INTERNATIONAL JOURNAL OF JUDICIAL LAW

Buying and Selling Personal Data on Digital Platforms According to Indonesian Positive Law (A Study of Article 67 Paragraph 3 of Law Number 27 of 2022 Concerning Personal Data Protection)

Lucas Abdul Ardiansyah [1*], Rommy Hardyansah [2], Pratolo Saktiawan [3], Mujito [4]
[1-4] Magister of Law, Sunan Giri University, Surabaya, Indonesia

* Corresponding Author: **Lucas Abdul Ardiansyah**

Article Info

ISSN (online): 2583-6536
Volume: 04
Issue: 05
September - October 2025
Received: 11-07-2025
Accepted: 12-08-2025
Published: 15-09-2025
Page No: 38-55

Abstract
In practice, cases of buying and selling databases containing personal data are still found. Typically, personal data is sold through dark web sites or illegal data trading forums on the internet, such as breached forums. The purpose of this research is to review and analyze personal data protection regulations in accordance with Law Number 27 of 2022; analyze misuse of personal data protection; and analyze future regulations related to personal data protection. This research is a normative juridical research type. The results show that the personal data protection regulations in accordance with Law Number 27 of 2022 concerning Personal Data Protection indicate that the legal purpose of the enactment of Law Number 27 of 2022 concerning Personal Data Protection in cases of criminal acts of personal data trading on digital platforms is to ensure that personal data collected by companies or institutions is processed fairly, securely, and in accordance with applicable law. Misuse of personal data protection includes: submitting false administrative requirements, creating fake accounts, acting as someone else, illegal data trading, bullying and sexual harassment, and information theft. Future regulations related to personal data protection can be implemented in several ways. First, tightening regulations. Second, increasing awareness and education. Third, developing technology for privacy. Fourth, increasing international cooperation; stronger international cooperation on data protection and privacy will be crucial. Fifth, ethical data use.

DOI: https://doi.org/10.54660/IJJL.2025.4.5.38-55

Keywords: Buying and Selling, Personal Data, Digital Platforms

Introduction

The 2015 Regulation of the Minister of Communication and Informatics of the Republic of Indonesia concerning the Protection of Personal Data in Electronic Systems states that personal data is specific individual data that is stored, maintained, and kept accurate, and its confidentiality is protected. Specific personal data is any information that is true and real, attached and identifiable, directly or indirectly, to each individual, and its use is in accordance with regulations. The owner of personal data is the individual to whom the personal data is attached.

Theoretically, a data breach is defined as an unauthorized or accidental disclosure by an organization that results in the loss of a customer's personally identifiable information. Culnan and William view data breaches as a privacy issue and recommend that, at the organizational level, companies must create a culture of privacy and implement robust governance processes to ensure that such breaches do not occur in the future. Within the concept of data protection, there are regulations related to the right to confidentiality and the right to erasure. Both rights provide data protection efforts, particularly for organizations providing electronic services (Santoso 2023) [47].

The formulation of regulations related to personal data protection can be understood sociologically. This is due to the need to protect individual rights in society related to the collection, processing, management, and dissemination of personal data. Adequate privacy protection regarding personal data will foster public trust in providing personal data for various broader interests without misuse or violation of their personal rights. In this regard, this regulation can create a balance between individual rights and the rights of the community, whose interests are represented by the state (Rosadi 2023) [45].

Referring to Law Number 27 of 2022 concerning Personal Data Protection, it regulates the form of criminal liability for personal data crimes and who can be held criminally responsible. The law stipulates that collecting personal data through unauthorized or illegal channels, whether through hacking or purchasing from another party, can be subject to a maximum of five years' imprisonment and/or a maximum fine of five billion rupiah, as stipulated in Article 67 paragraph (1).

The Indonesian Telecommunications Regulatory Agency (BRTI) confirms that the sale and purchase of personal data is an unlawful activity. The Ministry of Communication and Information Technology (Kominfo) explained that several cases related to data sale and unauthorized data access have been prosecuted. BRTI also suspects many cases of data buying and selling, which ultimately result in spamming of telecommunications service users by offering various types of products (Putra, Abdurrachman and Hamzani 2023) [38].

Lack of public awareness of privacy protection has led to several violations and misuse of personal data. There is potential for violations of the right to privacy regarding personal data in the virtual realm, online, or on digital platforms. Sociologically, it appears that Indonesians lack a respect for privacy (Rosadi 2023) [45].

The buying and selling of personal data is considered to be correlated with the number of internet users. Over time, the number of internet users in Indonesia has increased (Annur 2023) [4]. The number of internet users in Indonesia reached 213 million in January 2023. This figure equates to 77% of Indonesia's total population of 276.4 million at the beginning of 2023. This represents a 5.44% increase compared to the previous year, as in 2022 the number of internet users was only 202 million (Annur 2023) [4]. In fact, with the increase in the number of internet users, the potential for personal data theft and breaches in cyberspace also increases. Threats such as fraud, personal data theft, and the sale of personal data as a result of cyberattacks are increasingly becoming a major concern (Amir *et al*. 2023) [3].

In practice, cases of buying and selling databases containing personal data are still being discovered. Typically, personal data is sold through dark web sites or illegal data trading forums on the internet, such as breached forums. Breached forums are websites exploited by hacker Bjorka to carry out his personal data breaches. There are several methods for buying and selling personal data, including: collecting personal data for sale by posting fake job openings, pretending to be buyers on online shopping sites, creating applications that include personal data, or through illegal online lending or online gambling sites (Advertorial 2023) [1].

One case related to a lack of respect for privacy that led to the misuse of personal data is the Pelaihari District Court Decision Number 9/Pid.Sus/2021/PN Pli. The verdict shows that defendant Tahyan bin Dul Wahid has been proven legally and convincingly guilty of committing a crime by intentionally and without authorization to access another person's electronic system by any means.

According to the author, cases of personal data trading are increasingly prevalent in this digital era, giving rise to various serious problems that affect individuals and society as a whole. The urgency of addressing this issue lies in protecting the privacy and security of personal data, which are fundamental rights of every individual. Leaked and traded personal data without the owner's consent can result in financial loss, identity fraud, and significant privacy violations. This not only harms the individual whose data is leaked but also undermines public trust in institutions and companies that fail to protect their users' data. From an economic and social perspective, the leak and illegal trading of personal data can have far-reaching impacts, including undermining consumer trust, stifling innovation, and destabilizing financial and social systems. Therefore, it is crucial to take preventative measures and strengthen the law to address this issue.

Problem Formulation

1. How are personal data protection regulated under Law Number 27 of 2022?
2. How is misuse of personal data protection handled?
3. What are future regulations regarding personal data protection?

Research Methods

This research falls under normative legal research. Normative legal research is research aimed at discovering and formulating legal arguments through analysis of the core of a problem. Normative legal research is also considered research aimed at examining legal rules and principles. Normative legal research is legal research practiced through library research. This research falls under the normative juridical research type. Normative juridical research is research applied through the study and analysis of regulatory substance on the core of a problem or legal issue deemed relevant to the topic under study, with an emphasis on legal aspects. The use of normative juridical research is expected to be applied through comprehensive study and analysis, thus obtaining legal prescriptions that can be scientifically justified with a maximum level of accuracy (Yahman and Tarigan 2019) [56].

Discussion

A. Personal Data Protection Regulations in Accordance with Law Number 27 of 2022

Personal data is considered a fundamental human right. The implication of personal data as a fundamental human right is that it is inherent to each individual and cannot be transferred or assigned to another party. Any use of such personal data by another party must be based on the individual's consent. Exceptions to consent require provisions stipulated in law. The concept of personal data (privacy rights) as property is intended to provide inherent protection for personal data, similar to property rights that can be transferred by the rights holder to another party. Treating personal data as property requires costs and a robust system to ensure the operation of property rights, which, when compared to intellectual property rights, is not commensurate with the high costs involved. Personal data, as a fundamental human right, is inherent to each individual. Human rights themselves are not

viewed solely in a physical framework; non-physical elements of a person, such as information or data about a person, require protection.

It is the state's obligation to protect its citizens. The fourth paragraph of the preamble to the Constitution of the Republic of Indonesia clearly states that the government of the Republic of Indonesia is obliged to protect the entire nation. Article 29, paragraph (1) of Law Number 39 of 1999 concerning Human Rights also states that "Everyone has the right to receive personal protection..." While this protection is not specifically explained, it can be concluded that personal data protection also includes the right to privacy, where everyone has the right to conceal or keep private matters confidential.

