Protection and Legal Liability for Misuse of Personal Data Along with the Development of Technology

Tamara Prima Nathania[1], Arista Candra Irawati[2]
Universitas Ngudi Waluyo[1,2]
Email Correspondance: tamaraprimanathania16@gmail.com

Abstract. Personal data protection is one part of personal rights that must be protected and there are threats of sanctions for anyone who violates personal data. The protection ofpersonal data and the threat of sanctions have been regulated in Law No. 19 of 2016 concerning amendments to Law No. 11 of 2008 concerning Electronic Information and Transactions and Law No. 27 of 2022 concerning Personal Data Protection. The purpose of this study is to analyze the form of legal protection of personal data and legalliability for misuse of personal data. The method used in this research is the normative juridical approach method. This research shows that the protection of personal data has been regulated in legislation. However, Law No. 19 of 2016 concerning amendments to Law No. 11 of 2008 concerning Electronic Information and Transactions has not made real and explicit privacy data protection regulations, therefore the government has passed Law No. 27 of 2022 concerning Personal Data Protection to regulate the protection of personal data specifically.

Keywords: Protection, Misuse, Personal Data

Introduction

Indonesia has now entered the Industrial Revolution 4.0. Everything can be controlled from any place through the internet and interconnected devices. The implications of this era are enormous when digital-based technology is used by the community in everyday life, for example to increase work productivity, build socio- economic relationships, and help facilitate various things. The development of computer-based information communication technology has grown very rapidly, the community is then facilitated by the development of this technology. Advances in information technology, especially in the field of social networking, have proven to have a positive impact on the progress of human life. Behind the advantages and conveniences offered by this technological advancement, it also has a negative impact that can destroy human life and culture itself. One of them is the leakage of technology user data. Crimes committed due to the development of technology and information are also called *cyber crime*. Various cases related to *cyber crime* are online gambling, online fraud, *illegal access*, misuse of personal data, etc.

The utilization of technology and information can be beneficial both in the fields of education and economy and others, matters relating to the development of science, science and so on that can be easily accessed, so that billions and even trillions of information can be received quickly. In the field of work, the management of a very large amount of data can be managed properly, quickly, effectively and efficiently and minimize errors. In the economic field, promotions and potentials in improving the welfare of society are carried out quickly without restrictions on place or region and reach all levels of society both nationally and internationally (Situmeang, 2021). However, the development of technology and information not only provides benefits but also causes problems that can harm the community, such as data misuse, theft of personal data, sale of personal data, fraud and others. Information has been considered as "power" which is defined as strength and power that determines the fate of humans themselves. Currently, people's dependence on information technology is getting higher, so the risksfaced are also getting higher (Rumlus, 2020).

Business actors or electronic system providers can collect personal data from customers or prospective customers offline or online, where digital data can be traded without the knowledge and permission of the data owner or misused (for purposes outside the provision, submission of digital personal data), it can also happen that connected personal data is hijacked, stolen (*hacked*) by third parties. Indonesia is the country with the most social media users in the world. With the 4th most under China, India, and the United States. In Indonesia, there are approximately 150 million active social media users. With such a large number, understanding the privacy policy of a social media platform is very important so that personal data is safe. One of therequirements for using social media requires valid personal data. With the rise of Indonesian social media users, it cannot be denied that there are many cases ofleakage of users' personal data.

According to data from the Indonesian National Police, there is an average of 1,409 fraud

cases per year due to leaks of personal data of social media users (Pertiwi, 2021). In connection with the search in the field, it is known that there is a leak of personal data from BPJS Health reaching 279 million, Bukalapak in 2020, leakage or misuse of NIK (Population Identification Number) and also Tokopedia (Nurmalasari, 2021). Information technology activities can be utilized to disseminate and search for data that is useful for various daily activities. This activity cannot take place if it is not supported by a telecommunications system, so the internet has become a special problem since it is used in trade or business activities known as *e-commerce* transactions.

An *e-commerce* sale and purchase transaction is a sale and purchase contract thatis the same as buying and selling that is usually done by the community. It's just that in *e-commerce* transactions, the media used is electronic media, namely the internet. So that the agreement or contract created is through online where long-distance communication, anywhere, anyone, and from anywhere can access the website (Primata, 2020). Various sites that have been provided both from the government and the private sector are used by the community to trade all kinds of things that have selling value. Along with changes in the lifestyle of people who are currently dominated by information technology users, they demand a fast-paced life.

In addition to *e-commerce*, a person's personal data is also often used on existing social media. The rapid development of social media is characterized by the emergenceof various kinds of social media such as *Facebook*, *Twitter*, *Instagram*, *Line* and so on. Social media provides convenience in communicating and interacting between its users without having to be face-to- face which is not limited by space and time. Amid the widespread use of social media, user information on social media can be easily obtained including user personal data information and other things that are private. This can certainly trigger the misuse of personal data. This can happen if the owner of personal data feels that the personal data listed or included in his social media is used by other parties without his permission for purposes that are considered disturbing, self- beneficial, dangerous or threatening to others which will certainly cause harm to the data owner.

