

# CHAPTER I

## INTRODUCTION

### A. Context of Study

The development of information technology and the internet has brought many benefits to society and the business world in Indonesia. However, along with technological advances, various risks arise related to the security of users' Personal Data. The phenomenon of Personal Data leakage is a serious concern because it can threaten individual privacy and security. Many incidents of Personal Data leakage have occurred in companies and institutions in Indonesia, which indicates the need for in-depth research on the responsibilities of companies and related agencies for leaking the Personal Data of their users.

In 2008, Indonesia passed Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law). The ITE Law provides the first legal framework governing the protection of electronic data, including user's Personal Data in Indonesia.<sup>1</sup> However, regulated by law or not, Personal Data leaks do still happen. That begs for the question to be asked: How much do the companies and institutions that we trust understand their role in the safekeeping of the Personal Data of their clients in accordance with the laws in place?

---

<sup>1</sup>Law Number 1 of 2024 concerning Amendment to Law Number 11 of 2008 on Electronic Information and Transactions, Articles 26, 27, and 36.

Subsequently, the development of the digital world has presented new challenges to the use of Personal Data. Many companies and agencies in Indonesia collect, store, and process Personal Data of their users for various purposes, including marketing and behavioral analysis. The existence of data protection laws, such as Law Number 11 of 2008 and its amendment Law Number 19 of 2016 and its further amendment Law Number 1 of 2024 concerning Electronic Information and Transactions and Regulation of the Minister of Communication and Informatics Number 20 of 2016 concerning the Protection of Personal Data in Electronic Systems, states in sequential order and very explicitly that;

“... use of any information through electronic media concerning Personal Data of a person must be done with the consent of the Person concerned.”<sup>2</sup>

“Personal Data is confidential according to the Agreement and/or based on regulatory provisions legislation.”<sup>3</sup>

Consequently, it is giving a clear obligation for determining corporate responsibility and related agencies for the safekeeping and protection of the Personal Data of their users.

However, in recent years, there have been a number of important cases highlighting the lack of corporate and related agencies to hold accountable for Personal Data leaks. In March 2020, a data leak on one of the largest e-commerce websites in Indonesia, namely PT Tokopedia (hereinafter referred to as ‘Tokopedia’) revealed that users Personal Data had been sold on internet

---

<sup>2</sup> *Ibid.*, Articles 26.

<sup>3</sup> *Ibid.*, Articles 2.

forums. The leaked data covers more than 91 million user accounts and includes information such as names, addresses, phone numbers, and email addresses<sup>4</sup>. Then, in the same year in May, 'Bhinneka', also an e-commerce site in Indonesia, experienced a data leak involving 1.2 million user accounts. Data stranded on the internet, like the Tokopedia case, contains personal information such as names, addresses, telephone numbers, and email addresses<sup>5</sup>. Even worse, the Health Social Security Administering Body (BPJS Kesehatan), as a State-Owned Enterprise (BUMN), also experienced a data leak in March 2023. 18.5 million BPJS user data sold on dark forums for IDR 153 million. In a post on BreachForums in March, cybercriminal Bjorka leaked 19.5 million data under the name 'BPJS Ketenagakerjaan Indonesia 19 Million'. Bjorka then also distributed 100,000 samples containing Family Identification Number (NIK), full name, date of birth, address, cellphone number, email address, type of job, and company name<sup>6</sup>. These cases included cyberattacks against large companies that resulted in the leaking of millions of users' Personal Data.

The impact of this Personal Data leak does not only affect the affected individual but can also cause financial loss and reputational damage for companies or agencies that are unable to maintain data security properly.

---

<sup>4</sup> Eloksari, E. A., "Tokopedia data breach exposes vulnerability of personal data," *The Jakarta Post*, May 5, 2020, <https://www.thejakartapost.com/news/2020/05/04/tokopedia-data-breach-exposes-vulnerability-of-personal-data.html> Accessed 21 July 2025.

<sup>5</sup> Franedy, R., "1,2 juta data pengguna dikabarkan bocor, Bhinneka minta maaf," *CNBC Indonesia*, May 12, 2020, <https://www.cnbcindonesia.com/tech/20200512164725-37-157971/12-juta-data-pengguna-dikabarkan-bocor-bhinneka-minta-maaf> Accessed 21 July 2025.