Data protection in general is a regulation designed to protect personal information, whether collected, processed, and stored or not, intended as part of an archive. Personal data protection is an effort and means of providing legal certainty to individuals related to the use of personal data. Personal data is any information relating to the identification or identification of a data subject, either directly or indirectly, in whole or in part, based on numerical identification or one or more specific factors such as physical appearance, psychological well-being, economic circumstances, and social and cultural identity (Reza & Susanti, 2019) [43].

Data protection is a fundamental human right. Internationally, data protection has been recognized as a constitutional right in the form of habeas data, which is the right of individuals to secure their data and to rectify any errors found in the data (Oktavia *et al*., 2020) [34]. The first regulations relating to privacy and data protection were issued by the Organization for Economic Cooperation and Development (OECD) in 1980. Privacy and data protection are interrelated issues. Data protection aims to ensure that each individual's personal data is handled in accordance with applicable laws and regulations. Privacy is a fundamental human right. Therefore, individuals have the right to control their personal data and information (Perdana, 2020) [35].

The legal basis for the protection of personal data is based on Article 28G and Article 28H of the 1945 Constitution of the Republic of Indonesia. Thus, the protection of personal data is one form of realization of the constitutional mandate that must be regulated in the form of a Law. Article 28G of the 1945 Constitution of the Republic of Indonesia states that "Everyone has the right to protection of personal data, family, honor, dignity and property under his authority, and has the right to a sense of security and protection from the threat of fear to do or not do something is a basic right." Furthermore, Article 28H paragraph (4) of the 1945 Constitution of the Republic of Indonesia states that "Everyone has the right to have personal property rights and such property rights may not be taken over arbitrarily by anyone." These articles are considerations for the need to establish laws and regulations that protect personal data.

As previously explained, the House of Representatives (DPR) ratified Law Number 27 of 2022 concerning Personal Data Protection on October 17, 2022, as a manifestation of the state's commitment to safeguarding each individual's right to privacy and information security. Law of the Republic of Indonesia Number 27 of 2022 concerning Personal Data Protection states that personal data protection is a human right that is part of personal protection. Therefore, a legal basis for ensuring personal data security is necessary, based on the 1945 Constitution of the Republic of Indonesia. Personal data protection is the overall effort to protect personal data throughout the personal data processing process to guarantee the constitutional rights of personal data subjects. Personal data protection aims to guarantee citizens' rights to personal protection, raise public awareness, and ensure recognition and respect for the importance of personal data protection.

Personal data protection is a human right that is part of personal data protection. Personal data protection aims to guarantee citizens' rights to personal data protection, raise public awareness, and ensure recognition and respect for the importance of personal data protection. Personal data protection in electronic systems is carried out through the following processes (Hutabarat, *et al*., 2023) [18]: 1. Acquisition and collection of personal data; 2. Processing and analysis of personal data; 3. Storage of personal data; 4. Display, announcement, transmission, dissemination, and/or access to personal data; 5. Destruction of personal data.

Personal data protection is the protection of all data about a person's life, whether identified or identifiable individually or in combination with other information, directly or indirectly through electronic systems (Syafrial, 2023) [52]. The concept of personal data protection is a form of respect for the right to privacy, where data owners have the power or control to disseminate their information. However, data protection, as a human right, is hampered by the flow of capital, as personal data has a high economic value that drives the global economy. This situation poses a real threat given the unstoppable use of technology, including the mass collection of personal data, both online and offline, through social media, population records, health records, economic records, and law enforcement. In this regard, the role of the State is needed to create laws to provide guarantees for the protection of public privacy data.

The concept of personal data protection is a form of respect for the right to privacy, where data owners have the power and control to disseminate their information. However, data protection, as a human right, is hampered by the flow of capital, as personal data has a high economic value and can drive the global economy. This situation poses a real threat given the unstoppable use of technology, including the mass collection of personal data, both online and offline, through social media, population records, health records, the economy, and law enforcement. In this regard, the state needs to enact legislation to guarantee the protection of public data privacy. Indonesia is considered to be lacking in personal data protection. This results in data collection and management mechanisms carried out by the private sector or the state lacking legal certainty and potentially opening up space for arbitrary action. The tangible effect is that the public is disadvantaged due to the lack of data privacy protection (Tempo, 2019) [53].

Personal data protection actually impacts the country's economy. This is because it enables Indonesia to roll out the red carpet for investors by creating a safe and trustworthy business environment, including the interests of consumers, who will feel secure in conducting economic transactions. Furthermore, personal data protection is crucial because it fosters citizens' freedom of expression. Citizens' courage in expressing their ideas will be realized if they are guaranteed privacy protection.

The entities protected by the personal data protection mechanism are individuals, not legal entities. The right to personal data protection develops from the right to respect for

private life. The concept of private life relates to humans as living beings. Therefore, individuals are the primary holders of the right to personal data protection. Personal data itself is considered all data related to an identified and identifiable individual (Nugroho, Ratnaning, & Vibiantoro, 2022) [32].

Law Number 23 of 2006 concerning Population Administration (UU Adminduk), Article 85, states that the state must store and protect personal data. Personal data must be kept accurate and confidential by administrators and implementing agencies in accordance with statutory regulations. According to Article 84, Chapter IX of the UU Adminduk, the personal data that must be protected are: a) Family Card Number (KK); b) Population Identification Number (NIK); c) Date/month/year of birth; d) Information regarding physical and/or mental disabilities; e) Mother's National Identification Number (NIK); f) Father's National Identification Number (NIK); and g) Several important event records, including records regarding personal data related to important events that need to be protected, such as medical records, banking data, marriage certificates, divorce certificates, and others (Rahayu *et al*., 2021) [40].

Personal data is considered a private area of an individual whose publication cannot be forced upon another party. Information is considered personal data if it relates to an individual and the data owner can be identified from that data. Identification of an individual can be done through an identity card using the number listed and by physical, psychological, social, and cultural characteristics. Regarding personal data protection, it is important to understand that the right to personal protection is a transition from the right to respect for private life. In this regard, individuals are the primary parties to the right to personal protection (Shalihah, Putranti, Putri, Marwa, & Alwajdi, 2022) [49].

Personal data protection encompasses two categories of legal subjects. First, personal data managers, who can be individuals or legal entities, and community organizations that manage personal data, either individually or collectively. In managing personal data, the managers carry out a series of activities on personal data using automated or manual data processing tools, structured into a data storage system. Second, public or private legal entities and community organizations process data on behalf of the data managers (Shalihah, Putranti, Putri, Marwa, & Alwajdi, 2022) [49].

The protection of personal data and privacy is guaranteed in the Indonesian constitution. Article 28G explicitly states that individuals have the right to protection of their personal data, family, honor, dignity, and property under their control. This principle stems from the recognition of human rights values, which are intricately regulated in the 1945 Constitution, and the appreciation of individual rights. Therefore, to guarantee every right granted by the 1945 Constitution, additional regulations are needed to further strengthen guarantees for the security of privacy and personal data and to ensure a stable and conducive business climate. Legal protection of personal data and privacy will enhance human values, enhance self-control, and foster tolerance, while preventing discriminatory and arbitrary actions by those in power (Shalihah, Putranti, Putri, Marwa, & Alwajdi, 2022) [49].

The Minister of Home Affairs, as the person responsible for granting personal data access rights to provincial officials and implementing agency officials, is prohibited from disseminating personal data beyond their authority. Further provisions regarding the requirements, scope, and procedures for granting access rights are stipulated in Ministerial Regulation No. 102 of 2019 concerning the Granting of Access Rights and Utilization of Population Data. Funding for the implementation of population administration programs and activities, including physical and non-physical activities, both at provincial and district/city levels, is budgeted within the state budget. Funding for the implementation of population administration programs and activities was budgeted starting from the 2014 revised state budget (Raharjo & Icuk, 2021) [39].

In the context of information technology, personal data is part of personal rights that must be protected. The elucidation of Article 26 paragraph 1 of Law No. 19 of 2016 stipulates that personal rights include the following rights: 1. Personal rights are the right to enjoy a private life free from any influence; 2. Personal rights are the right to communicate with others without interference; 3. Personal rights are the right to access information related to one's personal life and data.