The availability of trade fields and the high needs of a person, make them legalize all means or legalize all things that are contrary to the law, but which they think aregood and earn. One of them that is currently happening is the illegal buying and selling of other people's personaldata even at a low price. A social media account offers to buy data on the Population Identification Number (NIK) and Family Card (KK), personal data is considered a gold mine because with this personal data we can know someone's identity and habits. According to Jerry Kang, personal data describes information that is closely related to a person that can distinguish the characteristics of each person. Data can be said to be personal data if the data can be used to recognize or identify a person (Saragih, 2020). These personal data include cell phone numbers, full names, full addresses, relative numbers, KK numbers and KTP numbers to KTP photos and selfies of someonespread on social media.

With the misuse of personal data, it can be seen that there is a weakness in the system, lack of supervision, so that personal data can be misused and cause harm to the owner of the data. The negative consequences of weak protection of personal data include unlawful misuse of personal data and information, theft of personal data and information to commit other crimes, forgery in its various dimensions, difficulties in handling and proving crimes, and the emergence of difficulties in tracking, investigating, investigating, prosecuting and proving crimes (Aprilia, 2017). The misuse, theft, sale of personal data is a violation of the law in the field of information technology and can also be categorized as a violation of human rights, because personal data is part of human rights that must be protected. Personal data protection is a form of privacy protection mandated directly by the Constitution of the Republic of Indonesia which contains respect for human rightsvalues and respect for individual rights so that it is necessary to provide a legal basis to further provide privacy and personal data security. It can be understood that personal data relates to an individual's life and is also closely related to the concept of confidentiality or one's right to privacy that must be maintained and protected by laws and regulations, hence the need for legal certainty to protect this. In Indonesia, the protection of personal data has been regulated in Law Number 27 of 2022 concerning Personal Data Protection and Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions.

This article will discuss the types of personal data that must be protected, the legal protection of people's personal data, and this article will discuss the legal liabilityobtained by perpetrators of criminal acts of personal data abuse based on Law Number 27 of 2022 concerning Personal Data Protection and Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions. Due to the lack of articles discussing

personal data protection based on Law Number 27 of 2022 concerning Personal Data Protection because the law was passed in October 2022 and is a relatively new regulation, this article will also look at the effectiveness of Law Number 27 of 2022 concerning Personal Data Protection. Through this research, it is hoped that people can be more careful in usingpersonal data on social media and in other applications. People are also expected to know how important their personal data is and the dangers if their personal data falls to the wrong people. People can also understand what to do to protect their personal data and understand what to do if there is misuse of personal data. Through this research, we can also understand the penalties that can be imposed on perpetrators of criminal acts of personal data abuse.

Methods

The approach method used in this research is the Normative Juridical approach method. Normative juridical research method is a library legal research conducted by examining library materials. This research is conducted in order to obtain materials in the form of theories, concepts, legal principles and legal regulations related to the subject matter. The scope of this research will be carried out by interpreting laws and regulations relating to the protection and misuse of personal data. In this method it is also necessary to collect relevant legal materials to be taken into consideration in examining a problem formulation arising from legal issues so as to provide a legal research related to sanctions to be given to perpetrators of personal data abuse.

Discussion

Types of Personal Data and Legal Protection of Personal Data

Personal data is the data of a particular individual that is stored, maintained, and kept true and protected by confidentiality. Personal data protection is one of the human rights which is part of personal protection. Data can be said to be personal data if the data can be used to recognize or identify a person. In Law No. 27 of 2022 concerning Personal Data Protection, it is stated that what is meant by personal data is data about an identified or identifiable individual individually or in combination with other information, either directly or indirectly through electronic or non-electronic systems. Referring to Article 4 of Law No. 27 of 2022 on Personal Data Protection, there are at least two types of personal data, namely, specific data and general data.

Specific personal data includes (Law No. 27 of 2022 on Personal Data Protection):

a. Health data and information
b. Biometric data
c. Genetic data
d. Criminal record
e. Child Data
f. Personal financial data
g. Other data in accordance with the provisions of laws and regulation

General Personal Data includes (Law No. 27 of 2022 on Personal Data Protection):

a. Full Name
b. Gender
c. Citizenship
d. Religion
e. Marital Status
f. Personal Data that is combined to identify an individual

The owner of personal data is an individual as the data subject who has personal data attached to him. So everyone who has personal data is a personal data owner.The owner of personal data also has several rights, here are the rights owned by the owner:

1. Obtain information about the clarity of identity, the basis of legal interests, the purpose of the request and use of Personal Data, and the accountability of the party requesting personal data.
2. Completing, updating and/or correcting errors and/or inaccuracies in personal data about him/her in accordance with the purposes of processing personal data
3. Get access to and obtain a copy of personal data about himself in accordance with the
4. provisions of laws and regulations
5. End the processing of personal data concerning him/her that has been provided to the personal data controller.
6. Object to decision-making measures based solely on automated processing, including

profiling, that give rise to legal consequences or have a significant impact on the personal data subject.

7. Delay or restrict the processing of personal data in a manner proportionate to the purposes for which the personal data are processed
8. Use and receive compensation for violations of the processing of personal data about him in accordance with the provisions of laws and regulations
9. Obtain and/or use personal data about him/her from the personal data controller in a form that is in accordance with the structure and/or format commonly used orreadable by electronic systems.
10. Use and transmit personal data about themselves to other personal data controllers, provided that the systems used can communicate with each other securely in accordance with the principles of personal data protection.

