

# CHAPTER I

## INTRODUCTION

### 1.1 Background of the Issue

The economic growth of a state, although not solely depending on one sector, is highly influenced by the growth of businesses. Businesses bring about not only profits, but also attract investors into investing their money in the country. As such, there is a push towards growing the business sector. Especially, in this era of globalization where technology is becoming more and more advanced, the business sector has grown to the area of electronic commerce, or what is better known as e-commerce.

Electronic commerce [“E-commerce”] refers to the business activity of buying and selling goods and/or services on the internet.<sup>1</sup> E-commerce market in Indonesia is growing significantly over the past decade, growing over 60-70 per cent annually from 2014 to 2018.<sup>2</sup> There are several factors that have roles in achieving this level of growth, including the increase of smartphone usage and internet penetration, increase of foreign direct investment in the e-commerce market, *e.g.*, Tokopedia, Go-Jek, Traveloka, Bukalapak, amongst others.<sup>3</sup>

---

<sup>1</sup> Cambridge Dictionary, “E-commerce”, <<https://dictionary.cambridge.org/dictionary/english/e-commerce>> accessed in August 6, 2020.

<sup>2</sup> Macquarie Research, “Online retail as a percentage of total sales”, Euromonitor, Statista, Macquarie Research, 12 April 2017, p.1, <[https://www.macquarieresearch.com/rp/d/r/publication.do?f=C&pub\\_id=7318216&file\\_name=IndonesiaEcommerce120417Re270473.pdf](https://www.macquarieresearch.com/rp/d/r/publication.do?f=C&pub_id=7318216&file_name=IndonesiaEcommerce120417Re270473.pdf)> accessed in August 6, 2020.

<sup>3</sup> Australian Trade and Investment Commission, “E-commerce in Indonesia: A guide for Australian business”, *Report*, Australia: Australian Trade and Investment Commission, January 2018, p.4; Reuters, “SoftBank leads \$100 million investment in Indonesian ecommerce firm Tokopedia”, 22 October 2014,

Moreover, the recent implementation of various online payment or e-transaction platforms also helped in ensuring the growth of the e-commerce market.<sup>4</sup>

The Capital Investment Coordinating Board [“BKPM”] reported that Indonesia’s e-commerce market has received around US\$2.5 billion to US\$3 billion over the last few years,<sup>5</sup> which amounts to 15 to 20 per cent of the total foreign investment to Indonesia.<sup>6</sup> Moreover, Indonesia reportedly have over 18 millions of online shoppers in 2015, which according to Google and Temasek is expected to grow to 119 million by the year of 2025.<sup>7</sup> Google and Temasek also predicted in 2018 that the value of e-commerce market in Indonesia amounts to US\$23.2 billion.<sup>8</sup> Especially, in the time of COVID-19 pandemic such as now, people are opting for online shopping as it does not require human-to-human contact. Hence, e-commerce becomes an essential need for people in order for them to fulfil their needs.

Considering the growth of the market as shown above, investing in e-commerce businesses in Indonesia should be highly desired by investors. However,

---

< <https://www.reuters.com/article/uk-tokopedia-%20softbank-indonesia/softbank-leads-100-million-investment-in-indonesian-e-commerce-firm-tokopedia-idUKKCN0IB0L920141022>> accessed in August 6, 2020; TechCrunch, “Alibaba leads \$1.1B investment in Indonesia-based e-commerce firm Tokopedia”, 17 August 2017, <<https://techcrunch.com/2017/08/17/alibaba-tokopedia/>> accessed in August 6, 2020.

<sup>4</sup> Australian Trade and Investment Commission, “E-commerce in Indonesia: A guide for Australian business”, *Report*, Australia: Australian Trade and Investment Commission, January 2018, p.4.

<sup>5</sup> Australian Trade and Investment Commission, “E-commerce in Indonesia: A guide for Australian business”, *Report*, Australia: Australian Trade and Investment Commission, January 2018, p.4.

<sup>6</sup> Rio Tuasikal, “Investasi Asing untuk E-Commerce, Perlukah Khawatir?”, 2 March 2019, <<https://www.voaindonesia.com/a/investasi-asing-untuk-e-commerce-perlukah-khawatir-4809616.html>> accessed on August 5, 2020.

<sup>7</sup> Google and Temasek, “E-conomy SEA: Unlocking the \$200 billion Digital Opportunity in Southeast Asia”, May 2016, p.10, <<http://apac.thinkwithgoogle.com/research-studies/e-conomy-sea-unlocking-200b-digital-opportunity.html>> accessed in August 5, 2020.