<sup>6</sup> Purnamasari, D. D., "BPJS Ketenagakerjaan Investigasi Klaim Bjorka," *Kompas*, 14 April 2023, <https://www.kompas.id/baca/polhuk/2023/03/14/bpjs-ketenagakerjaan-investigasi-klaim-bjorka> Accessed 21 July 2025.

However, in reality, it is seldom the case; only the user as an individual is affected by this. The case of Bhinneka, where 1.2 million user's data leaked, received no further action at all, be it administrative sanctions in the form of fines or termination of service. Meanwhile, in the data leak case, which is being followed up on, Tokopedia has instead positioned itself as a victim of the leak of its 91 million users' data and declared itself free from all administrative and criminal charges.<sup>7</sup> Even worse, both of these cases don't mention any attempts to compensate users whose data has been leaked.

For that reason, the Personal Data Protection Law Number 27 of 2022 was formed to answer the need for more centralized and comprehensive arrangements related to Personal Data protection. Previously, regulations regarding Personal Data were spread across various sectoral laws and regulations, which caused legal protection of Personal Data to be less than optimal. With the presence of this law, the management and protection of Personal Data in Indonesia have become more organized, so that it can provide more effective and comprehensive legal protection.

Therefore, this study aims to analyze the extent to which companies and related agencies understand and implement what are their liabilities and responsibilities in the leakage of users' Personal Data. This research will use a normative legal approach by analyzing various laws that apply in Indonesia related to the protection of Personal Data, including the ITE Law, PDP Law,

---

<sup>7</sup> Decision of the Central Jakarta District Court Number 235/PDT.G/2020/PN.JKT.PST, Year 2020.

and its derivative regulations. The results of this study are expected to provide recommendations for related companies and agencies to improve security measures to protect users' Personal Data and encourage awareness of responsibilities and their liabilities in managing Personal Data in this digital era.

## **B. Problem Formulation**

Based on the description above, several problems can be formulated by the author:

1. What are the civil liabilities and responsibilities of corporations and related agencies regarding their user's data leakage?
2. What legal remedy that users can take if their Personal Data has been leaked?

## **C. Research Objective**

The objectives to be achieved by the authors in this study are:

1. To find out what are the civil liabilities and responsibilities of companies and the prospective personal data protection authority in Indonesia for the leakage of Personal Data of their users based on Law Number 11 of 2008 and its amendment Law Number 19 of 2016 and its further amendment Law Number 1 of 2024 concerning Electronic Information and Transactions and Law Number 27 of 2022 concerning Personal Data Protection.
2. To find out whether there are legal steps that users can take if their Personal Data has been leaked.

#### **D. Literature Review**

There has not yet been any undergraduate thesis written specifically on “civil liability and responsibility of corporations and related agencies for the leakage of personal data of its users.” However, the author has found several theses with similar themes, namely:

1. The undergraduate thesis by Ramiz Afif Naufal, titled “*Tanggung Jawab PT. Tokopedia dalam Kasus Kebocoran Data Pribadi Pengguna*”, Faculty of Law, Islamic University of Indonesia, 2020, it discuss PT Tokopedia responsibility in the 2020 personal data leak, analyzing the case through the ITE Law and the draft Personal Data Protection Bill, and focusing on the lack of comprehensive regulation to protect users at that time. The difference is that this research takes a broader perspective by explaining the civil liability of corporations and related agencies for personal data leakage under the enacted Personal Data Protection Law, the role of supervisory authorities, and on a legal remedy for data subjects.
2. The undergraduate thesis by Arda Putri Ramadhani, titled “*Perlindungan Hukum Pengguna Marketplace Dalam Hal Keamanan Data Pribadi Pengguna*”, Faculty of Law, Islamic University of Indonesia, 2020, it discusses civil liability in electronic marketplace transaction disputes, focusing on how the liability is determined between sellers, buyers, and platforms when conflicts arise in online trade using Indonesian civil code and ITE law. The difference with this research is that this research concentrates on civil liability for personal data leakage, analyzing the

responsibilities of corporations and related agencies under the Personal Data Protection Law and exploring remedies available to data subjects.