While there are rights of personal data owners that are protected by laws and regulations, there are some rights that do not apply to the following interests:

1. National defense and security interests
2. The interests of the law enforcement process
3. Public interest in the framework of state administration
4. The interests of supervision of the financial services sector, monetary, payment systems, and financial system stability carried out in the context of state administration
5. Statistical and scientific research purposes

In carrying out the processing of personal data, the personal data controller shall comply with the following provisions:

Data controllers shall have a basis for processing personal data which includes:

a. Explicit valid consent of the personal data subject for 1 or more specified purposes that has been communicated by the personal data controller to the personal data subject;
b. Fulfillment of an agreement obligation in the event that the personal data subject is one of the parties or to fulfill the request of the personal data subject at the time of entering into an agreement;
c. Fulfillment of legal obligations of the controller of personal data in accordance with the provisions of laws and regulations;
d. Fulfillment of the protection of the vital interests of personal data subjects;
e. Implementation of tasks in the context of public interest, public services, or implementation of the authority of personal data controllers based on laws and regulations; and/or
f. Fulfillment of other legitimate interests by taking into account the purposes, needs and balancing interests of the personal data controller and the rights ofthe personal data subject.

In the case of processing personal data based on consent, the personal data controller shall provide information regarding:

a. Legality of personal data processing;
b. Purpose of processing personal data;
c. Type and relevance of personal data to be processed;
d. Retention period of documents containing personal data;
e. Details on the information collected;
f. The period of processing of personal data; and
g. Rights of personal data subjects

Agreement clauses in which there is a request for processing of personal data that does not contain the explicit valid consent of the personal data subject are declared null and void.

1. In carrying out the processing of personal data, the personal data controller shall be obliged to show proof of the consent that has been given by the personal datasubject;
2. Personal data controllers shall conduct limited and specific, lawful and transparent processing of personal data;
3. The controller of personal data shall carry out the processing of personal data in accordance with the purpose of the processing of personal data;
4. Personal data controllers shall ensure the accuracy, completeness and consistency of personal data in accordance with the provisions of laws and regulations;
5. The personal data controller shall record all personal data processing activities;
6. The controller of personal data shall provide the personal data subject with access to the personal data processed as well as a track record of the processing of the personal data in accordance with the period of retention of the personal data;

7. In conducting personal data processing, the personal data controller shall maintain the confidentiality of personal data;
8. The personal data controller shall supervise any party involved in the processing of personal data under the control of the personal data controller;
9. The controller of personal data shall protect personal data from unauthorized processing;
10. Personal data controllers shall prevent personal data from being accessed unlawfully;
11. The controller of personal data shall be responsible for the processing of personal data and demonstrate accountability in fulfilling the obligation to implement the principles of personal data protection.
12. The personal data controller shall protect and ensure the security of the personal data it processes, by:
    a. the preparation and implementation of technical operational measures to protect personal data from interference with personal data processing contrary to the provisions of laws and regulations; and
    b. determination of the security level of personal data by taking into account the nature and risks of the personal data to be protected in the processing of personal data.

Personal data protection is the specific protection of how the law protects how personal data is collected, registered, stored, exploited and disseminated. Personaldata protection is aimed at guaranteeing citizens' rights to personal protection and fostering public awareness and ensuring recognition and respect for the importance of personal data protection. In the utilization of Information Technology, personal data protection is one part of *privacy rights*. Personal rights contain the following meanings (Saragih, 2020):

Personal rights are the right to enjoy a private life and be free from all kinds of interference;

1. The right to privacy is the right to be able to communicate with others without spying;
2. The right to privacy is the right to control access to information about one's private life and data.

Furthermore, *privacy rights* in *cyberspace* include 3 (three) aspects that need to be considered, namely (Saragih, 2020):

1. Recognition of a person's right to enjoy their private life and be free fromharassment;
2. The right to communicate with others without surveillance (spying on others);and
3. The right to be able to monitor and control their personal information that can be accessed by others.

The right to protection of personal data develops from the right to respect for private life or "the right to private life". The concept of private life relates to humans as living beings. Thus, the individual is the main owner of the right to personal data protection. Personal data protection is a form of privacy protection mandated directly by the Constitution of the Republic of Indonesia which contains respect for human rightsvalues and respect for individual rights so that it is necessary to provide a legal basis to further provide privacy and personal data security.

The 1945 Constitution includes 40 citizen rights. One of them is the right topersonal protection. This right is regulated in Article 28 G Paragraph (1) with the outline that citizens are entitled to the protection of themselves, their families, honor, dignity and property under their control. The article assumes that personal rights are property rights. However, with the development of information and communication technology, personal rights should not only be defined as property rights. Personal rights should also be the right to privacy (Kusnadi, 2021). The right to privacy is a more sensitive right that can represent personal rights. Personal rights are sensitive matters relating to a person's personal data or identity.