Personal data is considered a property right. Personal data constitutes a human right inherent to an individual and therefore cannot be transferred or assigned to another party. Use of such personal data by another party must be based on the individual's consent. Personal data is also considered property, with the right to privacy intended to protect personal data, similar to property rights that can be transferred by the rights holder to another party. Broadly speaking, personal data is considered part of human rights and makes it inherent to each individual (Noventri, Sejati, & Putri, 2021) [30].

The Indonesian Telecommunications Regulatory Agency (BRTI) states that the sale and purchase of personal data is an illegal activity. Perpetrators and parties involved can be subject to legal prosecution under applicable Indonesian regulations. However, the Indonesian government is currently preparing more comprehensive personal data protection regulations. Protection of personal data is generally regulated by existing laws and regulations. This is stipulated in the 1945 Constitution, Law No. 39 of 1999 concerning Human Rights, and Law No. 23 of 2016 concerning Population Administration, as amended by Law No. 24 of 2013. Furthermore, there are at least 30 regulations governing data protection, relating to human rights, defense and security, health, population administration, finance and banking, and trade and industry. These regulations are also included in the Minister of Communication and Information Technology Regulation No. 20 of 2016 concerning the Protection of Personal Data in Electronic Systems (PDSE), which was issued on November 7, 2016. In this regard, the practice of buying and selling personal data is considered a violation of existing regulations (Kominfo, 2019) [23].

Personal data can be bought and sold to various parties, including the private sector and even the government. The personal data is used differently according to the needs of the purchaser. Furthermore, the datafication process will generate a number of recommendations that can be used for business development, marketing development, and so on. Therefore, all parties, from the private sector to the government, have an interest in seeking, mining, and datafication. Governments need personal data to identify or predict social unrest, for example, or to control citizens. Meanwhile, private sector stakeholders have more diverse interests depending on the platform. The most common occurrence is the sale of personal data for algorithms to attract consumers. Private sector companies view personal data as a gold mine, but the Indonesian public is not yet fully aware of

its value to them (Novika, 2020) [31].

On the other hand, personal data can be purchased from a data mafia. This mafia obtains data manually, usually from various event vendors, such as exhibitions and music concerts. Data from consumers or clients is sold to the data mafia. On a single exhibition day, hundreds or even thousands of people come, and they are asked to fill out personal data at each store to receive promotions. Without hesitation, they easily fill in personal data such as name, phone number, and home address.

In today's Industry 4.0 era, data is a crucial asset, and its acquisition is increasingly easy. When a buyer creates an account on an e-commerce website, they are asked to enter personal data, which is then entered into a system managed by the e-commerce business provider or seller. This situation necessitates the protection of personal data, from its acquisition, use, processing, distribution, and even destruction. These regulations can be accommodated in a privacy policy. When a buyer makes a transaction through a website or electronic media managed by an e-commerce provider, they are bound by an agreement with the e-commerce provider or seller, outlined in the privacy policy (Akbar & Alam, 2020) [2].

Personal data protection concerns a person's personal data that can be identified, either directly or indirectly, through electronic systems. This data includes telephone numbers, account numbers, dates of birth, names of parents, family members, addresses, medical history, and other information associated with an individual. Cases of credit card fraud, money lending, or embezzlement often involve the use of this personal data. In some cases, personal data is intentionally sold or leaked by irresponsible parties. Digital literacy needs to educate all parties to build awareness of personal data protection (Rahayu, *et al*., 2021) [40].

Online security concerns the ability to maximize personal security and mitigate security risks when using the internet. For example, security in storing online data, banking transactions, and online shopping are important. Digital literacy should convey the importance of using antivirus software on computers and smartphones, using hard-to-guess passwords, not downloading random applications, and avoiding certain sites or applications without first investigating. Furthermore, it's important to update software and store data in multiple locations to avoid unexpected data loss. Individual privacy is the right and ability of individuals to control, edit, organize, and delete personal information. Controlling this privacy includes deciding when, how, and for what purpose information is shared with others. Individual privacy is crucial because it concerns a person's personal secrets, which, if controlled by others, could threaten their safety (Rahayu *et al*., 2021) [40].

Philosophically, efforts to regulate the right to privacy over personal data are a manifestation of the recognition and protection of basic human rights. The philosophical foundation of personal data is Pancasila, namely rechtsidee (legal ideals), which is a conceptual construct that guides the law towards those aspirations. Sociologically, the formulation of regulations on personal data protection can also be understood due to the need to protect individual rights in society regarding the collection, processing, management, and dissemination of personal data.

Adequate protection of personal data privacy will enable the public to provide personal data for various broader societal interests without misuse or violation of their personal rights. In this regard, this regulation will create a balance between individual rights and the rights of the community, as represented by the state. Regulations on personal data protection will significantly contribute to the creation of order and progress in the information society. The following are some of the conditions that personal data protection regulations aim to achieve (Sugeng, 2020) [51]: 1. Protection and assurance of citizens' basic rights regarding personal data privacy; 2. Increased public legal awareness to respect everyone's right to privacy; 3. Guaranteed access to services from the government, businesses, and other community organizations; 4. Protection of the Indonesian nation from all forms of exploitation by other nations of the personal data of Indonesian citizens; 5. Increased growth of the technology, information, and communications industry.

The legal basis for personal data protection is derived from Article 28G of the 1945 Constitution of the Republic of Indonesia. Therefore, personal data protection is a manifestation of the constitutional mandate and must be regulated by law. Article 28G of the 1945 Constitution states that everyone has the right to protection of their personal data, family, honor, dignity, and property under their control, and the right to a sense of security and protection from the threat of fear for doing or not doing something is a fundamental right. This article stipulates the need for the establishment of laws and regulations protecting personal data.

Privacy protection for personal information has developed due to internet use and the increasing number of e-commerce transactions, which have resulted in a large amount of personal information being processed, profiled, and then disseminated to other parties for the purposes of electronic transactions as agreed upon by the parties. Several principles of personal data protection include (Christiawan, 2021) [8]:

1. Collection limitations. There must be limitations in the collection of personal data. Data obtained must be conducted through lawful and fair means. Furthermore, the knowledge and consent of the individual concerned is required.
2. Data quality. Personal data must be appropriate for the purposes for which it is used and must be accurate, complete, and up-to-date.
3. Purpose specification. The purposes for which the data is collected must be specific, and any subsequent use of the data must be limited to those purposes.
4. Use limitations. Data must not be disclosed, made publicly available, or used for purposes other than those specified except: a. with the consent of the data owner; b. with the consent of a legal authority.
5. Security measures. Data must be protected with appropriate safeguards to protect it from loss, destruction, use, alteration, and disclosure.
6. Openness. There must be a general policy regarding the disclosure of personal data.
7. Individual participation. Individuals must have the right to have incorrect data erased or corrected.
8. Accountability. Data controllers are responsible for implementing these measures.

As previously explained, the 1946 Constitution stipulates that every person has the right to protection of themselves, their families, their honor, their dignity, and their property under their control, as well as the right to a sense of security and protection from the threat of fear. The 1945 Constitution, as a constitution, protects an individual's private property. The

legal basis for personal data and data protection has been regulated separately in several regulations according to sectoral interests, such as (Nugroho, Ratnaning, & Vibiantoro, 2022) [32]:

1. Law Number 24 of 2013 concerning Population Administration. This regulation governs data protection for citizen registration in population administration figures. Law Number 24 of 2013 concerning Population Administration states that personal data that must be protected includes: Information about physical and/or mental disabilities; Fingerprints; Iris; Signature; and any other elements that constitute a person's disgrace. Furthermore, Article 95A of Law Number 24 of 2013 concerning Population Administration states that anyone who disseminates personal data without authorization will be subject to a maximum penalty of two years or a fine of Rp 25,000,000 (twenty-five million rupiah).
2. The definition of personal data can be found in the Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning the Protection of Personal Data in Electronic Systems. Articles 1, Number 2 and 2 indicate that personal data is defined as any true and real personal data that is attached to and can be identified with that person, specific personal data that is stored, maintained, and kept accurate, and its confidentiality is protected. Meanwhile, personal data protection is regulated under Article 2, number 1 of the Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning the Protection of Personal Data in Electronic Systems, which stipulates that personal data protection in electronic systems includes protection against the acquisition, collection, processing, analysis, storage, display, announcement, transmission, dissemination, and destruction of personal data. Such protection must adhere to the principles of personal data protection, which respect personal data as privacy.
3. The definition of personal data can also be found in Government Regulation No. 82 of 2012, which applies to Electronic System and Transaction Providers. Article 1 No. 27 states that personal data is specific individual data that is stored, maintained, and kept accurate, and its confidentiality protected. While this definition is considered to encompass any information about an individual, it is unclear what exactly constitutes personal data and whether anonymous or publicly available data is covered by this definition. The government intends to enact a specific law to regulate personal data protection in Indonesia in general.