3. The undergraduate thesis by Raihan Caesar Bhaskara, titled “*Analisis Yuridis Tanggung Jawab Perdata Pengendali Dan Prosesor Data Pribadi Dalam Hal Terjadinya Kegagalan Perlindungan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi*”, Faculty of Law, Brawijaya University, 2025, the research examines the civil liability of personal data controllers and processors in cases of data protection failure, analyzing Law No. 27 of 2022 on Personal Data Protection in comparison with the GDPR, with emphasis on strict liability and compensation standards. The differences are located in the approach, subject, and scope. The approach uses a comparative analysis with the GDPR, the subject is limited to data controllers and processors, and the scope addresses data protection failures in general rather than specific leaks cases.
4. The undergraduate thesis by M. Ciko ar Rasyid, titled “*Kajian Yuridis Undang-Undang Perlindungan Data Pribadi Terhadap Tanggung Jawab Perusahaan Pada Kasus Kebocoran Data Konsumen (Studi Kasus Pada PT Telkom Indonesia)*”, Faculty of Law, Muhammadiyah University of Magelang, 2024, the research explains the responsibility of PT Telkom Indonesia in a consumer data breach case, examining the company compliance with the Personal Data Protection Law alongside related regulations such as PP No. 71 of 2019 and the Minister of Communication

and Informatics Regulation No. 20 of 2016. The differences are located the approach, subject, and scope: the approach focus on assessing regulatory compliance, the subject is limited to a single corporation (PT Telkom), and the scope on one consumer data leakage case without explaining broader civil liability or user remedies.

## **E. Theoretical Framework**

To address legal issues related to liability for personal data breaches and the legal remedies available to data owners, a theoretical foundation that provides in-depth legal understanding is required. This theoretical framework will serve as a reference in analyzing two main aspects: first, the civil liability and responsibility that can be imposed on corporations as data controllers and data processor, and personal data protection authorities as supervisors; and second, the legal remedies available to data subjects when their personal data is leaked. Therefore, this study uses the theory of civil liability to examine the aspect of legal liability, and the theory of legal protection to explain the remedial options available to the harmed data owners. These two theories will serve as the conceptual foundation for further discussion and analysis in subsequent chapters.

### **1. Theory of Civil Liability**

The theory of civil liability is a theory of civil law that regulates the legal consequences of an act that harms and margraviate another party. Civil liability arises when a person or legal entity commits an unlawful act (*Perbuatan Melawan Hukum*) or breaks its promise

regarding an obligation (*wanprestasi*), thereby causing harm and loss to the other related party. In the context of Indonesian law, the normative basis of this theory can be found in Article 1365 of the Civil Code, which states that:

"every unlawful act, which causes harm to another person, requires the person at fault for causing the loss, to compensate for the loss."

Doctrinally, civil liability can be classified into two main forms: liability based on unlawful acts (*onrechtmatige daad*) and liability based on breach of contract (*wanprestatie*). In cases of personal data breaches, a corporation, as the data controller, can be held liable if its negligence in maintaining data security results in losses for the data owner. If the relationship between the data subject and the corporation is based on an agreement, such as a digital services agreement, then a violation of the obligation to protect personal data can also be classified as a breach of contract.

#### **a. Unlawful Act**

Unlawful acts are the primary basis for civil liability outside of a contract. In Indonesian civil law, this provision is regulated in Article 1365 of the Civil Code, which states that any unlawful act that causes harm to another person requires the perpetrator to compensate for that loss.

John G. Fleming (common law perspective) defines a tort (as a form of unlawful act) as a civil wrong, other than breach of

contract, which the law will redress by an award of damages.<sup>8</sup> R. Subekti, a leading Indonesian legal scholar, defines an unlawful act as every act that violates the law and causes harm to another person, which obligates the person who caused the harm to compensate for the loss.<sup>9</sup> Although they both come from distinct legal traditions, the definitions underline the theory of civil liability, the existence of an unlawful act (*perbuatan melawan hukum*) that causes harm to another party. This highlighting civil law's role as a way to receive compensation and protection from the damaged party.

As a result, the conditions that must be met to prove the existence of an illegal act as specified in Article 1365 of the Civil Code are:

#### 1) Unlawful Act

The first requirement is the existence of an element of unlawful act, which refers to any conduct that violates legal norms, whether by action or omission. In Indonesian civil law, the definition of "unlawful" goes beyond a simple breach of written laws. It also includes activities that violate others rights, moral norms, or fail to meet society standard.

In practice, a person can be held liable not only for breaking

---

<sup>8</sup> R. Subekti, *Pokok-Pokok Hukum Perdata* (Jakarta: Intermasa, 2008), p. 41.