In addition to the 1945 Constitution, the protection of personal data has also been stated in several laws and regulations, among others (Situmeang, 2020):

Article 1 numbers 1 and 2 of the Minister of Communication and Information Technology Regulation No. 20 of 2016 concerning Personal Data Protection in Electronic Systems states that personal data is intended as a person's clear and clear identity which is a determination of personal evidence against him which is maintained, kept correct and placed safely in confidentiality. Meanwhile, Article 2 number 1 regulates the acquisition, collection, processing, analyzing, storing, displaying, announcing, sending, disseminating and destroying personal data, which is the protection of personal data in electronic systems that respect personal data as privacy.

Article 1 number 27 of Government Regulation No. 82/2012 on the Implementation of Electronic Systems and Transactions, defines personal data as certain individual data that is stored

and kept correct and protected confidential.

In addition to the above laws and regulations, personal data protection is also regulated in several articles in Law No. 19 of 2016 concerning amendments to Law No. 11 of 2008 concerning Electronic Information and Transactions. Article 4 of the ITE Law states the purpose of this law. Article 4 reads as follows: "The utilization of Information Technology and Electronic Transactions is carried out with the aim of:

a. To educate the nation as part of the world information society;
b. Develop trade and the national economy in order to improve people's welfare;
c. Improve the effectiveness and efficiency of public services;
d. Open the widest possible opportunity for everyone to advance their thoughts and abilities in the field of the use and utilization of Information Technology asoptimally as possible and responsibly; and
e. Provide a sense of security, justice, and legal certainty for users and organizers of Information Technology."

The purpose contained in letter e in the article shows that the government wants to provide a sense of security for all users of information technology. So that information technology users can feel safe, including in the protection of their personal data, because the government has guaranteed security, justice and legal certainty as statedin the article. Then Article 26 reads as follows (Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions):

1. Unless otherwise provided by laws and regulations, the use of any information through electronic media concerning a person's personal data must be done withthe consent of the person concerned.
2. Any person whose rights are violated as referred to in paragraph (1) may file a lawsuit for losses incurred under this Act.
3. Every Electronic System Operator must delete irrelevant Electronic Information and/or Electronic Documents under its control at the request of the personconcerned based on a court order.
4. Every Electronic System Operator must provide a mechanism for deleting Electronic Information and/or Electronic Documents that are no longer relevant in accordance with the provisions of laws and regulations.
5. Provisions regarding the procedures for deleting Electronic Information and/or Electronic Documents as referred to in paragraph (3) and paragraph (4) shall be regulated in a government regulation.

Paragraph 1 of the article explains that the use of personal data must be done withthe consent of the data owner. The Minister of Communication and Information Regulation on Personal Data Protection in Electronic Systems Article 2 paragraph (3) contains a normative definition of personal rights or privacy, namely: "Privacy as referred to in paragraph (2) letter a is the freedom of the Personal Data Owner to declare the secret or not to declare the secret of his Personal Data, unless otherwise determined in accordance with statutory regulations". From the article above, it can be said that Privacy is a person's right to open or not open their Personal Data to the public. This means that the Personal Data Owner has full control over their personal data (Saragih, 2020).

In Law No. 27 of 2022 concerning Personal Data Protection, personal data that is regulated is not only of a general nature that can be known to the public in the form of full name, gender, nationality, or religion, or other Personal Data combined so that it is possible to identify a person, sensitive personal data is also accommodated for protection which requires special protection. Such data relates to health data, biometric data, namely data relating to the physical, physiological or behavioral characteristics of individuals, genetic data, sexual life, political views, personal financial data, educational data, and other personal data and information that may be harmful and detrimental to the privacy of data owners.

In Law No. 27 of 2022 on Personal Data Protection, there are personal data controllers and personal data processors. A personal data controller is any person, public body, and international organization acting singly or jointly in determining the purposes and exercising control over the processing of personal data. And a personal data processor is any person, public body and international organization acting singly or jointly in carrying out personal data processing on behalf of a personal data controller.

Personal data controllers and personal data processors must appoint an official or officer who carries out the personal data protection function in the event that (Law No. 27 of 2022 on

Personal Data Protection):

a. Processing of personal data for the purposes of public services;
b. The core activities of the personal data controller have a nature, scope and/or purpose that requires regular and systematic monitoring of personal data on a large scale; and
c. The core activities of a personal data controller consist of large-scale processing of personal data for specific personal data and/or personal data relating tocriminal offenses.

Officials or officers performing personal data protection functions are appointed based on professionalism, knowledge of the law, personal data protection practices, and ability to fulfill their duties. The official or officer who carries out the function of personal data protection is in charge of at least:

a. Inform and advise personal data controllers or personal data processors tocomply with the provisions of the PDP Law;
b. Monitor and ensure compliance with the PDP Law and the policies of thepersonal data controller or personal data processor;
c. Advising on personal data protection impact assessments and monitoring the performance of personal data controllers and personal data processors; and
d. Coordinate and act as a contact person for issues related to personal data processing.