In practice, companies must ensure they comply with Law Number 27 of 2022 concerning Personal Data Protection and adhere to ethical practices in managing their personal data. Companies or institutions that violate Law Number 27 of 2022 concerning Personal Data Protection may be subject to substantial sanctions and fines. Therefore, it is crucial for companies or institutions to understand and comply with Law Number 27 of 2022 concerning Personal Data Protection when processing personal data. In practice, the implementation of the Personal Data Protection Law is still not fully effective in Indonesia. This is due to the continued high number of data privacy violations. To address this, the government and regulatory bodies must ensure that companies or institutions comply with the regulations and impose strict sanctions on violators (Lambi, 2023) [24].

Personal data owners have the right to receive protection for their personal data. Personal data protection is regulated comprehensively, not just by a few parties, but by all parties involved in storing personal data. Article 1, paragraph 2 of Law Number 27 of 2022 concerning Personal Data Protection states that personal data protection encompasses all efforts to protect personal data throughout the personal data processing process to guarantee the constitutional rights of personal data subjects.

The Personal Data Protection Law protects citizens' fundamental rights and provides a legal framework for personal data protection. The Personal Data Protection Law will prioritize the perspective of personal data protection in all new technological developments, thereby encouraging ethical innovation and respect for human rights (Rahmaniar, 2023) [41]. Chapter IX of Law Number 27 of 2022 concerning Personal Data Protection demonstrates the government's role in ensuring the implementation of personal data protection in accordance with the provisions of Law Number 27 of 2022 concerning Personal Data Protection. Personal data protection is implemented by an institution appointed by the president and is accountable to the president. This institution formulates and establishes personal data protection policies and strategies that serve as guidelines for personal data subjects, personal data controllers, and personal data processors; and oversees the implementation of personal data protection. Administrative law enforcement against violations of Law Number 27 of 2022 concerning Personal Data Protection; and out-of-court dispute resolution facilities. In addition, the institution has several authorities, including:

1. Formulate and establish policies in the area of personal data protection.
2. Supervise compliance by personal data controllers.
3. Impose administrative sanctions for violations of personal data protection committed by personal data controllers and/or personal data processors;
4. Assist law enforcement officials in handling alleged personal data crimes as referred to in the Law.
5. Cooperate with personal data protection agencies in other countries to resolve alleged cross-border personal data protection violations.
6. Assess compliance with requirements for the transfer of personal data outside the jurisdiction of the Republic of Indonesia.
7. Issue orders regarding follow-up actions to personal data controllers and/or personal data processors regarding the results of supervision.
8. Publish the results of personal data protection supervision in accordance with statutory provisions.
9. Receive complaints and/or reports regarding alleged violations of personal data protection.
10. Conduct and respond to complaints, reports, and/or supervision results regarding alleged violations of personal data protection.
11. Summon and present any person and/or public body related to an alleged violation of personal data protection.
12. Request statements, data, information, and documents from any person and/or public body related to an alleged violation of personal data protection.
13. Summon and present any experts needed for investigations and inquiries related to alleged violations of personal data protection.

14. Conduct inspections and inquiries of electronic systems, facilities, spaces, and/or premises used by personal data controllers and/or personal data processors, including obtaining access to data and/or appointing third parties.
15. Request legal assistance from the prosecutor's office in resolving personal data protection disputes.

Philosophically, efforts to regulate the right to privacy over personal data are a manifestation of the recognition and protection of basic human rights. In this regard, the drafting of the Law on Personal Data Protection has a strong and accountable philosophical foundation. This philosophical foundation is Pancasila, which serves as the legal ideal or construct of thought (idea) to guide the law towards its aspirations. In practice, Indonesia was somewhat late in implementing personal data protection regulations, considering that several neighboring countries, such as Malaysia and Singapore, had already enacted similar regulations. As a country with a large population and significant market potential, Indonesia should have implemented regulations governing personal data management earlier.

The House of Representatives (DPR) has passed Law Number 27 of 2022 concerning Personal Data Protection, demonstrating the government's commitment to protecting Indonesian citizens' data, particularly personal data. Law Number 27 of 2022 concerning Personal Data Protection adopts similar protection laws in the European Union. Law Number 27 of 2022 concerning Personal Data Protection was issued to provide protection to digital application users for various transactions. Furthermore, Law Number 27 of 2022 concerning Personal Data Protection stipulates that individuals, including those conducting business or e-commerce activities from home, can be categorized as personal data controllers. Therefore, they are legally responsible for the processing of their personal data and comply with the provisions of Law Number 27 of 2022 concerning Personal Data Protection.

Law Number 27 of 2022 concerning Personal Data Protection was enacted to prevent crimes and management errors that lead to personal data leaks. Personal data leaks not only represent institutional failure and negligence in data governance but also impact public trust in the institution. The enactment of Law Number 27 of 2022 concerning Personal Data Protection is expected to address various issues related to data leaks in Indonesia. Furthermore, Law Number 27 of 2022 concerning Personal Data Protection also serves as a strong and firm warning to application managers. Application managers are obliged to protect user data from leaks and misuse.

Law of the Republic of Indonesia Number 27 of 2022 concerning Personal Data Protection states that personal data protection is a human right that is part of personal protection. Therefore, a legal basis is needed to ensure the security of personal data based on the 1945 Constitution of the Republic of Indonesia. Personal data protection aims to guarantee citizens' rights to personal protection, raise public awareness, and ensure recognition and respect for the importance of personal data protection. The government has a role in implementing personal data protection in accordance with the provisions of Law Number 27 of 2022 concerning Personal Data Protection.

Law Number 27 of 2022 concerning Personal Data Protection does not address norms, but rather procedures, explaining how personal data processing should be carried out. Personal data processing is carried out in accordance with the principles of personal data protection, namely, limited, lawful, and transparent; carried out according to the purpose; carried out while guaranteeing the rights of the personal data subject; carried out accurately and up-to-date; secure; has a purpose and processing activity; can be destroyed or deleted at the request of the personal data subject; and carried out responsibly. Personal data processing begins with acquisition and collection; processing and analysis; storage; correction and updating; display, announcement, transfer, dissemination, or disclosure; and deletion or destruction.

Law Number 27 of 2022 concerning Personal Data Protection stipulates that disputes concerning personal data protection may be resolved through arbitration, courts, or other alternative dispute resolution institutions in accordance with statutory provisions. The applicable procedural law for dispute resolution and/or judicial proceedings concerning personal data protection is implemented based on applicable procedural law in accordance with statutory provisions. Regarding evidence, two types of evidence are considered valid, namely: 1. Evidence as defined in the procedural law; 2. Other evidence in the form of electronic information and/or electronic documents in accordance with statutory provisions.

Article 65 of Law Number 27 of 2022 concerning Personal Data Protection stipulates several prohibitions on the use of personal data, including: 1. Every person is prohibited from unlawfully obtaining or collecting personal data that does not belong to them for the purpose of benefiting themselves or others, which could result in harm to the personal data subject; 2. Every person is prohibited from unlawfully disclosing personal data that does not belong to them; 3. Every person is prohibited from unlawfully using personal data that does not belong to them.

Furthermore, Article 66 of Law Number 27 of 2022 concerning Personal Data Protection stipulates that every person is prohibited from creating false personal data or falsifying personal data for the purpose of benefiting themselves or others, which could result in harm to others.

Regarding criminal provisions for misuse of personal data, these are contained in Articles 67 to 70 of Law Number 27 of 2022 concerning Personal Data Protection.

Law Number 27 of 2022 concerning Personal Data Protection was enacted on October 17, 2022, as a manifestation of the state's commitment to protecting the privacy and information security of every individual. The Personal Data Protection Law is a regulation created to protect individuals' privacy rights regarding the collection, use, and processing of personal data by third parties, including companies or institutions. The purpose of Law Number 27 of 2022 concerning Personal Data Protection is to ensure that personal data collected by companies or institutions is processed fairly, securely, and in accordance with applicable law. Law Number 27 of 2022 concerning Personal Data Protection includes several principles that companies or institutions must adhere to when processing personal data, namely the principles of fairness, accuracy, and transparency. Companies or institutions must ensure that personal data collected and processed is only for legitimate purposes and does not violate the law. There are four important points to note in Law Number 27 of 2022 concerning Personal Data Protection, namely:

1. Every organization that collects, manages, and processes

personal data must obtain permission from the data owner. This is particularly relevant to the ethics of collecting and using information in management information systems. Companies must ensure that the data collected and used is legitimate and has obtained permission from the data owner.

