

CHAPTER I

INTRODUCTION

A. INTRODUCTION

This information constitutes a part of the recipient's data and can be used to identify the data owner; therefore, it can be referred to as personal data. Minister of Communication and Informatics Regulation No. 20, concerning the protection of personal data in the system, was issued in 2016. Article 1(1) of the Electronic defines personal data as specific personal data that is stored, maintained, and protected for accuracy and confidentiality. This situation mirrors cases that have occurred in Indonesia. According to CNBC Indonesia, there have been instances of 58 individuals engaging in fraud under the guise of a fake parcel courier application¹.

Additionally, there have been cases of abduction where the perpetrator acquired all the victim's data through packages sent to the victim's location. The perpetrators collected all the packages (Shipping labels) in the victim's name, matched all the personal data, and one day, they gained complete knowledge of the victim's full address and family, subsequently carrying out their action, including harming the victims².

In this case, there are applicable rules regarding the protection of personal data in Article 65, Paragraphs (1) and (3) of the PDP Law, namely:

¹Binekasri,R "Revealed! This is the Fraud Mode Under the Guise of a Package Courier" <https://www.cnbcindonesia.com/tech/20230123180846-37-407629/terungkap-begini-modus-penipuan-berkedok-kurir-paket> access at 25 May 2024

² Ibid.

1. Every person is prohibited from unlawfully obtaining or collecting personal data that does not belong to them to benefit themselves or others, which may result in harm to the personal data subject. Any person who violates this provision shall be punished with a maximum imprisonment of 5 years and/or a maximum fine of IDR 5 billion.
2. Every person is prohibited from unlawfully using personal data that does not belong to them. Any person who violates this provision shall be punished with a maximum imprisonment of 5 years and/or a maximum fine of IDR 5 billion.

Other provisions related to the theft of personal data can also be seen in Article 26, paragraph (1) of Law 19/2016, which reads: Unless otherwise provided by laws and regulations, the use of any information through electronic media concerning a person's data must be done with the consent of the person concerned. Any person whose rights are violated may file a lawsuit for losses incurred under this Law³.

Article 1 (1) Personal data is data about an identified or identifiable natural person individually or in combination with other information, either directly or indirectly through electronic or non-electronic systems. Electronic systems and/or non-electronic systems. Law No. 27 of 2022 explains that personal data protection is the overall effort to protect personal data throughout a series of personal data processing activities, ensuring the constitutional rights of individual data subjects.

The legal protection of personal data needs to be studied in detail and objectively to ascertain how the legal arrangements for personal data protection in

³ Law No. 19 of 2016 concerning Electronic Information and Transactions (ITE Law).

Indonesia are. Indonesia, which currently lacks its own individual data protection supervisory authority, should examine the practices, establishment standards, and mechanisms employed in several countries that comprehensively regulate personal data protection supervisory authorities in their regions.

Personal data refers to data about an individual who can be identified from that data, or from that data and other information to which the organization has or may have access.⁴ Singapore is one of the countries that also has regulations related to privacy rights and personal data sectoral, namely the Personal Data Protection Act No. 26 of 2012 Singapore (PDPA). Singapore has a personal data protection supervisory authority known as the Personal Data Protection Commission (PDPC), which is attached to the existing Info-communications and Media Development Authority (IMDA).

The personal data leak that occurred in Singapore in 2020 involved the personal data of Lazada users, compromising as many as 1.1 million accounts. In the data leak, this illegally accessed user information also included names, phone numbers, email and mailing addresses, encrypted passwords and some credit card numbers.⁵ In 2018, Singhealth patients also experienced a data leak, one of the health institutions in Singapore, in this case there were 1.5 million leaked patient

⁴ "PDPA Overview" PDPA Overview - Singapore Accessed on February 25, 2024 at 20:40

⁵ "Lazada Singapore Admits to Breach of 1.1 Million Users' Personal Data" 2020. Lazada Singapore Admits to Breach of 1.1 Million Users' Personal Data - Selular.ID Accessed on February 25, 2024 at 21.30

personal data, of which there were 160 thousand leaked patient medical record data including the prime minister of Singapore Lee Hsien Loong.⁶

Moving on to personal data protection regulations, if Indonesia has rules governing personal data, then Indonesia has Law Number 27 of 2022 concerning Personal Data Protection (UU PDP). Singapore also has privacy laws, and personal data protection in Singapore is regulated under the Personal Data Protection Act (PDPA).