Legal Liability for Criminal Acts of Misuse of Personal Data

The protection of *privacy rights is* closely related to the protection of one's personal data (personal data) because currently the development of technology in the internet world has progressed so much that people can access one's personal data without the knowledge of the party concerned. The possibility of violating one's personal rights is very high. In the realm of criminal law, it is understood that in computer networks such as the internet, the problem of criminality becomes increasingly complex due to its broad scope. Internet criminality (*cyber crime*) is basically a criminal act that occurs in cyberspace, either oppressing community facilities or a person's ownership (private). The government ensures the application of sanctions for the misuse of personal data by third parties without rights and guarantees the protection of personal data in the virtual world. Legal liability for criminal acts of misuse of personal data is regulated in laws and regulations, including Law No. 19/2016 on Amendments to Law No. 11/2008 on Electronic Information and Transactions and Law No. 27/2022 on Personal Data Protection.

The elaboration of personal electronic data is further mandated by Law Number 19 of 2016 on the Amendment to Law Number 11 of 2008 on Electronic Information and Transactions, the protection of personal data in an electronic system includes protection from unauthorized use, protection by electronic system providers, and protection from illegal access and interference (Primanta, 2020). Regarding the protection of personal data from unauthorized use, Article 26 of Law Number 19 of 2016 on the Amendment to Law Number 11 of 2008 on Electronic Information and Transactions. Requires that the useof any personal data in an electronic media must obtain the consent of the data owner concerned. Any person who violates this provision can be sued for losses incurred.

Law No. 19/2016 on the Amendment to Law No. 11/2008 on Electronic Information and Transactions actually comprehensively contains provisions that regulate how data protection is provided to individuals, legal entities, and the government. ITE Law expressly prohibits unlawful access to data belonging to other people through electronic systems to obtain information by bypassing security systems. ITE Law explicitly states that *interception* is a prohibited act unless it is carried out by a party who has the authority to do so in the context of legal efforts. Based on Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, everyone is prohibited by any means from disclosing information belonging to other people for any purpose, even if the data is confidential until it can be opened to the public.

The involvement of many parties, both organizers and fellow users, is one form of electronic information and transaction activity, which cannot be avoided from these activities, it also does not rule out the possibility of fraud which has the potential for unwanted actions. One of them is the act of misuse of personal data by fellow users. Such actions are certainly prohibited and avoided by the parties involved, both electronic system organizers, data owners, or the state as the formulator of rules where it can run well as it should (Agustina, 2021).

The threat of sanctions against perpetrators of criminal acts of misuse of personal data is listed in several articles in Law Number 19 of 2016 concerning Amendments to Law Number 11 of

2008 concerning Electronic Information and Transactions. Article 30 of Law Number 19 of 2016 on the amendment to Law Number 11 of 2008 on Electronic Information and Transactions regarding illegal access reads (Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions):

1. Article 30 paragraph (1): "Every person intentionally and without right or unlawfully accesses another person's Computer and/or Electronic System by anymeans."
2. Article 30 paragraph (2): "Every person intentionally and without right or unlawfully accesses a Computer and/or Electronic System by any means for the purpose of obtaining Electronic Information and/or Electronic Documents."
3. Article 30 paragraph (3): "Every person intentionally and without right or unlawfully accesses a Computer and/or Electronic System in any way by violating, breaking through, exceeding, or breaching the security system."

The content in article 46 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions regarding criminal sanctions based on article 30, reads:

1. Article 46 paragraph (1): "Every person who fulfills the elements as referred to in Article 30 paragraph (1) shall be punished with a maximum imprisonment of 6 (six) years and/or a maximum fine of Rp 600,000,000.00 (six hundred million rupiah).
2. Article 46 paragraph (2): "Every person who fulfills the elements as referred to in Article 30 paragraph (2) shall be punished with a maximum imprisonment of 7 (seven) years and/or a maximum fine of Rp 700,000,000.00 (seven hundred million rupiah).
3. Article 46 paragraph (3): "Every person who fulfills the elements as referred to in Article 30 paragraph (3) shall be punished with a maximum imprisonment of 8 (eight) years and/or a maximum fine of Rp 800,000,000.00 (eight hundred millionrupiah).

In addition to the acts of illegal (unauthorized) access as mentioned above, this law also regulates the prohibition of the types of data misappropriation that can potentially be carried out by fellow users against other users turning into public data. Contents in article 32 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions):

1. Article 32 paragraph (1): "Every person intentionally and without right or unlawfully by any means alters, adds, reduces, transmits, damages, removes, moves, hides electronic information and/or electronic documents belonging to another person or to the public."
2. Article 32 paragraph (2): "Every person intentionally and without right or unlawfully
3. by any means moves or transfers electronic information and/or electronic documents to the electronic system of another person who is not entitled." Article 32 paragraph (3): "Against the act as referred to in paragraph (1) which results in the disclosure of electronic information and/or electronic documents that are confidential to be accessible to the public with data integrity that is not asit should be." The content in article 48 of Law Number 19 of 2016 concerning Amendments to Law
4. Number 11 of 2008 concerning Electronic Information and Transactions regarding criminal sanctions based on article 32, reads (Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions):
    1. Article 48 paragraph (1): "Any person who fulfills the elements as referred to in Article 32 paragraph (1) shall be punished with 8 (eight) years imprisonment and/or a maximum fine of Rp. 2,000,000,000,- (two billion rupiah)."
    2. Article 48 paragraph (2): "Any person who fulfills the elements as referred to in Article 32 paragraph (2) shall be punished with imprisonment of 9 (nine) years and/or a maximum fine of Rp. 3,000,000,000,- (three billion rupiah)."
    3. Article 48 paragraph (3): "Any person who fulfills the elements as referred to in Article 32 paragraph (3) shall be punished with imprisonment of 10 (ten) years and/or a maximum fine of Rp. 5,000,000,000,- (five billion rupiah)."