<sup>9</sup> John G. Fleming, *The Law of Torts*, 9th ed. (Sydney: LBC Information Services, 1998), p. 1.

formal laws but also for socially unacceptable behavior that causes harm to others.<sup>10</sup>

## 2) Fault or Negligence

The second element requires that the unlawful act be attached to the actor through fault, which can come from intentional misconduct (*dolus*), or negligence (*culpa*). Fault indicates that the individual has control over their actions and intended the harmful or failed to do the reasonable care expected from them. Indonesian civil law does not impose strict liability in most cases under Article 1365; rather, it presumes liability only when there is demonstrable fault. This means the victim must show that the perpetrator acted either recklessly or without the proper standard of caution that a prudent person would have observed under similar circumstances.

## 3) Loss or Damage

A valid claim for unlawful act liability must include proof of actual loss and harms suffered by the claimant. These harms could take the forms of material damage such as financial losses, physical damage to property, or loss of income or immaterial harm, including emotional distress, loss of reputation, or psychological suffering. The claimant in this

---

<sup>10</sup> District Court of Tangerang, *Putusan Nomor 305/Pdt.G/2009/PN.Tng*, regarding a compensation lawsuit due to a unilateral flight cancellation by the airline, 2009.

liability bears the burden of proofs on the extent and impact of the damage. Indonesian courts generally require that the damage be concrete, measurable, and directly linked to the unlawful conduct. Without such damage, even a proven unlawful act does not result in civil liability.

#### 4) Causal Relationship

Finally, there must be a causal link between the unlawful act and the damage suffered. This means that the harm experienced by the victim must be a direct and attributable consequence of the defendant's conduct. In Indonesian legal doctrine, this is often analyzed through the concept of "adequate causation", which asks whether the act was sufficiently connected to the loss to warrant a civil liability.<sup>11</sup> If the damage results from a completely independent or unforeseeable event, liability may not be imposed. Establishing causation ensures that defendants are only held accountable for harm they actually caused or could reasonably have anticipated.

In the context of personal data protection, an action or omission by a corporation that results in a leak of personal data can be classified as an unlawful act if it is not in line with the legal

---

<sup>11</sup> Wirjono Prodjodikoro, *Perbuatan Melawan Hukum* (Bandung: Sumur Bandung, 1971), 59.

obligations or due diligence principles that should be carried out by the data controller.

## **b. Breach of Contract**

Breach of contract is a form of civil liability arising from a violation of an agreement or contract. According to Article 1243 of the Civil Code, default is:

“Compensation for costs, losses, and interest due to non-performance of an obligation is required when the debtor, after being declared in default, still fails to fulfill the obligation.”

If a party fails to fulfill its obligations, it may be in breach of contract and liable for any resulting losses. To make a valid claim, the following elements must be present:

### 1) Existence of a Valid Agreement

The first essential element of breach of contract is the presence of a legally binding agreement between the parties. According to Article 1320 of the Indonesian Civil Code, A valid contract requires mutual consent, legal capacity, a specific and lawful object, and a lawful cause. Without a valid contract, no breach can occur. Any claim for breach of contract must be based on the existence of a legitimate contractual relationship.

### 2) Obligation to Perform

Once a valid contract is established, it must create specific obligations for the parties involved. As stipulated in Article

1234 Indonesian Civil Code, an obligation may consist of giving something, doing something, or refraining from doing something. The debtor must carry out the performance in accordance with the terms and conditions set out in the agreement. Failure to carry out this performance, either wholly or in part, can give rise to legal consequences if the performance was indeed required under the contract.

### 3) Failure to Perform or Improper Performance

A breach of contract occurs when the debtor does not fulfill their agreed obligations. This may include failing to perform, performing late, not complying with contract terms, or acting against agreed restrictions. The breach must be substantial enough to affect the creditor's rights or interests under the agreement.

### 4) Debtor's Fault

A fundamental principle in establishing liability for breach of contract is the presence of fault (*culpa*) on the part of the debtor. The law assumes that the debtor is at fault unless they can prove otherwise. This includes both intentional breach and negligence. However, the debtor may be relieved of liability if they can demonstrate that the failure to perform

was due to force majeure (*keadaan memaksa*)<sup>12</sup> that is, extraordinary circumstances beyond their control which made performance impossible.