In Singapore, personal data is protected under the Personal Data Protection Act 2012 (PDPA 2012). Singapore's Personal Data Protection Act 2012 and the Public Sector Governance Act 2018 include the principles of consent, purpose, and reasonableness.

Globally, e-commerce platforms are frequently targeted by hackers and data thieves, particularly as people's activities have mainly shifted to digital platforms. According to the Cyber Security Agency of Singapore (CSA) records, cybercrime accounted for 26.8 percent of all crimes in Singapore last year, with e-commerce fraud being the most prevalent type. A total of 9,430 cybercrime cases were reported in 2019, representing a 51.7% increase from the previous year⁷.

⁶Nursalikhah, A. "Singapore Breached, Health Data of 1.5 Million Citizens Leaked" International Republic. 2020. | Republika Online Mobile accessed on February 25, 2024 at 22.00 WIB

⁷ Baharuddin, H. "Three times more phishing attacks in Singapore in 2019, twice as many during Covid-19 pandemic" <https://www.straitstimes.com/singapore/three-times-more-phishing-attacks-in-singapore-in-2019-twice-as-many-during-covid-19> accessed on February 25, 2024 at 23.50 WIB

The PDPC is Singapore's primary authority responsible for rights related to personal data protection, and it represents the Singapore government in matters concerning the handling of personal data protection.

These protections are included in the Personal Data Protection Act and the Public Sector Governance Act. The Singapore government also imposes criminal sanctions and fines for breaches of personal data. Based on the above explanation, this research will analyze the regulations on a Comparison between Indonesia's Personal Data Protection Act of 2022 and Singapore's Personal Data Protection Act of 2012, focusing on aspects related to criminal offenses. Singapore's data privacy protection practices are also sufficient to serve as a benchmark for Indonesia, particularly with the establishment of the Personal Data Protection Commission (PDPC) institution. Indonesia is expected to emulate Singapore, which has provided guarantees for the protection of personal data as outlined in the laws of the Lion Country, namely the PDPA and PSGA.

B. Problem Formulations

1. What is the comparison of regulations on violations of personal data protection in Indonesia and Singapore?
2. What are the differences between law enforcement agencies related to personal data protection in Indonesia and Singapore?

C. Objectives of Research

1. To analyze the comparison of regulations on violations of personal data protection in Indonesia and Singapore

2. To analyze the differences between law enforcement agencies related to data protection in Indonesia and Singapore.

D. Research Originality

This research raises the title of “The Comparison of the Provisions on the Offence against Personal Data Protection in Indonesia and Singapore”. There are several studies that are relevant to the title studied by the author, here are the relevant studies:

Research conducted by Watkat, F. X., Ingratubun, M. T., & Apriyanti, A. (2024) with the title “Personal Data Protection Through The Application Of The Criminal Law System In Indonesia” the results of the research found are that although there are regulations regarding personal data in Indonesia, namely Indonesian Law No.27 of 2022 concerning Personal Data Protection, criminal law has not been applied in accordance with what has been stated in articles 65 to 73 which regulate the prohibition of misuse of personal data Year 2022 concerning Personal data protection, but criminal law has not been applied in accordance with what has been stated in articles 65 to 73 which regulates the prohibition of misuse of personal data and regulates criminal provisions carried out both by individuals, legal entities (corporations) in Indonesia. The factors causing this are that the formulation of legal policy by the legislator prioritizes administrative sanctions, then criminal law enforcement is the last resort in follow-up sanctions, dispute resolution can be done outside the judicial system, and the Personal Data Protection