<sup>8</sup> Rio Tuasikal, “Investasi Asing untuk E-Commerce, Perlukah Khawatir?”, 2 March 2019, <<https://www.voaindonesia.com/a/investasi-asing-untuk-e-commerce-perlukah-khawatir-4809616.html>> accessed on August 5, 2020.

the market growth is not the only thing they must consider. The regulatory framework for e-commerce is one of the most crucial points to consider, and with that comes several legal issues. One of said issues that must be addressed for the e-commerce market to continue as strong, is the consumer protection issue that e-commerce as a business relying heavily on the internet or online database entails, along with the easiness and simplicity of such.

In the course of purchasing products and/or services from e-commerce platforms, consumers would have to register their personal data into said database and consequently, it requires trust from the consumers towards the security or safety of the platforms. This is why a definite regulation on consumer protection is crucial for the growth of e-commerce, as they rely heavily on attracting consumers to use the e-commerce platforms. However, the reality is that e-commerce platforms may be prone to hacking, and thus puts the personal data of consumers at risk of being spread.<sup>9</sup>

One of the most recent cases of data breach in e-commerce sector is with regard to the Tokopedia data breach that occurred on March 2020.<sup>10</sup> Subsequently, the massive data of 91 million Tokopedia users were allegedly being spread online through a link shared in a Facebook group, according to the Communication and Information System Security Research Center (CISSReC).<sup>11</sup> Despite such,

---

<sup>9</sup> Tirta Citradi, “Data Pengguna E-Commerce Bocor, Ini Bukti RI Rawan Cybercrime”, 6 July 2020, <<https://www.cnbcindonesia.com/tech/20200706140435-37-170521/data-pengguna-e-commerce-bocor-ini-bukti-ri-rawan-cybercrime>> accessed in September 21, 2020.

<sup>10</sup> Eisy A. Eloksari, “Personal data at risk as e-commerce booms”, 5 May 2020, The Jakarta Post, <<https://www.thejakartapost.com/news/2020/05/05/personal-data-risk-e-commerce-booms.html>> accessed in August 6, 2020.

<sup>11</sup> Eisy A. Eloksari, “Tokopedia data breach exposes vulnerability of personal data”, 5 May 2020, The Jakarta Post, <<https://www.thejakartapost.com/news/2020/05/04/tokopedia-data-breach-exposes-vulnerability-of-personal-data.html>> accessed in August 6, 2020; Tempo, “Tokopedia files

Tokopedia claimed that its users' passwords, financial information as well as transaction history remained secure.<sup>12</sup> The culprit of this data leak has not been caught as of yet as it is difficult to pinpoint exactly where the leak may have come from, especially considering that the internal database of a company as large as Tokopedia may be easily accessible to a lot of employees. Moreover, the reliance on a third-party company for products or services in integrating their systems exposes the company to more risks of such leaks. According to a cybersecurity research collective named Under the Breach, hackers would usually utilize this fact to find access to the company's systems through the employees in the form of phishing e-mails.<sup>13</sup>

While the illegal data leak is attributable to a yet-unidentified third party, Tokopedia as the platform provider still has its own obligations to dispense. In particular, they must coordinate with the government and stakeholders in this case regarding the data theft.<sup>14</sup> This entails their obligation to act in accordance with relevant laws and regulations, namely the Government Regulation Number 71 Year 2019 on Electronic Systems and Transactions [**“Government Regulation 71/2019”**] as well as the Communication and Information Ministerial Regulation Number 20 Year 2016 [**“PERMENKOMINFO No. 20/2016”**] in this instance.

---

police report over alleged data breach,” <<https://en.tempo.co/read/1361807/tokopedia-files-police-report-over-alleged-data-breach>> accessed in September 21, 2020.

<sup>12</sup> Tempo, “Government Responds to Alleged Tokopedia Data Breach”, <<https://en.tempo.co/read/1338407/government-responds-to-alleged-tokopedia-data-breach>> accessed in September 21, 2020.

<sup>13</sup> Eisy A. Eloksari, “Tokopedia data breach exposes vulnerability of personal data”, 5 May 2020, The Jakarta Post, <<https://www.thejakartapost.com/news/2020/05/04/tokopedia-data-breach-exposes-vulnerability-of-personal-data.html>> accessed in August 6, 2020

<sup>14</sup> Tempo, “Tokopedia files police report over alleged data breach,” <<https://en.tempo.co/read/1361807/tokopedia-files-police-report-over-alleged-data-breach>> accessed in September 21, 2020.