2. Law Number 27 of 2022 concerning Personal Data Protection guarantees individuals' rights to access and control their personal data. This requires companies to provide access and control over their personal data to data owners. Companies must also ensure that personal data is not accessed by unauthorized persons or used for unauthorized purposes.
3. Law Number 27 of 2022 concerning Personal Data Protection requires companies to provide clear and transparent information about how personal data is collected, used, and stored. This relates to the ethics of using information technology and business decision-making. Companies must ensure that the information provided about the collection and use of personal data is clear and understandable to data owners.
4. Law Number 27 of 2022 concerning Personal Data Protection emphasizes that personal data must be adequately protected against unauthorized use and access. This relates to ethical data ownership and protection within management information systems. Companies must ensure that security systems are robust enough to protect personal data from unauthorized access or data leaks.

The Personal Data Protection Law also grants individuals the right to know what information is collected about them and to request that companies or institutions amend or delete inaccurate or irrelevant data. Furthermore, individuals also have the right to restrict the use of personal data by certain companies or institutions. Overall, Law Number 27 of 2022 concerning Personal Data Protection is crucial for protecting individuals' right to control their personal data. This also relates to ethics in the collection and use of information, ethics in the use of information technology, and ethics in data ownership and protection.

Law Number 27 of 2022 concerning Personal Data Protection has the primary objective of protecting individuals' personal data from misuse, unauthorized processing, and unauthorized access by third parties. Furthermore, Law Number 27 of 2022 concerning Personal Data Protection also has several specific objectives. First, it provides adequate protection for individuals' personal information, including identity information, contact information, and other sensitive information. Second, it creates a legal framework that encourages organizations and companies to adhere to data privacy principles, both in the collection, use, storage, and deletion of personal data. Third, preventing the misuse of personal data, including unauthorized commercial use or use that violates individual privacy.

The Personal Data Protection Law is intended to harmonize various overlapping regulations. Among these overlapping regulations, several regulations exist at a more specific level. In addition, there are laws and regulations related to personal data—the protection, collection, processing, use, and disclosure of personal data. These laws and regulations can be grouped into various sectors, including: telecommunications and informatics; population and archiving; finance, banking and taxation; trade and industry; healthcare; and security and law enforcement.

Gustav Radbruch explains the concept of three basic legal elements, which some experts identify as the objectives of law. In this regard, the objectives of law are justice, benefit, and legal certainty. These three elements collectively constitute the objectives of law: justice, benefit, and legal certainty (Is 2021).

1. Legal justice. Justice is the primary goal of law, so it is often the primary focus of all law enforcement. Although justice is a highly abstract concept, throughout human history, there has never been a definitive picture or true meaning of justice. Kanter explains that justice essentially means giving everyone their due, because all people are inherently equal in value as human beings. Therefore, the most basic demand is fairness, equal treatment for all people, naturally in the same situation. Thus, justice expresses the obligation to treat everyone equally in the same situation, respecting the rights of all parties involved. Therefore, Jimly Asshiddiqie explains that justice is the fulfillment of individual desires to a certain extent. The greatest justice is the fulfillment of the desires of as many people as possible.

Law Number 27 of 2022 concerning Personal Data Protection is a significant step by Indonesia in addressing the need for personal data protection in the digital age. The law reflects the principle of legal justice by providing a clear and comprehensive framework for protecting the personal data of Indonesian citizens. This includes regulations regarding the collection, processing, and storage of personal data, as well as granting data subjects the right to control their personal data. Therefore, Law Number 27 of 2022 concerning Personal Data Protection aims to ensure that all personal data processing is conducted fairly, transparently, and responsibly.

In the context of legal justice, Law Number 27 of 2022 concerning Personal Data Protection stipulates obligations for data controllers and processors to ensure that personal data is processed in accordance with the law and that data subjects' rights are protected. This includes the requirement to obtain data subjects' consent before processing personal data and the obligation to protect data from unauthorized access or leakage. Furthermore, Law Number 27 of 2022 concerning Personal Data Protection grants data subjects the right to access, correct, and delete personal data, which is a crucial step in ensuring fairness and transparency in personal data processing.

On the other hand, the effectiveness of Law Number 27 of 2022 concerning Personal Data Protection in realizing legal justice depends not only on the law's content but also on its implementation and enforcement. This includes the establishment of an effective oversight body, increasing public awareness of rights, and implementing adequate sanctions for violations. Therefore, the success of Law Number 27 of 2022 concerning Personal Data Protection in creating a fair and secure environment for personal data requires commitment and cooperation from all parties, including the government, the private sector, and the wider community.

2. Legal Benefit. Benefit is paramount in the objectives of law. In discussing the objectives of law, it is first necessary to understand what is meant by its objectives. Only humans have objectives. However, law is not the goal of humans; it is merely a tool to achieve these

objectives in society and the state. The purpose of law can be seen in its function as a protection of human interests; the law has goals to be achieved.

Law Number 27 of 2022 concerning Personal Data Protection brings several significant benefits in the legal and social context of the country. Here are some of these benefits:

a. Law Number 27 of 2022 concerning Personal Data Protection strengthens the protection of individuals' rights to personal data, an aspect that has become increasingly important in the digital age. By establishing a clear legal framework for the processing of personal data, Law Number 27 of 2022 concerning Personal Data Protection ensures that all entities, both governmental and private, process personal data in a fair, lawful, and transparent manner. This creates a safer environment for citizens to participate in the digital economy, knowing that their privacy is protected by law.
b. Law Number 27 of 2022 concerning Personal Data Protection supports economic growth and innovation by providing legal certainty for businesses and investors. In today's global economy, trust is a valuable currency. With clear and legally guaranteed standards for personal data protection, companies can build trust with consumers and business partners, which in turn can expand market opportunities and encourage innovation. Law Number 27 of 2022 concerning Personal Data Protection also helps ensure that Indonesia remains competitive on the international stage, in line with global best practices in personal data protection, thus opening the door to secure cross-border data exchange and strengthening international economic relations.
c. Law Number 27 of 2022 concerning Personal Data Protection plays a crucial role in promoting responsibility and accountability from entities that process personal data. By establishing strict requirements for consent, data security, and data breach notification, Law Number 27 of 2022 concerning Personal Data Protection forces companies and organizations to adopt best practices in personal data management. This not only protects individuals from data misuse but also helps improve overall cybersecurity standards. In the long term, these efforts contribute to building a more resilient and secure digital society, where personal data is treated as a critical asset that is protected by all means possible.

3. Legal certainty. Legal certainty is a theory born from the development of legal positivism, which developed in the 19th century. Legal certainty is closely related to positive law, namely, the law that applies within a country and/or specific circumstances, in written form (statutory regulations). These regulations, in principle, regulate or contain general provisions that serve as guidelines for the behavior of every individual in society. The existence of such legal regulations and their implementation will create legal certainty.

Law Number 27 of 2022 concerning Personal Data Protection provides a strong legal foundation for personal data protection in Indonesia, creating long-awaited legal certainty in this area. Prior to the adoption of Law Number 27 of 2022 concerning Personal Data Protection, personal data protection in Indonesia was fragmented and scattered across various regulations, creating an inconsistent and sometimes contradictory legal framework. With the enactment of Law Number 27 of 2022 concerning Personal Data Protection, Indonesia now has clear and unified standards for personal data protection, covering the principles of data processing, the rights of data subjects, and the obligations of data controllers and processors.

Law Number 27 of 2022 concerning Personal Data Protection specifically regulates consent as the legal basis for personal data processing, introducing stricter concepts regarding whether and how consent must be obtained and documented. This gives individuals greater control over their data, allowing them to provide, withdraw, or limit consent for specific uses. Thus, Law Number 27 of 2022 concerning Personal Data Protection provides legal certainty not only for data subjects but also for data controllers and processors, who now have clear guidance on how to lawfully obtain and use personal data.