Institution has not been formed as referred to in the provisions of Article 58 of the Personal Data Protection Law.⁸

Research conducted by Almira. T, et al (2020) with the title “Protection of Privacy Data in Indonesia and Singapore Regarding the Application of Digital Contact Tracing as an Effort to Prevent Covid-19 and its Responsibilities” that the results of his research are the application of digital contact tracing in Indonesia with tracking applications violating several principles related to personal data.

Personal data regulations in Indonesia itself are specifically still limited to ministerial regulations. In contrast to Singapore, it has guaranteed the protection of personal data of its people through the Personal Data Protection Act and the Public Sector Governance Act 2018, and regarding responsibility for personal data, in Indonesia it is still limited to administrative sanctions, while in Singapore, it reaches criminal liability. The method used in this research is the normative juridical method.⁹

Furthermore, research conducted by Sylvia Faradina Amandasari Arthaputri, et al (2024) entitled “Perlindungan Data Pribadi Sebagai Bentuk Perwujudan Cyber Security (Comparative Study of Indonesia and Singapore)” the type of research used is normative law with three approaches, namely legislative approach, concept approach, and comparative approach. The results of his research state that Law Number 27 of 2022 concerning Personal Data Protection has realized 3 indicators

⁸ Watkat, F. X., Ingratubun, M. T., & Apriyanti, A. (2024). Personal Data Protection Through the Implementation of the Criminal Law System in Indonesia. *Ius Publicum Law Journal*, 5(1), 153–175. <https://doi.org/10.55551/jip.v5i1.83>

⁹ Almira. T, et al. “Data Privacy Protection in Indonesia and Singapore Regarding the Implementation of Digital Contact Tracing as an Effort to Prevent Covid-19 and its Responsibilities” *Journal of Legal Certainty*. Volume 2 Number 1, December 2020.

of cyber security, namely Confidentiality, Integrity, and Availability so that it has protected the personal data of the Indonesian people. The comparison with Singapore's Personal Data Protection Act 2012 is the difference in the scope of regulation, definition of personal data, and sanctions imposed.¹⁰

Research conducted by Fitrahul Azza Faizah, et al (2023) with the title “Strengthening Personal Data Protection Through Supervisory Authority in Indonesia Based on Comparison of Hong Kong and Singapore Law”. The research method used is normative comparative with descriptive analytical research specifications, namely research conducted by comparing the mechanism of the supervisory authority for personal data protection and positive laws relating to privacy and personal data protection in Hong Kong and Singapore. The research results show that: First, the existence of LPPDP which has independence will strengthen the law of personal data protection effectively and fulfill adequacy with other developed countries. Second, there are several recommendations in forming the LPPDP institutional model if it is formed with a single supervisory authority or ministry-based-models.¹¹

Research conducted by Yuniarti, S (2023) with the title “Personal Data Protection Officers in the Personal Data Protection Ecosystem: Indonesia, the European Union and Singapore” The research method used is normative juridical, from the research conducted the existence of data protection officers is part of

¹⁰ Sylvia Faradina Amandasari Arthaputri, et al. “PERSONAL DATA PROTECTION AS A FORM OF CYBER SECURITY (Comparative Study of Indonesia and Singapore)”. Vol 30 No 1. January 2024, pp. 9495-9509

¹¹ Fitrahul Azza Faizah, et al. “Strengthening Personal Data Protection Through Supervisory Authorities in Indonesia Based on Comparison of Hong Kong and Singapore Laws”. Hakim: *Journal of Law and Social Sciences* Vol.1, No.3 August 2023

personal data protection regulations, both appearing as an obligation for all organizations and in the event of the fulfillment of certain conditions. The need for emphasis on independence and organizational support so that data protection officers are optimal in carrying out their functions and duties which have been comprehensively regulated in the GDPR and the presence of data protection officers as a service as an effort to meet the need for data protection officers by organizations.¹²

¹² Yuniarti, S. "Personal Data Protection Officers/Officials in the Personal Data Protection Ecosystem: Indonesia, the European Union and Singapore" *BECOSS JOURNAL (Business Economic, Communication, and Social Sciences)*, Vol.4 No.2 May 2022: 11-120.