Further, the Minister of Communication and Informatics, Mr. Johnny G. Plate also specifically asked Tokopedia to conduct three main measures in order to ensure the safety of users' personal data: (1) to immediately secure the system to prevent further data breach; (2) to let the users know about the possibility that their personal data have been exposed; and (3) to conduct an internal investigation to confirm whether allegation of data breach is indeed true, and if it is, to investigate on the cause of such.<sup>15</sup>

Prior to this, there have also been other cases of data breach, *e.g.*, to Bukalapak in 2015, or to Go-jek in 2016, amongst others, which are also left unsolved.<sup>16</sup> These unsolved cases, in which the affected consumers may not be getting any form of remuneration, and some might not even be aware of the infringement to their right, show the lack of certainty in the responsibility mechanism for cases of personal data infringement, and becomes an eye-opener for consumers of the high risk of their personal data on online platforms being misused and for them to be more alert in giving their personal data into e-commerce systems.

This in turn, birthed fear towards possible misuse of their personal data already within the e-commerce system and might as well make people more reluctant in becoming customers of e-commerce businesses. Therefore, there is an

---

<sup>15</sup> CNBC Indonesia, "Hari ini Tokopedia Jelaskan Kebocoran 91 Juta Data ke Kominfo", May 2020, <<https://www.cnbcindonesia.com/tech/20200504083624-37-155959/hari-ini-tokopedia-jelaskan-kebocoran-91-juta-data-ke-kominfo>> accessed in September 19, 2020.

<sup>16</sup> Wahyu T. Rahmawati, "Data Tokopedia, Gojek, dan Bukalapak bocor saat RUU perlindungan data pribadi absen", 5 May 2020, Kompas.com, <<https://industri.kontan.co.id/news/data-tokopedia-gojek-dan-bukalapak-bocor-saat-ruu-perlindungan-data-pribadi-absen>> accessed in September 21, 2020.

urgent need to address this matter and properly ensure the public whether the existing law and regulation can effectively protect the consumers against the losses that may occur due to possible data theft through e-commerce platforms, especially considering that e-commerce has become an essential need in the current pandemic situation where direct contact is preferably avoided.

The relevant applicable law with regard to the existence of consumers' right over their personal data is derived from the 1945 Constitution and the Law Number 8 of 1999 concerning Consumer Protection [**"Consumer Protection Law"**]. Article 28 point E and G of the 1945 Constitution sets forth the fundamental human right over their personal data and their right to control the use of said data.<sup>17</sup> Meanwhile, consumer protection as stipulated under Article 1(1) of the Consumer Protection Law refers to all means which guarantee the legal security to protect the consumers.<sup>18</sup> In this sense, consumer protection is used to define any measures that aim to protect and promote the consumers' well-being and/or financial interests. Such measures are taken in order to ensure that consumers will be able to make well-informed decisions regarding their choices to purchase or buy products and/or services, and that producers and sellers will have the obligation to fulfill their promises about the products and services they offer in accordance with the consumers' expectation from earlier representations.

---

<sup>17</sup> Article 28E, 28G, the 1945 Constitution.

<sup>18</sup> Article 1(1), Law Number 8 of 1999 concerning Consumer Protection [**"Consumer Protection Law"**].

Moreover, in relation to the protection of personal electronic data, the relevant regulation is Law Number 11 of 2008 concerning Electronic Information and Transactions [“**EIT Law**”], as well as Law Number 19 of 2016 on the Amendment to Law Number 11 of 2008 Regarding Electronic Information and Transactions [“**AEIT Law**”]. Article 26(1) of the AEIT Law asserts that unless otherwise stipulated by other regulations, the usage of any information through electronic media relating to a person’s personal data must be made with the consent of the person concerned.<sup>19</sup> Thus, in the event that a person’s personal data is used without their consent, said person may file a suit for the losses caused due to such. Article 30 and 32 of the EIT Law also prohibit the act of illegal accessing of an Electronic System and the act of illegal data interference, respectively.<sup>20</sup>

Another regulation that may be relevant to this matter is the Government Regulation 71/2019, which requires digital platform and data holder to notify users or consumers whose data were breached.<sup>21</sup> The PERMENKOMINFO No. 20/2016 allows them to have a period of 14 days to notify the users,<sup>22</sup> meanwhile the Personal Data Protection Bill [“**PDP Bill**”] that is currently still being discussed only allows a shorter period for notification, and require it to be done within just three days. Despite this, there are still questions as to the procedure in handling personal data theft cases, the obligation of e-commerce businesses and the extent of their responsibility in cases of personal data theft through their platforms or

---

<sup>19</sup> Article 26(1), Law Number 19 of 2016 on the Amendments to the EIT Law [“**AEIT Law**”].

<sup>20</sup> Article 30, 32, Law Number 11 of 2008 concerning Information and Electronic Transactions [“**EIT Law**”].

<sup>21</sup> Government Regulation Number 71 of 2019 [“**Government Regulation 71/2019**”].