Protection of data does not only regulate access to data opening, but also when data can be opened and changed in any way such as manipulation, alteration, removal, destruction, so that it appears as if the data is authentic data. Apart from actions directly related to *unlawful access* to data, Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions also states that it prohibits any action that causes electronic systems to be disrupted, which systematically means that it can also result in disruption of data access for

the owner. Data protection here is not only about the freedom of data to be open in any way and forany purpose without the consent of the data owner, but data protection also means securing the electronic system where data is stored and used so that it can run properly (Primanta, 2020).

In general, the regulation of privacy data protection contained in Law Number 19 of 2016 amending Law Number 11 of 2008 concerning Electronic Information and Transactions, but this law has not yet made real and explicit privacy data protection regulations. Although this law creates regulations that protect electronic data or information, both public and private. The protection of personal data in an electronic system in Law Number 19 of 2016 concerning Electronic Information and Transactions includes protection from unauthorized use, protection by electronic system providers, and protection from illegal access and intervention. Therefore, the Indonesian government has sought the protection of personal data by passing Law No. 27 of 2022 on Personal Data Protection.

Law No. 27 of 2022 on Personal Data Protection contains rules such as protection of citizens' fundamental rights, strengthening the government's authority in monitoring parties that process data, a legal umbrella for personal data protection, balancing the rights of personal data subjects with the obligations of data controllers, encouraging reform of data processing practices in all personal data controllers, providing protection to vulnerable groups, especially children and people with disabilities, and opportunities to improve industry standards.

The scope of the PDP Law applies to the processing of personal data by natural persons, corporations, public bodies, and international organizations. However, it does not apply to the processing of personal data by natural persons in private or household activities. For people who have been concerned about the leakage of personal datasuch as cellular numbers, the presence of the PDP Law certainly provides constitutional rights for every citizen to have sovereignty over personal data attached to each individual. Thus, forms of personal data abuse that often disturb the community can/should be reduced, such as the use of other people's personal data, namely NIK to illegal online lending platforms (pinjol) or the dissemination of one's personal data for negative purposes (doxing).

The scope of personal data processing includes activities related to personal data such as acquisition and collection; processing and analysis; storage; correction and updating; display, announcement, transfer, dissemination, or disclosure; and/or erasure or destruction. The basic implication of Law No. 27 of 2022 on Personal Data Protection is that the processing of personal data must be carried out in accordance with the principles of personal data protection (Erdisy, 2020).

These principles include, among others, that the collection of personal data is limited and specific, lawful, and transparent; the processing of personal data is carried out in accordance with its purpose; the processing of personal data is carried out by guaranteeing the rights of personal data subjects; the processing of personal data is accurate, complete, not misleading, up-to-date, and accountable; the processing of personal data is carried out by protecting the security of personal data from unauthorized access, unauthorized disclosure, unauthorized alteration, misuse, destruction, and/or erasure of Personal Data. Processing of Personal Data is carried outby informing the purposes and activities of the processing, as well as the failure of Personal Data Protection; Personal Data is destroyed and/or erased after the end of the retention period or upon request of the Personal Data Subject, unless otherwise provided by laws and regulations; and processing of Personal Data is carried out responsibly and can be clearly proven.

In the governance of the use of personal data, there are two things that need to be considered, namely the personal *data controller* and the personal data processor. Article 1 point 5 of the PDP Law states that the Personal Data Controller is every person, public body, and international organization that acts individually or jointly in determining the purpose and controlling the processing of Personal Data. This means that the personal data controller is obliged to fulfill, collect, and approve the use of personal data to data users so that personal data processing is carried out based on the provisions stipulated in the PDP Law and the principles of personal data protection. This Personal Data Controller is then obliged to maintain the confidentiality of personal user data and inform data users in the event of leaks, violations and other matters related to the use of one's personal data.

Personal data failure is a failure to protect one's Personal Data in terms of confidentiality, integrity, and availability of Personal Data, including intentional, or unintentional, security breaches that lead to damage, loss, alteration of disclosure, or unauthorized access to Personal Data. Based on the provisions of Article 46 paragraph 3, if the failure of personal data protection interferes with the public interest, the personal data controller shall notify the public of the failure of personal data protection.

Meanwhile, a Personal Data Processor is any person, public body, and international organization acting individually or jointly in the processing of Personal Data on behalf of the Personal Data Controller. So in this case, a personal data processor is a party that performs personal data processing appointed by a personal data controller. Where the processing of personal data must be in accordance with the principles of personal data protection. The obligations of the processor are also stipulated in Articles 51 to 52 that the processing of personal data must first obtain written consent from the personal data controller and its implementation is based on the orders of the personal data controller. The PDP Law also regulates the rights of personal data subjects (*data owners*), which in this case is each individual as the owner of personal data.