E. Literature Review

1. Personal Data Protection

a. Definition and principles

The issue of personal data security is increasingly important in today's society. Personal data is all information about a person, both data that can be identified or verified. A lot of personal data is listed starting from telephone numbers, full names, personal addresses that can directly identify individuals.

Personal data is so related to personal information, a lot can be known through personal data about a person. Personal information is understood as information that describes an individual, from this understanding it can describe a person's individual who is related to the individual's personal data, whether it is sensitive or something that is considered normal.

The individual is a social unit that has rights that cannot be denied and aims to fulfill individual interests. In the cultural relativism model, the community is a social unit. In this case, concepts such as individualism, freedom of choice, and equality become unclear. Personal information, according to Raymond Wax, is personal information about an individual consisting of facts, communications, and opinions about that individual that the individual believes to be confidential and that the individual does not agree to collect, use, or distribute may be restricted or prohibited.

b. The offences against personal data protection

In the protection of personal data there are also several explanations of existing violations, as follows:

1. Every person is prohibited from unlawfully obtaining or collecting personal data that does not belong to him/her with the intention of benefiting himself/herself or others which may result in the loss of the Personal Data Subject.

In this case, if there is a violation such as copying someone's personal data without rights and does not belong to him, he will be subject to the law according to what has been regulated, or misusing personal data for defamation on social media or not.

2. Every person is prohibited from unlawfully disclosing personal data that does not belong to him.
3. Every person is prohibited from unlawfully using personal data that does not belong to him/her.

In this case, the form of violation included is using personal data that does not belong to it, such as misuse of personal data as an emergency contact for loan sharks or misuse of personal data for online loans made by personal data controllers or in this case, loan shark operators do not have a basis for processing personal data, one of which is in the form of consent from the subject of personal data. data subject to administrative sanctions such as written warnings, cessation of data processing, deletion of personal data or administrative fines.

4. Every person is prohibited from creating false personal data or falsifying personal data with the intention of benefiting themselves or others which may result in harm to others.

Personal data protection is a form of privacy protection that includes protecting one's privacy or protecting one's personal data. Indonesian laws regulate personal data protection and identify legal barriers to personal data protection and solutions. Data protection laws apply to protect automated data and personal data in automated data processing, as well as in structured formats for manual data storage.

Everyone is obliged to obtain personal protection as stipulated in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia which states that everyone has the right to protection of self, family, honor, dignity, and property under their control. The right to security and freedom from the threat of fear to do or not do something is a human right.

c. Principles of personal data protection

From the many comparisons of privacy principles in various countries, there are at least 8 principles that almost certainly appear in every regulation. Especially the rules regarding personal data protection based on the OECD.¹³ The eight principles are Principles of collection limitation, data quality, purpose specification, purpose limitation, security protection, openness, individual participants, and accountability.¹⁴ Of the eight principles, the following is an explanation of each principle:

¹³ Wahyuni, W. "8 Principles of Privacy Rights in Personal Data Protection Rules". 2023. <https://www.hukumonline.com/berita/a/8-prinsip-hak-privasi-dalam-aturan-pelindungan-data-pribadi-lt64a2dcec71359/?page=2> accessed on March 28, 2024, at 20.40

¹⁴ (Business Economic, Communication, and Social Sciences), Vol.1, No.1 September 2019: 147-154