Conversely, Law Number 27 of 2022 concerning Personal Data Protection establishes clear requirements regarding the responsibilities of data controllers and processors in protecting personal data. This includes the obligation to implement adequate security measures and report data breaches within a specified timeframe. Law Number 27 of 2022 concerning Personal Data Protection strengthens personal data security in Indonesia and provides mechanisms to ensure that violations are handled in a transparent and accountable manner, offering further legal certainty for all parties involved.

Law Number 27 of 2022 concerning Personal Data Protection also addresses cross-border data transfers, a critical issue in the global digital economy. By establishing terms and conditions for international data transfers, this law ensures that personal data protection is not diminished when data crosses national borders. This not only benefits data subjects but also assists business entities conducting international operations by providing legal certainty regarding the lawful and secure flow of cross-border data.

Regarding the establishment of an independent supervisory authority, Law Number 27 of 2022 concerning Personal Data Protection ensures that there is a body responsible for overseeing the implementation of the law, handling complaints, and imposing sanctions for violations. The existence of this supervisory authority strengthens legal certainty by ensuring that effective enforcement mechanisms exist and that data subjects have a place to seek redress. Law Number 27 of 2022 concerning Personal Data Protection represents a significant step forward in personal data protection in Indonesia, providing necessary legal certainty for individuals and business entities in the digital era.

The following are some uses of information technology that have the potential to violate privacy and personal data protection (Sugeng, 2020) [51].

1. Registering for internet services. When a user uses a computer to access the internet and pays for the service, they register with an Internet Service Provider (ISP). The ISP provides the mechanism for connecting to the internet, and each internet user is assigned an IP (internet protocol) address.
2. Browsing the internet. When an internet user provides personal data to a website, the user's browser provides the IP address to the site operator. As the user moves from one site to another, the website's algorithm can identify and track user patterns and habits. Search engines can record the user's IP address, search terms

used, search times, and other specific information.
3. Cookies (pieces of information). When a user visits multiple internet sites, a customer trail is recorded on the user's hard drive. Cookies can include information such as login or registration identification data, online user preferences, and so on.
4. Use of mobile devices/mobile apps. Every time a mobile application is downloaded onto a smartphone, whether paid or free, various user data is collected. This data can include phone numbers and email addresses, internet data, device location, and user interaction patterns and behaviors. This important data is collected and processed, becoming valuable information.
5. Cloud computing. The cloud computing industry is a relatively new industry and is attracting a large number of internet users. Users can utilize this service to store relatively large amounts of data, including personal data. When users store data with a program hosted on someone else's hardware, they can lose control over their personal data. Many cloud computing service users have experienced serious security breaches, potentially compromising user data stored on the service provider's servers.
6. Social media (social media networking). Social networks allow users to build connections and relationships with other users. The personal data provided by users when downloading an application, including social media patterns and behaviors, is stored by the social media platform. This allows users to identify news preferences, food preferences, favorite travel destinations, and other information. This data collection is then processed and transformed into a commodity with high economic value in today's information age. If this data is sold to advertising companies, various products will be promoted on social media timelines.

The concept of personal data protection is a form of respect for the right to privacy. The concept of information privacy reaffirms how data owners have the power and control to disseminate their information. However, the ideal of data protection as a human right is challenged by the flow of capital. Economically, personal data has a high market value, driving the global economy. This poses a real threat, given the unstoppable flow of technology. This includes the mass collection of personal data, both online and offline, through social media, population records, health records, the economy, and law enforcement. In this context, the role of the state is essential to ensure the protection of public data privacy.

The Indonesian National Police (Polri), as a state institution authorized as a law enforcement operator, can maintain security and create social order. They are expected to function to achieve this through their pre-emptive, preventive, and repressive police functions. In fact, when dealing with social issues in society involving violations or criminal acts, the Polri is always involved and required to prioritize its repressive function to resolve existing social problems. In essence, combating crime through criminal law sanctions can be considered a tool of criminal politics. Criminal law itself is almost always used in legislative products to deter and secure various types of crimes that may arise in various fields. Crime prevention cannot be resolved solely by the application of criminal law, because criminal law has limitations, two of which are:

1. The nature of crime. Crime, as a social and humanitarian problem, is caused by complex factors that lie beyond the scope of criminal law. Therefore, criminal law will not be able to deeply examine the root causes of crime without the assistance of other disciplines. Therefore, criminal law must be integrated with a social approach.
2. The nature of the function of criminal law itself. The use of criminal law is ultimately only a remedy that addresses the symptoms, not a comprehensive adjustment tool that eliminates the root cause. Criminal law is considered to function after the crime has occurred, thus having no deterrent effect before the crime occurs.

When carrying out their duties, the police serve as law enforcers who interact directly with the public. They receive complaints from the public, which are documented in police reports, and conduct investigations to determine whether the case is a crime. Furthermore, the police conduct investigations, seeking evidence supporting the crime. Law enforcement, in an effort to create order and security, requires synergistic subsystems, including the formulation of effective legal design, the stages of law enforcement, and legal awareness as a manifestation of the community's legal culture. The community is a resource that contributes to a legal system, and in its processes, values, concepts, and ideas are embedded in the implementation of the law. Therefore, law enforcers with integrity, professionalism, and a high level of honesty will be able to drive social change.

The role of law enforcers in carrying out their duties, namely preventing and addressing crime, is a subsystem that cannot stand alone. However, in general enforcement efforts, law enforcers are expected to have a spirit of preventing and addressing crime resulting from the misuse of personal data. In addition to actively enforcing the law, law enforcers must also be aware of the causal factors and preventative measures. Therefore, it is important to be aware of security gaps that can be exploited by irresponsible individuals.

Law No. 27 of 2022 concerning Personal Data Protection states that personal data protection is a human right that is part of personal protection. Therefore, a legal basis for ensuring personal data security is necessary, based on the 1945 Constitution of the Republic of Indonesia. Personal data protection aims to guarantee citizens' rights to personal protection, raise public awareness, and ensure recognition and respect for the importance of personal data protection.

Law No. 27 of 2022 concerning Personal Data Protection defines a personal data subject as an individual to whom personal data is attached. A personal data subject has several characteristics, including:

1. Personal data subjects have the right to obtain information regarding the clarity of their identity, the basis for the legal interest, the purpose of the request and use of personal data, and the accountability of the party requesting the personal data (Article 11).
2. Personal data subjects have the right to sue and receive compensation for violations of the processing of their personal data in accordance with statutory provisions (Article 12 paragraph 1).
3. Personal data subjects have the right to obtain and/or use personal data about themselves from personal data controllers in a form that conforms to a commonly used structure and/or format or is readable by electronic systems (Article 13 paragraph 1).

4. Personal data subjects have the right to use and transmit personal data about themselves to other personal data controllers, as long as the systems used can communicate securely with each other in accordance with the principles of personal data protection (Article 13 paragraph 2).

Some of the aforementioned rights are exempted for: National defense and security interests; Law enforcement interests; Public interests in the administration of the state; Oversight of the financial services sector, monetary affairs, payment systems, and financial system stability carried out within the framework of state administration; Statistics and scientific research interests.

In practice, personal data breaches can occur anytime and anywhere. Therefore, each individual must be more vigilant in safeguarding their personal data. Personal data management in Indonesia is considered crucial and requires a robust and secure security system to minimize theft or data breaches, as well as online data and information trading in Indonesia. This is due to the impact of these crimes, namely the misuse of personal data and information by irresponsible individuals. To prevent hacker attacks, several things can be done, including (Rahmaniar, 2023) [41]: 1. Do not share or reveal personal data carelessly, such as showing your National Identification Number (NIK), National Identity Card (KTP), Family Card (KK), ATM card, and General Election Commission (KPU) data; 2. Use a virtual private network (VPN); 3. Disable Wi-Fi or Bluetooth when not in use; 4. Do not use the same password across all social media accounts; 5. Change your email password monthly; 6. Use an antivirus.

The vulnerability of personal data security and confidentiality is a widely discussed topic. This ranges from data leaks occurring in various institutions, the rampant buying and selling of data through online sites, to overlapping existing regulations. The issuance of Law Number 27 of 2022 concerning Personal Data Protection is expected to guarantee citizens' basic rights regarding personal data protection. In addition to the importance of industry readiness and government firmness in enforcing regulations, a proper understanding is key to achieving the primary goal of personal data protection (Iskandar, 2023) [19].