Broadly speaking, Law Number 27 Year 2022 on Personal Data Protection regulates the Personal Data Protection Institution (PDP). In addition, it also regulates sanctions or penalties for violations of the PDP Law. Sanctions apply to electronic system operators (PSE), both government (public) and private (private), individuals, and corporations. Mentioned, Law Number 27 of 2022 concerning Personal Data Protection mandates the establishment of a PDP Institution under the president and is responsible to the president. The PDP Institution is regulated in Articles 58 and 60 of the PDP Law. The PDP Institute has a number of functions and tasks, including formulating and determining PDP policies and strategies, supervising the implementation of PDP, enforcing administrative law against violations of the PDP Law, and facilitating *out of court* dispute resolution related to personal data protection in the digital realm.

In the PDP Law, there are two types of sanctions for violators of personal data. The first type is for controllers or processors of personal data if they violate the provisions of the PDP Law. Among other things, not processing personal data according to its purpose and not preventing unauthorized data access. Legal sanctions consist of four types, namely first, administrative sanctions in Article 57 of the PDP Law in the form of written warnings; second, temporary suspension of personal data processing activities; third, deletion or destruction of personal data; and / or fourth, administrative fines / a maximum of two percent of annual revenue or annual revenue on the violation variable.

The second type is for individuals or corporations that commit prohibited acts. Among others, collecting personal data that does not belong to them to benefit themselves or others, disclosing personal data that does not belong to them, and falsifying personal data for profit that results in harm to others can be subject to Articles 67 through 73 of Law Number 27 Year 2022 on Personal Data Protection. Law No. 27of 2022 on Personal Data Protection is also classified as a strict personal data protection regulation that regulates prohibitions and criminal provisions that are quite severe.

Law No. 27 of 2022 on Personal Data Protection includes criminal penalties for prohibited acts in the use of personal data, such as stealing, disseminating, using personal data that does not belong to them, including falsification of personal data. The following are some articles that regulate the prohibition of the use of personal data and the penalties for violating personal data.

Article 65 of Law No. 27 of 2022 on Personal Data Protection regarding prohibitions on the use of personal data (Law No. 27 of 2022 on Personal Data Protection):

1. Article 65 paragraph (1): "Every Person is prohibited from unlawfully obtaining or collecting Personal Data that does not belong to him/her with the intention to benefit himself/herself or others which may result in the harm of the Personal Data Subject."
2. Article 65 paragraph (2): "Every Person is prohibited from unlawfully disclosing Personal Data that does not belong to them."
3. Article 65 paragraph (3): "Every Person is prohibited from unlawfully using Personal Data that does not belong to them."

Article 66 of Law No. 27 of 2022 on Personal Data Protection regarding prohibitions on the use of personal data (Law No. 27 of 2022 on Personal Data Protection):

"Every Person is prohibited from creating false Personal Data or falsifying Personal Data with the intention to benefit themselves or others which may result in harm to others."

Article 67 of Law No. 27 of 2022 on Personal Data Protection regarding penalties for violations of personal data (Law No. 27 of 2022 on Personal Data Protection):

1. Article 67 paragraph (1): "Any Person who intentionally and unlawfully obtains or collects Personal Data that does not belong to him/her with the intent to benefit himself/herself or another person which may result in harm to the Personal Data Subject as referred to in Article 65 paragraph (1) shall be punished with amaximum imprisonment of 5 (five) years and/or a maximum fine of Rp 5,000,000,000.00 (five billion rupiah)."

2. Article 67 paragraph (2): "Every person who intentionally and unlawfully discloses Personal Data that does not belong to him as referred to in Article 65 paragraph shall be punished with a maximum imprisonment of 4 (four) years and/or a maximum fine of Rp 4,000,000,000.00 (four billion rupiah)."
3. Article 67 paragraph (3): "Every person who intentionally and unlawfully uses Personal Data that does not belong to him as referred to in Article 65 paragraph shall be punished with a maximum imprisonment of Rp 5,000,000,000.00 (five billion rupiah)."

Article 68 of Law No. 27 of 2022 on Personal Data Protection regarding penalties for violations of personal data:

"Any Person who intentionally creates false Personal Data or falsifies Personal Data with the intent to benefit themselves or others which may result in harm to others as referred to in Article 66 shall be punished with a maximum imprisonment of 6 (six) years and/or a maximum fine of Rp 6,000,000,000.00 (six billion rupiah)."

In addition to the punishment as referred to in Article 67 and Article 68, additional punishment may also be imposed in the form of confiscation of profits and/or assets obtained or resulting from criminal acts and payment of compensation.[31] In the event that the criminal offense as referred to in Article 67 and Article 68 is committed by a Corporation, the punishment may be imposed on the management, controllers, commanders, beneficial owners, and/or the Corporation. The punishment that can be imposed on the Corporation is only a fine. The fine imposed on the Corporation is a maximum of 10 (ten) times the maximum fine imposed. In addition to being sentencedto a fine, the Corporation may be sentenced to additional punishment in the form of:

a. Forfeiture of profits and/or assets obtained or resulting from a criminal offense
b. Suspension of all or part of the Corporation's business
c. Permanent prohibition of certain acts
d. Closure of all or part of the place of business and / or activities of the Corporation
e. Carry out obligations that have been neglected
f. Payment of compensation
g. License revocation
h. Dissolution of Corporation

The key to the effective implementation of the PDP Law lies in the authority of the data protection institution, which of course has independence as a supervisory, administrative law enforcement and dispute facilitation institution that will ensure compliance in the processing of personal data and guarantee the fulfillment of the rightsof personal data subjects.