1. The Collection Limitation principle means that there must be limits to the collection of personal data and such data must be obtained by lawful and fair means with the knowledge or consent of the data subject.
2. The principle of data quality is that all personal data must have relevance to the purpose for which it is used, and that purpose must be clear and complete, accurate and kept up to date.
3. The Principle of Purpose Specification is the principle that the purposes for which personal data are collected must be specified no later than when the data are collected and subsequent use is limited to the fulfillment of either those purposes or their incompatible purposes, and is specified for any change in purpose.
4. The principle of restriction of use means that personal data is not allowed to be disclosed, either made available or used for purposes other than those specified, but this has exceptions: (a) with the consent of the data subject; or (b) by a legal authority.
5. The Security Protection Principle means that personal data must be protected by reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, alteration or disclosure of data.
6. The principle of transparency means that there is a policy of openness about the practice, development and regulation of personal data. It must be available to establish the existence or nature of personal data as well as the main purpose of its use, not to forget the identity and location of the data controller.

7. The Individual Participant Principle is that every individual has the right;
 - a. to obtain from the data controller, or confirm, whether or not the data controller holds the relevant data;
 - b. to communicate with them, data relating to them: (i) within a reasonable time; (ii) for a fee, if any; (iii) for sufficient reason; and (iv) provided in an intelligible form.
 - c. Reasons shall be given if a request made under (a) and (b) is refused, and it can be argued that the refusal is justified;
 - d. To challenge the data to which they relate, and if the challenge is correct, to delete the data, correct, supplement or amend.
or amend.¹⁵
8. The Accountability Principle means that data controllers must be responsible for complying with the procedures that impact the above principles.

2. Law Enforcement of Personal Data Protection

a. Definition of Law Enforcement

Law enforcement is an effort to realize the ideas of justice, legal certainty and social benefit into reality. Law enforcement is the process of making efforts to uphold or function legal norms in reality as guidelines in the legal relations of life in society and the state. Law enforcement has two types of stages, namely in abstracto and in concreto.

¹⁵ Law Number 27 of 2022 concerning Personal Data Protection

Law enforcement in abstracto is carried out through the process of legislation / formulation / making laws and regulations. An integral criminal law enforcement system needs to be seen in abstracto (law making and law reform) because this form of law enforcement is the stage of making or formulating the formulation of legislative body laws (can be called tahao legislation). Law enforcement in abstracto is conceptualized in the form of efforts to tackle crime through the formation of criminal law rules that prohibit certain activities, which in the context of law enforcement are still in the form of formulations of rules (articles) that are used as a guide for the community not to commit prohibited acts¹⁶.

Law enforcement in concreto has an application stage (investigation) and the implementation stage of the law-by-law enforcement officials which can be called the judicial stage and the execution stage. In essence, law enforcement in concreto is the process of imposing punishment or the process of punishment, where the punishment process itself is the process of enforcing criminal law to uphold truth and justice. This law enforcement is also still influenced by the habit or culture of dirty games and shortcuts carried out by corrupt and collusive law enforcement officers with criminal offenders.

3. Factors affecting the effectiveness of law enforcement

¹⁶ Ali, Mahrus “Optimal Criminal Law Enforcement (Economic Analysis Perspective on Law)” LAW JOURNAL NO.2 VOL.15 APRIL 2008: 223 - 238

Some things that affect the effectiveness of law enforcement based on what Lawrence Friedmen said that the effectiveness of law enforcement is influenced by three things, namely the substance includes legal material which is outlined in the legislation, then for the legal structure regarding institutions or institutions for implementing the law, the authority of institutions and personal law enforcement officials, the last is the legal culture that concerns the legal behavior of the community.