Law Number 27 of 2022 concerning Personal Data Protection balances individual rights in efforts to mitigate potential misuse of personal data, from data leaks to data trading practices. In the increasingly complex digital era, personal data has become a valuable asset vulnerable to various forms of misuse. Law Number 27 of 2022 concerning Personal Data Protection addresses this challenge by regulating various aspects related to the management, processing, and storage of personal data to prevent data leaks and trading practices.

One of the key points of Law Number 27 of 2022 concerning Personal Data Protection is the establishment of individual rights over their personal data. Everyone has the right to know how their personal data is collected, processed, and used. Everyone also has the right to request deletion of data if it is no longer relevant or has been processed unlawfully. This right gives individuals full control over their personal data, allowing them to take action if they believe their data is being misused. Furthermore, Law Number 27 of 2022 concerning Personal Data Protection regulates the obligations of data controllers and processors in protecting personal data. They are required to implement adequate technical and organizational measures to ensure data security from the threat of leaks or unauthorized access. This obligation includes providing robust protections ranging from data encryption to regular audits of the security systems used. With this obligation, companies and institutions that manage personal data must be more responsible in maintaining data confidentiality and integrity.

On the other hand, Law Number 27 of 2022 concerning Personal Data Protection guarantees the rights of personal data subjects as a form of personal protection as a human right. This constitutional right consists of nine rights, including (Gatra 2022) [13]:

1. Right to information. Personal data subjects have the right to obtain information regarding the clarity of their identity, the basis for legal interest, the purpose of the request and use of personal data, and the accountability of the party requesting the personal data.
2. Right to update and/or correct. Every individual, as a personal data subject, has the right to complete, update, and/or correct errors and/or inaccuracies in their personal data in accordance with the purposes for which the personal data is processed. This right can be exercised by any individual to correct any incorrect personal data so that the data controller can process it appropriately as soon as possible.
3. Right to access. Personal data subjects have the right to access and obtain a copy of their personal data in accordance with statutory provisions. This right can be exercised by any individual to actively obtain the information they desire regarding the processing of their personal data.
4. Right to terminate processing. Personal data subjects have the right to terminate processing, delete, and/or destroy their personal data in accordance with statutory provisions. This right provides personal data subjects with the opportunity to request the termination of the processing of their personal data, either due to errors in the data, unclear legal basis for processing the personal data, or simply to cancel the processing by the personal data subject.
5. Right to withdraw consent. Personal data subjects have the right to withdraw consent to the processing of their personal data that they have given to the personal data controller. This right explains that processing of personal data based on consent as the basis for processing personal data can be withdrawn by the personal data subject, and the personal data controller must comply with and fulfill this right.
6. Right to object to automated processing. Personal data subjects have the right to object to decision-making based solely on automated processing, including profiling, that produces legal consequences or significantly impacts the personal data subject. This right relates to personal data processing carried out by machines without human intervention.
7. Right to suspend or restrict the processing of personal data. Personal data subjects have the right to suspend or restrict the processing of personal data in a manner proportional to the purposes for which the personal data is processed. In this case, the personal data subject may request that the processing of their personal data be suspended. The data controller does not need to delete the personal data, as this restriction is only temporary.
8. Right to sue and receive compensation. Personal data

subjects have the right to sue and receive compensation for violations of the processing of their personal data in accordance with statutory provisions. This right provides an opportunity for any individual who suffers losses due to violations of the processing of their personal data.

9. Right to data portability for themselves. Personal data subjects have the right to obtain and/or use their personal data from personal data controllers in a form that conforms to a structure and/or format commonly used or that can be read by electronic systems. Personal data subjects also have the right to use and transmit their personal data to other personal data controllers, as long as the electronic systems used can communicate securely with each other in accordance with the principles of personal data protection under the PDP Law. This right guarantees personal data subjects the ability to obtain personal data held by a particular data controller so that the data can be transferred for processing by themselves or other controllers. This right ensures that each controller does not represent personal data related to each individual in a structure and/or format that is so difficult or complex to read that other parties cannot read it for their own purposes. Data must be stored in a format commonly used by machines at that time.

Overall, Law Number 27 of 2022 represents a significant step forward in providing personal data protection in Indonesia. By regulating individual rights, the obligations of data controllers and processors, and sanctions for violations, Law Number 27 of 2022 concerning Personal Data Protection creates the necessary balance to protect personal data from the threat of misuse. The public now has a strong legal tool to safeguard privacy, while companies and institutions are expected to be more responsible in managing personal data.

B. Misuse of Personal Data Protection

The development of the digital world has penetrated all aspects of life. However, many internet users are still only able to receive information without being able to understand and process it properly, resulting in many people being exposed to inaccurate information. Personal data is any data about an individual, whether identified and/or identifiable individually or in combination with other information, either directly or indirectly, through electronic or non-electronic systems. Forms of personal data misuse include: submitting false administrative requirements, creating fake accounts, impersonating someone else, illegal data trading, bullying, and sexual harassment (Kominfo 2021) [22].

One common problem with personal data is information theft. Information theft occurs when someone steals personal or confidential information. Data theft can occur for several reasons, including (Nugroho, Azam, and Winardi 2022) [33]:

1. Phishing. Phishing is a common method for gaining access to personal information or information from user accounts where personal information can be found.
2. Poor passwords. Using easy-to-guess passwords across multiple application or web accounts makes it easy for attackers to gain access to all user accounts. Furthermore, if a company stores all its customer information but doesn't have good password practices, it makes it easy for attackers to gain access to all customer accounts.
3. Database or server issues. If a company's database or server that stores customer information is successfully compromised, attackers can access all of the company's customers' personal information.
4. Bad employees. Employees who work for a company have access to a large amount of personal customer information, but who have malicious intent, can misuse the information.
5. Spying. If a user uses a computer in an area where others can easily see the screen, they can view the screen and keyboard to steal information such as login details and other information.

To address the issue of personal data breaches or misuse, Mawrence Lessig proposed several alternative solutions, including (Sugeng 2020) [51]:

1. Through law. This legal solution involves establishing regulations that clearly define the types of violations to be addressed, determine the sanctions to be imposed, and establish principles that must be adhered to by all parties.
2. Through norms. This takes the form of a code of conduct, which applies consistently among online companies to build public trust.
3. Through architecture (code). This involves technology, for example, privacy-enhancing technology.

C. Future Arrangements Regarding Personal Data Protection

In practice, several legal problems can be identified in cases of personal data trading on digital platforms from the perspective of Law Number 27 of 2022 concerning Personal Data Protection. First, Law Number 27 of 2022 concerning Personal Data Protection regulates various types of personal data, but the specific interpretation of the types of data included can be controversial. For example, data taken from social media or other applications may have unclear status. Second, law enforcement against violations of personal data trading can be difficult due to the need for coordination between various agencies, such as the National Police, the Ministry of Communication and Information Technology, and the National Cyber and Crypto Agency. Furthermore, many cases occur in cyberspace involving perpetrators outside of Indonesian jurisdiction. Third, Law Number 27 of 2022 concerning Personal Data Protection stipulates administrative and criminal sanctions. However, the implementation and effective enforcement of these sanctions can be challenging. Courts need a good understanding of technology and cybercrime to impose appropriate penalties. Fourth, digital platforms, especially those based overseas, may not fully comply with Indonesian regulations. This complicates law enforcement, especially when these platforms do not have representative offices in Indonesia. Fifth, public awareness and understanding of personal data protection remains low, requiring increased education about individual rights regarding personal data and the risks of selling it. Sixth, criminal acts of buying and selling personal data often involve international networks. Therefore, strong international cooperation is needed to effectively handle these cases. This includes extradition of perpetrators, asset confiscation, and cooperation in cross-border investigations. Seventh, rapid technological developments often outpace existing regulations. This results in outdated regulations that are less effective in addressing new problems emerging in the digital world.

In principle, personal data protection is divided into two forms. First, data protection involves securing physical data,

both tangible and intangible. Second, regulations govern the use of data by unauthorized parties, misuse of data for specific purposes, and destruction of the data itself (Wulandari, *et al*. 2021) [55].

However, Constitutional Court Decision No. 006/PUU-I/2003 stipulates that personal data protection regulations must be enshrined in law. The ruling stipulates that provisions concerning human rights must be enacted in law. The utilization of science and technology must be carried out to realize a strong and competitive nation, as stipulated in Law No. 17 of 2007 concerning the 2005-2025 National Long-Term Development Plan. One way to achieve this is through regulations related to privacy and human rights (Rosadi 2023) [45]. The mandate to protect human rights related to personal data is implemented in Article 3 of Law No. 39 of 1999 concerning Human Rights.

