware programs, aiming to render them unidentifiable to antivirus programs while also achieving the expected hacker outcome.¹⁴
 3. **Insider Misuse.** Employees of a specific organization or enterprise may deliberately abuse their employee privileges concerning the organization/enterprise's systems for personal gain.
 4. **Theft of a data-carrying device.** Stolen laptops, smartphones, tablets, hard drives, and many electronic devices that store a company's or an organization's sensitive information can be accessible for unauthorized parties to attain data.
 5. **Human Error.** "Human error contributes to 52 per cent of the root causes of data breaches," according to figures from a CompTIA report.¹⁵ The nature of the mistake can vary, such as:
 - I. Using weak passwords to protect a device
 - II. Having confidential information accessible to the wrong individuals
 - III. Trusting phishing scams
 - IV. Sharing details about personal passwords and accounts

¹⁴ Calyptix. "Verizon Data Breach Report 2015: Top 10 Charts and Summary." Calyptix Security, 7 June 2017, www.calyptix.com/research-2/verizon-data-breach-report-2015-top-10-charts-and-summary/.

¹⁵ Maurer, Roy. "Human Error Cited as Top Cause of Data Breaches." SHRM, 16 August 2019, www.shrm.org/ResourcesAndTools/hr-topics/risk-management/Pages/Human-Error-Top-Cause-Data-Breaches.aspx.

According to Hacker-Powered Security Report 2019, data breaches in retail and e-commerce platforms are frequently occurring, as more than two-thirds of all businesses view data breaches as their main security concern.¹⁶ Since many individuals, enterprises, and organizations worldwide have been affected by a data breach attack, Indonesia has also experienced an awful experience.

Recently, an Indonesian owned technology company specializing in e-commerce, named "Tokopedia" encountered a data breach attack in March 2020.¹⁷ The data breach has jeopardized more than 15 million users registered in Tokopedia,¹⁸ Which included records compromising names of Tokopedia accounts, password hashes, and email addresses. Unfortunately, many names of Tokopedia users were being put for sale on the dark web forum, worth USD 5,000.¹⁹

The neoteric event of Tokopedia left many of its consumers feeling uncertain over their legal rights regarding the compensation they are entitled to receive. Law Number 8 of 1999 explicitly requires that the business actors must

¹⁶ "The Hacker-Powered Security Report 2019." HackerOne, 3 Dec. 2019, www.hackerone.com/resources/reporting/the-hacker-powered-security-report-2019.

¹⁷ The Jakarta Post. "Tokopedia Data Breach Exposes Vulnerability of Personal Data." The Jakarta Post, www.thejakartapost.com/news/2020/05/04/tokopedia-data-breach-exposes-vulnerability-of-personal-data.html.

¹⁸ Fachriansyah, Rizky. "Data Breach Jeopardizes More than 15 Million Tokopedia Users, Report Finds." *The Jakarta Post*, 2020, www.thejakartapost.com/news/2020/05/03/data-breach-jeopardizes-more-than-15-million-tokopedia-users-report-finds.html.

¹⁹ Ibid.

protect their consumer's personal data. Under the Government Regulation (PP) No. 71/2019, oblige Tokopedia as a digital platform and data holder to inform its consumers, particularly those whose data are breached without delay. As article 14(5) of the Government Regulation stipulates, *“If there is a failure in protecting data of its consumers, the System Provider Electronics must notify in writing to the owner of the Personal Data.”*²⁰ Also, Regulation No 20/2016 of the Minister of Communication and Information provides for a 14-day notification period,²¹ while the Personal Data Protection Bill would demand that this be achieved within three days.²² Yet, Tokopedia failed to inform its consumers during the event of the data breach, as they only released a mere statement 2 months after the accident occurred. The message was sent to consumers of Tokopedia, entailing that account holders of Tokopedia, such as their security and financial information are secure.²³

With that said, Tokopedia has not responded regarding the legality of the incident and its obligation to compensate the damages towards their consumers. In this case, laws and regulations that can be enforced have yet to be implemented by Tokopedia and the Indonesian legal system. Therefore,

²⁰ Article 14(5) of Government Regulation No.71/2019

²¹ Article 28(C)(4) of Ministerial Regulation No.20 of 2016 concerning Personal Data Protection in Electronic Systems

²² Fachriansyah, Rizky. "Data Breach Jeopardizes More than 15 Million Tokopedia Users, Report Finds." The Jakarta Post, 2020, www.thejakartapost.com/news/2020/05/03/data-breach-jeopardizes-more-than-15-million-tokopedia-users-report-finds.html.

²³ Pratomo, Yudha. "Sidang Perdana Kasus Kebocoran Data Tokopedia Digelar Hari Ini Halaman All." *KOMPAS.com*, Kompas.com, 10 June 2020, tekno.kompas.com/read/2020/06/10/09144017/sidang-perdana-kasus-kebocoran-data-tokopedia-digelar-hari-ini?page=all.

there must be clarity within the law. Coherence within the legal system will initiate a concrete solution to solve ongoing disputes between Tokopedia and its consumers.