Moreover, the PDP Law applies bindingly not only to corporations or the private sector, but also public bodies (ministries/agencies) andinternational organizations.

Conclusion

Personal data is the data of a particular individual that is stored, maintained, and kept correct and protected from confidentiality. Based on Article 4 of Law No. 27 of 2022 on Personal Data Protection, there are two types of personal data, namely, specific data and general data. Specific personal data includes health data and information, biometric data, genetic data, crime records, child data, personal financial data, other data in accordance with the provisions of laws and regulations. Meanwhile, general personal data includes full name, gender, nationality, religion, marital status, personal data combined to identify a person.

Personal data protection is the specific protection of how the law protects how personal data is collected, registered, stored, exploited and disseminated. Personaldata protection is a form of privacy protection mandated directly by the Constitution of the Republic of Indonesia which contains respect for human rights values and respect for individual rights so that it is necessary to provide a legal basis to further provide privacy and personal data security. The 1945 Constitution includes 40 citizen rights. One of them is the right to personal protection. This right is regulated in Article 28 G Paragraph (1) with an outline that citizens are entitled to protection of themselves, their families, honor, dignity and property under their control. Apart from the 1945 Constitution, personal data protection is also regulated in several articles in Law No. 19 of 2016 concerning amendments to Law No. 11 of 2008 concerning Electronic Information and Transactions and Law No. 27 of 2022 concerning Personal Data Protection**.**

The government ensures the application of sanctions for the misuse of personal data by third parties without rights and guarantees the protection of personal data in the virtual world. Legal liability for criminal acts of misuse of personal data is regulated in laws and regulations, including

Law Number 19 of 2016 on Amendments to Law Number 11 of 2008 on Electronic Information and Transactions and Law Number 27 of 2022 on Personal Data Protection. Law No. 19 of 2016 on the Amendment to Law No. 11 of 2008 on Electronic Information and Transactions expressly prohibits unlawful access to data belonging to other people through electronic systems to obtain information by bypassing security systems.

The threat of sanctions against perpetrators of criminal acts of misuse of personal data is listed in several articles in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions. In general, the regulation of privacy data protection contained in Law Number 19 of 2016 on the amendment of Law Number 11 of 2008 on Electronic Information and Transactions, but this law has not made the regulation of privacy data protection real and firm. Therefore, the Indonesian government has sought the protection of personal data by passing Law No. 27 of 2022 on Personal Data Protection to regulate the protection of personal data more specifically. The threat of criminal sanctions for violations of personal data is contained in Articles 67 to 73 of Law Number 27 of 2022 concerning Personal Data Protection.

References

Agustina, Rabiatul, et al. *Juridical Review of Law Number 19 of 2016 concerning Information and Electronic Transactions on Personal Data of Telecommunication Service Users*. 2021.

Aprilia, Mega Lois, and Endang Prasetyawati. "Legal Protection of Consumer Personal Data of Gojek Users." *Mimbar Keadilan*, 2017, pp. 90-105.

Erdisy, Ibrahim Fikma. "The Crime of Misuse of Other People's Personal Data in Online Lending." *Law Journal*, vol. 2, no. 2, 2020, pp. 48-69.

Kusnadi, Sekaring Ayumeida, and Andy Usmina Wijaya. "Legal Protection of Personal Data as a Right to Privacy." *AL WASATH Journal of Legal Science*, vol. 2, no. 1, 2021, pp. 19-32.

Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions

Law No. 27 of 2022 on Personal Data Protection

Nurmalasari. The *Urgency of Ratification of the Draft Law on Personal Data Protection for the Realization of Legal Certainty*. 2021, pp. 47-66.

Pertiwi, Endah, et al. "Juridical Analysis of the Misuse of Personal Data of Social Media Users."

Rechten Journal: Legal Research and Human Rights, vol. 3, no. 3, 2021, pp. 10-16.

Primanta, Asa Intan. "Criminal Liability for Misuse of Personal Data." *Jurist-Diction*, vol.

3, no. 4, 2020, pp. 31-52.

Rumlus, Muhamad Hasan, and Hanif Hartadi. "Policies to Counter Personal Data Theft in Electronic Media." *Journal of Human Rights*, vol. 11, no. 2, 2020, pp. 85-99.

Saragih, Lydia Kharista, et al. "Legal Protection of Personal Data Against Misuse of Personal Data on Social Media Platforms." *De Rechtsstaat*, vol. 6, no. 2, 2020, pp. 25-42.

Situmeang, Sahat Maruli Tua. "Misuse of Personal Data as a Form of Perfect Crime in the Perspective of Cyber Law." *Sasi*, vol. 27, no. 1, 2021, pp. 38-52.