<sup>22</sup> Communication and Information Ministerial Regulation Number 20 of 2016.

systems, as well as the legal remedies that may be sought by the victims in such cases.

Based on the elucidation above, therefore the Author gave this Thesis the title: “Juridical Analysis on Consumer Protection Against Personal Data Theft from E-Commerce Platforms in Indonesia”.

## **1.2 Formulation of Issues**

Based on the information that was previously mentioned as the basis for the background, the Author suggests the following legal issues that will be discussed below:

1. What are the available legal remedies in Indonesia that victims of personal data theft from e-commerce platforms can resort to?
2. What is the extent of the obligation of e-commerce platform providers in relation to the protection of personal data and in cases of personal data theft through their platforms?

## **1.3 Research Purpose**

Based on the issues formulated above, therefore this Thesis aims to:

1. Determine the available legal remedies for victims of personal data theft from the e-commerce platforms under Indonesian Law.

2. Determine the extent of the obligation of e-commerce platform providers in relation to the protection of personal data and in cases of personal data theft through their platforms.

## **1.4 Benefits of Research**

### **1.4.1 Theoretical Benefits**

The result of this writing is expected to be a contribution to the development of legal studies and to be used as material knowledge, specifically in the area of protection of consumers' right to privacy in relation to their data stored in e-commerce platforms against the possibility of data theft. It will focus on the importance of the protection of consumers regarding their data that is held by e-commerce businesses in the course of business activity or being a consumer of said businesses. It will also talk about how e-commerce businesses may be prone to data theft and its implication towards the safety of consumers' data.

The research will explore more on how Indonesian Law regulates the procedures taken in the occurrence of personal data theft, and substantive aspects of it, including the articles in the relevant laws and regulations that may be deemed violated in such cases, either by the data thief or the e-commerce platform storing its users' personal data in their system, as well as the legal remedies that the victims may pursue to compensate for the damages suffered in that case. Moreover, this Thesis will also explore on the recommendations for the possible actions the government can take in order to further secure e-commerce consumers' right over their personal data in this regard.

### **1.4.2 Practical Benefits**

The result of this writing is expected to provide input and contribute thoughts for legal practitioners, especially in relation to cases of consumers' personal data theft from e-commerce platforms in Indonesia. Therefore, the Author hopes that with this analysis and report, not only the law scholars and those who are interested in consumer protection, particularly in relation to consumers' data safety, but also general audiences will be able to learn and understand the importance of clear legal protection for consumers' personal data and raise awareness on this matter, especially since e-commerce businesses are currently booming. With this, the Author also hopes that the general public will have knowledge about their own rights over their personal data, as well as the steps that they can take in the event that data theft occurred to them, for the purpose of getting an appropriate and adequate remedy for the infringement of their right.

## **1.5 Structure of Writing**

### **CHAPTER I: INTRODUCTION**

The first chapter, which is the introduction, talks about the background of the Thesis topic, research question that the research will address, the purpose of the research and the significance of the research.

### **CHAPTER II: LITERATURE REVIEW**

The second chapter is the theoretical and conceptual frameworks that are the foundation for this Thesis' research. It also includes in-depth elaboration regarding the protection accorded to consumers in the course of engaging in a business activity or purchasing certain goods and/or services, the extent of the rights accorded to consumers as well as the respective obligations on the part of the entrepreneur or company, and all relevant laws and regulations with regard to the protection of consumers' personal data stored in e-commerce platform, procedures of filing criminal and civil claims relating to personal data theft, as well as cases that serve as precedents that are integral in understanding this research. These are so that there is no expansion of meaning or distortion in the writing of this Thesis.

### **CHAPTER III: RESEARCH METHODOLOGY**

The third chapter, which is the methodology, explains the research approach, research method, data collection technique, and data analysis technique used in gathering data and information for the research. It will also cover the object of the research, legal materials, both primary and secondary, and non-legal materials that support the discussion of legal issues, as well as the obstacles experienced during the research.

### **CHAPTER IV: ANALYSIS**

The fourth chapter, which is the analysis, is the peak of the Thesis and analysis. This chapter analyzes and presents all the data gathered regarding the research issues as well as the solution that is based on legal principles, applicable

laws and regulations, as well as previous court decisions. The result of the analysis can be used to address the research question of the Thesis or the legal issues that are the focus of this Thesis.

## **CHAPTER V: CONCLUSION AND RECOMMENDATIONS**

The fifth chapter, which is the conclusion and recommendation, summarizes the analysis of the previous chapters with regard to the result of the research on the legal issues. The chapter will also point out recommendations for the means available to victims of personal data theft from e-commerce platforms that the Author believes are the most effective in order to obtain adequate remedies as well as future normative legal studies which gives prescriptions on what should be the norms regulating on the matter in the future.