These three elements influence the success of law enforcement in a society (state), which synergize with each other to achieve the goal of law enforcement itself, known as justice. In terms of substance or legal material, Indonesia is experiencing a shortage in the skills of lawmakers in determining how the legal material is.

a. Legal Substance

The substance of the law includes all statutory rules and legal materials that are compiled to regulate all behavior of society as well as ensure order. In Indonesia, the quality of legal substance is often a big problem that causes public dissatisfaction. For example, the DPR as a lawmaker has an important role in determining whether or not the legal products will be produced, but DPR members themselves come from diverse backgrounds and not all of them have a deep understanding of the law. As a result, the resulting legal products are always considered not to meet the needs of the community or even invite controversy.

b. Legal Structure

The legal structure involves institutions in charge of implementing and enforcing the law, such as the police, prosecutors, courts and various other institutions. The success of law enforcement is highly dependent on the integrity, performance and effectiveness of law enforcement officials. However, what happens in Indonesia is that many people think that the performance of this institution is still lacking because there are still many cases of bribery, corruption, and abuse of authority among police, prosecutors, and judges which clearly damage their image. This condition reduces public trust in law enforcement agencies and creates the view that the law is not fully reliable as a means of justice.

c. Legal Culture

Legal culture is a form of attitude, views and habits of society towards law. Legal culture is strongly influenced by people's tendency to shortcut rules for the sake of convenience. It often happens because legal procedures are considered too long and convoluted, so many choose a faster way even though it is not fully in accordance with the law. The legal culture in Indonesia is influenced by customary values, traditions, and people's outlook on life, which sometimes contradicts formal law, which results in many people feeling that there is no need to really follow these rules.

In law enforcement there are also things that become factors that cause the effectiveness of the occurrence, in this case conveyed by Soerjono Soekantor there are five things that become factors that greatly affect law

enforcement, namely, law, law enforcers, facilities and facilities, society and culture.

- 1) The legal factor that influences effectiveness is because the law has a very important role in society and not just as a parameter for justice, order, peace and order. Legal factors become the main issue in this case is certainty and justice. Basically, justice is an abstract formulation while legal certainty is a procedure that has been determined normatively, in its development the law is also interpreted as a means to promote the welfare of the community.
- 2) Cultural factors, namely as a result of copyright, work, and taste based on the human spirit in the association of life
- 3) Facility factors or facilities that support law enforcement
- 4) Community Factors, namely the environment where the law is applied
- 5) Law enforcement factors, namely those who apply and form legislation.

In terms of personal data protection, Indonesia can learn from other countries such as Singapore which has implemented the Personal Data Protection Act (PDPA) since 2012. The PDPA provides a clear and robust legal framework to address personal data breaches and further establishes a Personal Data Protection Commission (PDPC) with full authority to monitor compliance with the law.

On the other hand, in Indonesia, it is important to have an independent body that specifically oversees the protection of personal data, so it is worth considering

discussions to strengthen the role of the Information Commission as an organization that deals with personal data issues. The establishment of an independent body that specifically regulates and monitors the implementation of the Personal Data Protection Law (PDP Law) is very important.

As with Singapore, where the PDPC operates under the auspices of existing agencies, Indonesia needs to establish an independent law enforcement agency with full authority to protect personal data and ensure effective law enforcement. This is important not only to ensure legal certainty, but also to maintain the confidentiality and security of personal data, prevent data misuse, and build public trust in personal data management in Indonesia.

Indonesia has only recently begun to develop a legal and institutional framework for personal data protection. This dependency reduces independence as these institutions must follow broader government policies and guidelines.

F. Operational Definition

1. Personal Data Protection

Personal data is an important part of privacy, so protecting personal data is also an obligation that must be respected by the State.

2. Criminal Offence

Criminal offense is a series of acts that are prohibited by law and punishable by criminal sanctions.

3. Law Enforcement

Law enforcement in the context of Personal Data Protection (PDP) in Indonesia refers to actions to ensure compliance with Law No. 27 of 2022 concerning Personal

Data Protection (PDP Law). Law enforcement can be carried out by a wide range of subjects and can also be interpreted as law enforcement efforts by subjects in a limited sense.