#### 5) Losses Suffered by the Creditor

To claim compensation, the creditor must prove that they have suffered a loss as a direct result of the breach. This loss can be material such as financial damage, increased costs, or lost profits or immaterial, such as damage to reputation or emotional distress in certain cases. The burden of proof lies with the creditor, who must show a clear link between the debtor's failure and the damage incurred.

#### 6) Default Notice

Under Article 1243 KUHPerdata, compensation for damages becomes enforceable only after the debtor has been declared in default (*lalai*). In practice, this often requires a written warning or summons (*somasi*), informing the debtor of their failure to perform and providing them an opportunity to fulfill their obligation. However, summon is not required in cases where the breach is clear and immediate such as when a fixed performance date is missed.<sup>13</sup> Once the debtor is formally in default, the creditor may then seek legal remedies

---

<sup>12</sup> J. Satrio, *Wanprestasi Menurut KUHPerdata, Doktrin, dan Yurisprudensi* (Bandung: Citra Aditya Bakti, 1992), p. 112–118.

<sup>13</sup> Indonesia, *Civil Code*, article 1238.

including compensation for damages, cancellation of the contract, or enforcement of specific performance.

In summary, breach of contract is a party's failure to fulfill obligations under Articles 1234 and 1243 of the Indonesian Civil Code. It requires a valid agreement, a breached obligation, debtor fault, resulting loss, and, when applicable, a default notice. These elements provide the legal basis for remedies and highlight the importance of honoring contractual commitments in civil law.

In the context of the state's role, personal data protection authorities tasked with overseeing data controllers' compliance with legal provisions may also be held indirectly liable if proven negligent in carrying out their statutory oversight duties. While state accountability is generally public or administrative, under certain circumstances, it can also give rise to civil liability if such negligence directly impacts the loss of citizens.

Thus, the theory of civil liability provides a normative and analytical framework for assessing the legal obligations of parties involved in the management of personal data, as well as providing a basis for victims of data breaches to claim restitution and compensation.

## 2. Theory of Legal Protection

The theory of legal protection serves as the main framework for this research. According to Philipus M. Hadjon, the theory of legal protection explains how the law provides guarantees of protection to individuals against arbitrary actions, through preventive and repressive mechanisms, with the aim of creating justice and legal certainty.<sup>14</sup> Thus, legal protection can be divided into two forms:

- a. Preventive legal protection, refers to legal mechanisms that are designed to prevent the occurrence of rights violations before they happen. According to Philipus M. Hadjon, this form of protection provides individuals or the public the opportunity to raise objections, submit opinions, or participate in decision-making processes before a governmental or administrative decision takes a final and binding form. The aim of preventive protection is to ensure that decisions made by authorities are legal, fair, and in line with the public interest, thereby minimizing the potential for arbitrary or unlawful actions.; and
- b. Repressive legal protection, On the other hand, repressive legal protection applies after a rights violation or unlawful act has occurred. This protection refers to the legal remedies available to individuals to sue, correct, or seek compensation for the violation.

---

<sup>14</sup> Philipus M. Hadjon, *Perlindungan Hukum Bagi Rakyat Indonesia* (Surabaya: Bina Ilmu, 1987), p. 2.

This form of protection is reactive and is usually implemented through judicial or quasi-judicial mechanisms, such as filing a lawsuit in court, filing a complaint with a regulatory body, or requesting review by an ombudsman or state administrative court.

The theory of legal protection has a strong normative basis in the Indonesian legal system. One of its main foundations is found in the 1945 Constitution of the Republic of Indonesia, specifically Article 28D paragraph (1), which states that

"Everyone has the right to recognition, guarantees, protection, and certainty of fair law and equal treatment before the law."

This article emphasizes that legal protection is a constitutional right of every citizen.

### **3. Theory of Legal Remedies**

In examining the civil liability of corporations and related agencies for personal data breaches, this research employs the theory of legal remedies as a fundamental theoretical basis. According to Salmond, law does not merely establish rights and duties, but also provides remedies when those rights are violated; in his words, "where there is a right, there is a remedy" (*ubi jus ibi remedium*).<sup>15</sup> This maxim reflects the idea that the recognition of a legal right must necessarily be accompanied by a mechanism to enforce it, otherwise the right itself would be meaningless.