Hence, this thesis analyzes and emphasizes the importance of implementing the consumer's data protection under Law No.8 of 1999 concerning Consumer Protection. This thesis elaborates on the concept of *Strict Liability* related to personal data protection. Subsequently, this thesis aims to provide recommendations that will secure the rights that the consumers have lost during the process of the uncertain legal enforcement of handling the dispute.

1.2 Formulation of Issues

Embarking from the previous descriptions, this thesis will discuss and analyze the following formulation of issues:

1. How and to what extent can the Tokopedia consumers demand compensation due to the personal data breach, under the *Strict Liability* principle in reference to Indonesian Consumer Protection Law?
2. What are the measures that the Indonesian government can undertake to protect the consumer's rights on personal data protection based on the International and Regional Treaties?

1.3 Research Purpose

The purpose of writing this thesis is to answer the aforementioned formulation of issues, which entails:

1. Finding a resolution to legally protect Tokopedia's consumers over the loss they have suffered due to their personal data being exposed. By doing so, there must be an analytical study of the Tokopedia data breach case, with referencing the *Strict Liability* concept under the Indonesian Consumer Protection Law, and how consumers can be compensated over the damages that they have suffered.
2. Analyze International and Regional Treaties regarding consumer's rights on personal data protection and how the Indonesian government can find a solution to solve the undertaking issues of Tokopedia's data breach.

1.4 Research Benefits

1.4.1 Theoretical Benefits

The aim of this thesis is to give a theoretical understanding of the legal certainty regarding the concept of strict liability, in which the consumers of Tokopedia are entitled for, based on Law No.8 of 1999 concerning Consumer Protection. Therefore, the Author would determine the various regulations and laws that allow consumers to be able to secure their rights for compensation, as well as legal protection against data breaches that occur in E-commerce. As such, readers can obtain knowledge of the Indonesian legal system and what aspects does the law thereof lack. Moreover, International and Regional

Treaties concerning consumer protection will be analyzed in order to implement the standards of rights that consumers are entitled to receive.

1.4.2 Practical Benefits

For practical benefits, the Author hopes that this thesis and the formulated issues will become an advantage for the Indonesian legal system. Hence, this thesis will provide solutions for the Indonesian government and court to implement in its laws and regulations, specifically their Consumer Protection Law of Law No.8 of 1999. Moreover, the author suggests that the Indonesian government establishes a coherent regulation that can be feasible for consumers to attain their legality regarding the rights to be protected and compensated over data breach occurrences. As a result, consumer's rights will be enforced by the Indonesian Legal system, with equality, justice and fairness.

1.5 Framework of Writing

This thesis consists of five main chapters that will aid the readers to gain an understanding of the issue at stake within this topic.

CHAPTER I: INTRODUCTION

In this section of the thesis, it will mainly contain the introduction of the topic, which is divided into five subtopics, such as:

1. Background
2. Research of Question

3. Research Purpose
4. Research Benefits
5. Structure of Writing

CHAPTER II: LITERATURE REVIEW

In this chapter, the Author will categorize this chapter into 2 topics, in which the first part consists of 3 subtopics incorporating:

1. Protection of Private Data as Fundamental Rights
2. History of Consumer Protection in Indonesia
3. Strict Liability within Consumer Protection Framework

The second part of this chapter, will further provide a detailed description of concepts concerning Consumer Protection, such as:

1. The broad definition of Consumer protection, and how the topic is perceived in the Indonesian legal system.
2. The definition of Consumer Protection
3. Legal structure of Consumer Protection
4. The meaning of Consumer
5. The scope of Business Actor
6. Laws and Regulations protecting consumer's rights towards data breaches
7. The scope of *Strict Liability*
8. Elements of Compensation

9. The theory of Data Breach

CHAPTER III: RESEARCH METHODS

This chapter discusses the variety of research methods that are utilized to formulate this thesis. Such methods are the type of data, data analysis technique, and the type of approach to research this thesis.

CHAPTER IV: DISCUSSION AND ANALYSIS

The fourth chapter will discuss the research issues as well as the solutions to such matters. Therefore, this chapter will answer the respective research question that has been affirmed in chapter two of this thesis. Hence, chapter four will be divided into two sub-chapters to analyze and elaborate on the issues stipulated in this thesis. Subsequently, the first chapter will examine regulations and policies established by the Indonesian government regarding consumer protection, specifically consumer's rights over data breaches. Also, the second chapter evaluates the legal certainty of consumers, in regard to the *Strict Liability* concept, and whether or not it is stipulated and enforced under the Indonesian legal system.

CHAPTER V: CLOSING

In this last chapter, the author will conclude this thesis by answering the issues stipulated in the previous chapters. The author will explain the conclusion in depth by formulating solutions and recommendations

regarding the complications that are faced within the law. Therefore, such constructive insights can be implemented for the legal certainty of consumers that experienced data breach due to Tokopedia's negligence protecting its securities in regard to maintaining sensitive information to be confidential. Thus, consumers who suffered damages from the data breach will be able to attain clarity and compensation over the incident.