G. Research Method

1. Type of Research

In this study, the type of research used by researchers is doctrinal legal research, namely legal research conducted by examining library documents or secondary data, also known as doctrinal research which often involves in-depth understanding and analysis of legal doctrine, where law is often conceptualized as “law written in legal regulations” (law in legal regulations). However, from a broader perspective, law can also be conceptualized as “rules or standards deemed appropriate for human conduct” In the context of doctrinal research, researchers tend to look at legal documents such as statutes, regulations, court decisions, and opinions of legal experts to understand and analyze the written law.

2. Research Approach

The research to be conducted is to analyze a problem regarding the protection of personal data, so the research approach method used is as follows:

a. Statutory approach

Basically, normative research uses a legislative approach because it is the various legal rules that guide research. The statutory approach is also used to examine existing laws and regulations.

b. Conceptual Approach

This conceptual approach departs from doctrines and views that develop in legal science. By understanding the views of doctrines in legal science, researchers will find legal notions, legal concepts and legal principles that are significant to the issues that occur. This research approach is carried out by combining practical concepts that can be implemented in one point of view and then the solution to the problems that have occurred.

c. Comparative approach

A comparative approach is an approach to comparing one country's law with another, in this study researchers compared state law in Indonesia with Singapore, in this case the comparison is the Regulation Between Personal Data Protection (PDP) Indonesia Year 2022 and Personal Data Protection Singapore (PDPA) Year 2012 in the Aspect of Criminal Offenses.

3. Object of Research

In this research, the object of research is the regulation of personal data protection in Indonesia and Singapore. This research also examines the differences between law enforcement agencies related to data protection in Indonesia and Singapore.

4. Research Data Source

This research uses secondary data in the form of legal opinions / doctrines / theories obtained from legal literature, research results, scientific articles, and websites related to research such as research journals, literature books and articles.

- a. Primary legal materials are laws and regulations and all official documents containing legal provisions. In this research, the primary legal materials used are Law Number 27 2022 concerning Personal Data Protection article 67 - 70 and PDPA (Personal Data Protection Act) 2012 Singapore part 10 article 51 – 52.
- b. Secondary legal material is legal material that provides an explanation of the primary legal material. In this research, secondary legal materials are research results, journals, books, theses, theses and dissertations.

c. Data Collection Techniques

The data collection techniques used in this research are literature study, document study.

1. Literature study is a technique of collecting data and information by conducting library reviews and reading literature books, journals, articles, magazines, and report results related to the research conducted.
2. Document study is a form of record of past events. These documents can be in the form of pictures, writings or historical works of a person.¹⁷

5. Data analysis

The data analysis used in this research is carried out in a qualitative form, explaining with descriptive sentences. Identify and collect all relevant laws and regulations regarding personal data protection in delivery services. This includes the Personal Data Protection Act, any additional regulations that may be

¹⁷ Sugiyono. 2018. Quantitative, Qualitative, and R&D Research Methods, publisher. Alfabeta, Bandung. Dharmayana, I. M. A., & Rahanatha, G. B. (2017).

relevant, such as e-commerce regulations or regulations governing the delivery service industry.

This research will provide insights into the text of these regulations, including their terms, definitions and scope, as well as how they apply in the context of the use of personal data in service delivery.

H. Thesis Framework

In this framework section, the author aims to provide a clearer picture of this research. In this study, researchers divided it into three parts

1. CHAPTER I INTRODUCTION

In this CHAPTER is the introduction. There is a background of the problem, the formulation of the problem, the purpose of the research, why the author raises the issue that exists then made in the form of research.

2. CHAPTER II OVERVIEW

This chapter contains a theoretical framework which includes a clearer explanation of the research problem, namely legal protection and personal data.

3. CHAPTER III Data and Analysis

This chapter contains the results of research that has been conducted by researchers, as well as a discussion of the research results obtained.

4. CHAPTER IV CLOSING

CHAPTER IV is a cover that contains conclusions and suggestions for future research.