---

<sup>15</sup> John Salmond, *Jurisprudence* (12th ed., Sweet & Maxwell 1966), p. 95.

The theory of legal remedies is concerned with the instruments of redress available when legal norms are breached, such as damages, restitution, injunctions, or specific performance. In this view, remedies serve not only as corrective measures for the injured party but also as a means of reinforcing the authority of the legal system. As Friedmann observes, the effectiveness of law depends not only on the substantive rules it contains but also on the availability of adequate remedies for those whose rights are infringed.<sup>16</sup>

Applied as a theoretical framework, this approach emphasizes that legal obligations imposed on actors. Whether corporations, agencies, or individuals, must be accompanied by enforceable remedies in the event of non-compliance. Remedies thus function both as a guarantee of justice for the victim and as a deterrent for potential violators. This research therefore situates the analysis of civil liability for data breaches within the paradigm that law must provide not only duties and prohibitions but also concrete legal consequences that restore balance when harm occurs.

In addition, these are legal principles that are used to resolve incompatibility between laws and regulations:

1. *Lex specialis derogate legi generali*. “the special law derogates from the general law” used to resolve conflicts between laws with broader

---

<sup>16</sup> W. Friedmann, *Legal Theory* (5th ed., Stevens & Sons 1967), p. 107.

regulatory substance and laws with narrower regulatory substance.<sup>17</sup>

Principle *lex specialis derogat legi generali* only applies to two regulations that are hierarchically equal and regulate the same material.

2. *Lex superior derogate legi inferiori*. If a conflict occurs between higher and lower-level laws and regulations, the higher-level regulations must take precedence. This principle only applies to two regulations that are in conflict but not hierarchically equal.<sup>18</sup>

3. *Lex posterior derogate legi priori*. This is the principle that a law that applies later revokes a previous law, as long as that law regulates the same object. The purpose of this principle is to prevent legal uncertainty that may arise when there are two regulations that are equal based on hierarchy.<sup>19</sup>

## **F. Operational Definition**

1. Corporation and related agencies, are a term used freely by the researcher to refer to all parties whether individuals or corporations involved in the following activities:
  - a. Controlling Personal Data
  - b. Processing of personal data
  - c. Personal Data supervision

---

<sup>17</sup> Shidarta and Petrus Lakonawa, "Lex Specialis Derogat Legi Generali: Makna dan Penggunaannya," *Business Law BINUS*, March 3, 2018, <https://business-law.binus.ac.id/2018/03/03/lex-specialis-derogat-legi-general/>, accessed December 4, 2024.

<sup>18</sup> Jonaedi Effendi, *Kamus Istilah Hukum* (Jakarta: Kencana, 2009), p. 69.

<sup>19</sup> Ibid.

2. Personal Data, is any data about an individual who is identified and/or can be identified either independently or in combination with other information, directly or indirectly, through electronic or non-electronic systems.
3. Personal Data Subject/Data subject refers to the individual (natural person) to whom a set of personal data relates. This person is the owner or holder of the data and is granted specific rights and protections under data protection laws.
4. Personal Data Controller is any party that determines the purpose and has control over the processing of Personal Data.
5. Personal Data Processor is any party that processes Personal Data on behalf of a Personal Data Controller.
6. Personal Data Supervisory Body is a government institution established to oversee the implementation of personal data protection in Indonesia. Until the Supervisory Body is officially formed, its functions are carried out temporarily by the Ministry of Communication and Informatics (*Kominfo*).

#### **G. Research Method**

The method used in this research is as follows:

##### 1. Type of research

The type of research that the author uses in the preparation of this legal writing is normative legal research, namely legal research conducted by examining library materials or secondary data consisting of primary

legal materials, secondary legal materials, and tertiary legal materials. These materials are arranged systematically, studied, and then a conclusion is drawn in relation to the problem under study.<sup>20</sup>

## 2. Research Approach

In this research, the author will use an approach method in the type of normative legal research approach such as:<sup>21</sup>

### a. Statutory Approach

The statutory approach referred to in this study is the approach used to examine and analyze all laws and regulations that have relevance or have to do with the legal issues at hand.

### b. Conceptual Approach

A conceptual approach is an approach that departs from the views, doctrines that already exist and develop in the science of law, as well as to find out their application in practice and legal decisions.

## 3. Object of Research

The object of this research is to determine the liability and responsibility of the corporation and its related agencies for the leakage of Personal Data of its users.

## 4. Sources of Research Data

---

<sup>20</sup> Soerjono Soekanto, *Penelitian Hukum Normatif Suatu Tinjauan* (Jakarta: Rajawali Pers, 2013), p. 13.

<sup>21</sup> Peter Mahmud Marzuki, *Penelitian Hukum*, 6th print (Jakarta: Kencana Prenada Media Group, 2010), p. 93.

The data sources used in this study are secondary data sources consisting of primary legal materials, secondary legal materials, and tertiary legal materials, namely:

a. Primary legal materials

Primary legal materials are binding legal materials, consisting of statutory regulations, official treaties, court decisions, and official state documents.<sup>22</sup> The legal materials include:

- A. The 1945 Constitution of the Republic of Indonesia
- B. Indonesian Civil Code
- C. Indonesian Commercial Code
- D. Law Number 11 of 2008 and its amendment Law Number 19 of 2016 and its amendment Law Number 1 of 2024 concerning Electronic Information and Transactions (ITE Law)
- E. Regulation of the Minister of Communication and Informatics Number 19 of 2016 concerning the Protection of Personal Data in Electronic Systems
- F. Law Number 27 of 2022 concerning Personal Data Protection
- G. Law No. 30 of 1999 Arbitration and Alternative Dispute Resolution

b. Secondary legal material

Then, secondary legal materials, in this case, secondary legal materials, are legal materials that do not have legally binding legal force

---

<sup>22</sup> Soerjono Soekanto and Sri Mamudji, *Penelitian Hukum Normatif: Pengantar Singkat* (Jakarta: Rajawali Press, 1990), p. 13.

as primary legal materials, while secondary legal materials include, among others, legal books and scientific journals.<sup>23</sup>

c. Tertiary legal material

Tertiary legal materials, in this case, tertiary legal materials as intended, are legal materials whose function is to provide explanations for primary legal materials and secondary legal materials. The tertiary legal materials include a large Indonesian dictionary, a legal dictionary, English dictionary, law encyclopedia and Statutory regulations index.<sup>24</sup>

5. Method of Data Collection

The method of collecting secondary data in normative legal research is carried out by studying literature on legal materials, both primary legal materials, secondary legal materials, and tertiary legal materials related to the research.<sup>25</sup>

6. Method of Data Analysis

The data analysis method used by the author in this study is a qualitative descriptive analysis method, namely, data obtained from written materials such as legislation and books that are described qualitatively first and then analyzed based on a literature study to obtain a conclusion on the formulation of the problem in this study.

According to Waluyo, descriptive research is research that aims to describe something in a certain area and at a certain time. Usually in this

---

<sup>23</sup> Muhaimin, *Metode Penelitian Hukum*, 1st printing (Nusa Tenggara Barat: Mataram University Press, 2020), p. 56.

<sup>24</sup> Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Kencana, 2005), p. 141.

<sup>25</sup> Muhaimin, *Op. Cit.*, p. 65.

research, the researcher has got/has an overview in the form of initial data about the problem to be studied.<sup>26</sup>

## **H. Structure of Writing**

The writing of this research is structured by dividing into 4 (four) chapters, as follows:

Chapter I is an Introduction, consisting of Context of Study, Problem Formulation, Research Objectives, Literature Review, Operational Definition, Research Methodology, and Writing Structure.

Chapter II is Theoretical Review. This chapter will discuss in detail the theories related to the formulation of the problem in this research, including an overview of Personal Data Protection and an overview of Data Leakage.

Chapter III is Findings and Results. This chapter will answer 2 (two) problem formulations in this study. First, what are the civil liability and responsibility of companies and related agencies as Personal Data Controller and Personal Data Processor for the leakage of Personal Data? Second, to find out whether there are legal steps that website users can take if their Personal Data has been leaked.

Chapter IV is the Conclusion and Recommendation. In this chapter, the conclusions will be drawn from the summary of answers to the analysis of the three problem formulations in this study. Meanwhile, the recommendation

---

<sup>26</sup> Eray Hendrik Mezak, "Jenis Metode dan Pendekatan dalam Penelitian Hukum," *Law Review*, Faculty of Law, Universitas Pelita Harapan, Vol. V, No. 3 (2006), p. 88.

will be made based on the author's thoughts after analyzing and drawing conclusions from the 2 (two) problem formulations.