The implementation of human rights, particularly those related to personal data, must respect the rights of others. Restrictions to ensure public interest or order are implemented as a manifestation of the principle of social function. This is regulated in Article 28J of the 1945 Constitution of the Republic of Indonesia.

Protection of personal or private rights will enhance humanitarian values, improve the relationship between individuals and their communities, increase independence or autonomy to exercise control and achieve appropriateness, and increase tolerance, prevent discrimination, and limit government power. Several principles regarding personal rights exist, including (Sugeng 2020) [51]: 1. The right not to be disturbed by others in one's private life; 2. The right to keep confidential sensitive information concerning oneself; 3. The right to control the use of one's personal data by other parties.

On the other hand, there are several legal principles that can serve as a basis for formulating personal data protection norms, including (Sugeng 2020) [51]:

1. The principle of protection. The principle of protection is highly relevant to personal data protection because the law is essentially intended to provide data owners with protection regarding their privacy, their personal data, and their rights to the data, so that the data is not misused and detrimental to the data owner's interests.
2. The principle of public interest. The principle of public interest is crucial as one of the principles of personal data protection, because it is the public interest that can be pursued for legitimate reasons, as formulated in the law, as a justification for bypassing or making exceptions to the protection of personal data privacy. These public interests include: national security, state sovereignty, and the eradication of corruption and crime.
3. The principle of balance. The principle of balance is also an important principle that needs to be considered as a basis for formulating norms on personal data protection, because the provisions in the law actually reflect an effort to balance personal rights on the one hand and legitimate state rights based on the public interest.
4. The principle of accountability. The principle of accountability provides the basis for all parties involved in the processing, dissemination, management and supervision of personal data to act responsibly so as to ensure a balance between the rights and obligations of the parties involved, including the data owner.

The future of data and privacy is influenced by technological advancements, increasingly stringent regulations, and growing awareness of personal data protection. Here are some possible trends and directions (Zulkifli *et al*. 2024) [60]:

1. Tightening regulations. In the face of data protection and privacy challenges, regulations are expected to tighten further. Countries and regions will implement stricter laws to protect personal data, such as regulations similar to the General Data Protection Regulation (GDPR) that have been extended to various jurisdictions.

Tightening regulations in future efforts to protect personal data will become increasingly crucial with the increasing digitalization and use of information technology. In various countries, personal data protection laws, such as the GDPR in the European Union, have set high standards for personal data management. These measures are taken to reduce the risk of privacy breaches and data misuse that can harm both individuals and organizations. With rapid technological developments, these regulations need to be continuously updated to address emerging challenges, such as the use of artificial intelligence and big data. Furthermore, governments and relevant institutions are expected to strengthen oversight and law enforcement mechanisms related to personal data protection. This includes enhancing the capabilities of data supervisory agencies, imposing stricter sanctions on violators, and increasing transparency in data management by companies. Stricter law enforcement is expected to act as a deterrent to violators and increase compliance with existing regulations.

Personal data protection will also involve closer collaboration between the public and private sectors. Technology companies are expected to take a proactive role in protecting user data by implementing high security standards and complying with applicable regulations. Meanwhile, the government needs to provide a flexible yet robust regulatory framework that can adapt to technological developments without stifling innovation. This collaboration is crucial for creating a safe and trusted digital ecosystem, where personal data is properly protected and used responsibly.

2. Raising awareness and education. Public awareness of the importance of privacy and personal data protection will continue to grow. More individuals will become involved in understanding their privacy rights and how to protect their own data.

Raising awareness and education regarding personal data protection is increasingly important in this digital age. Many individuals still lack an understanding of the risks associated with the misuse of personal data and how they can protect their information. Therefore, comprehensive and ongoing education is needed to increase public understanding of the importance of maintaining data privacy. Public awareness campaigns conducted by governments, non-governmental organizations, and the private sector can play a key role in explaining the various threats and steps that can be taken to mitigate these risks.

Formal education must also adapt to the current needs by incorporating personal data protection into school and university curricula. These educational programs can cover topics such as cybersecurity, an introduction to data protection regulations, and best practices in managing

personal information. By equipping young people with this knowledge from an early age, they will be better prepared to face future privacy challenges and be able to act more wisely in managing their data. Furthermore, companies and organizations need to take the initiative to provide training to their employees regarding personal data protection. This training should include a thorough understanding of privacy policies, employee responsibilities in safeguarding data, and how to recognize and respond to security incidents. By increasing awareness and knowledge across all levels of the organization, companies can build a strong and proactive security culture in protecting personal data. The combination of public education, formal education, and professional training will create a safer and more secure ecosystem for personal data in society.

3. Development of privacy technologies. In an effort to maintain a balance between innovation and privacy protection, new technologies designed to enhance privacy will emerge. This is evident in the use of more secure encryption technologies, data anonymization, or personal control tools that provide more options to users.

The development of privacy technologies plays a crucial role in personal data protection efforts in the digital age. Encryption technology, for example, is a highly effective tool in protecting sensitive information from unauthorized access. End-to-end encryption ensures that data can only be read by authorized parties by encoding information during transmission and storage. This reduces the risk of data leakage, even if the network or system is compromised. In addition to encryption, technologies such as Virtual Private Networks (VPNs) help protect user privacy by hiding their IP addresses and encrypting data transmitted over the internet.

On the other hand, data anonymization and pseudonymization technologies provide additional protection by removing or obscuring individual identities within a dataset. Anonymization ensures that data cannot be linked back to a specific individual, while pseudonymization replaces identifiable information with a pseudonym or false identifier. The use of this technology allows organizations to leverage data for analysis and development without compromising individual privacy. Advances in artificial intelligence and machine learning can also help detect and respond to privacy threats in real time, by identifying suspicious patterns and preventing data breaches before they occur.

The development of privacy technology also includes innovations in the design of more privacy-friendly systems and applications. The concept of Privacy by Design (PbD) encourages the integration of data protection from the earliest stages of technology development, ensuring that privacy is a fundamental element considered at every step of the design and implementation process. Technologies such as role-based access control and multi-factor authentication enhance security by ensuring that only authorized users can access specific data. By continuing to develop and adopt these technologies, we can create a safer and more secure digital environment, where personal data privacy is effectively and sustainably protected.

4. Enhanced international cooperation. In the face of a globally interconnected digital environment, stronger international cooperation on data protection and privacy will be essential. Countries will work together to develop consistent frameworks and standards for data protection.

Enhanced international cooperation in personal data protection efforts is becoming increasingly important in the era of growing globalization and digitalization. Personal data often crosses national borders via the internet, so regulations in one country can impact individuals and organizations in other countries. Therefore, global standards that can be widely adopted are needed to ensure consistent and effective data protection worldwide. International cooperation can help harmonize regulations and best practices across jurisdictions, reducing legal loopholes that can be exploited by unscrupulous parties.

International forums such as the United Nations (UN), the Organisation for Economic Co-operation and Development (OECD), and the European Union have played a crucial role in promoting the harmonization of data protection standards. Through ongoing dialogue and collaboration, countries can share experiences and knowledge to improve the effectiveness of data protection globally.

International cooperation is also crucial in enforcing laws related to personal data protection. Data breaches and cybercrime incidents often involve actors operating across borders, necessitating international cooperation to address these threats. Countries can collaborate through bilateral or multilateral agreements to expedite the investigation, extradition of perpetrators, and prosecution of data breaches. International organizations such as Interpol can also play a crucial role in coordinating cross-border law enforcement operations, providing a platform for sharing intelligence and best practices. Furthermore, international collaboration can strengthen countries' technical capacity to protect personal data. Countries with advanced information technology and data protection capabilities can share expertise and technology with those still developing in this area. Training programs, workshops, and technical assistance can help raise countries' awareness and capacity to address data privacy and security challenges. Through this collaboration, countries can build a stronger and more secure digital ecosystem where personal data is effectively protected worldwide.

5. Ethics in Data Use. Increasing attention will be paid to the ethics of data use in the context of the digital economy. Fair, transparent, and non-discriminatory data use will be a primary focus, with efforts to avoid bias and discrimination in data-driven decision-making.

Ethical data use requires that personal data be used responsibly, transparently, and with the explicit consent of data owners. These principles ensure that data is not misused or exploited for purposes that harm individuals. Adopting an ethical framework helps organizations build trust with users, ultimately strengthening relationships and reputation in the marketplace.

One important aspect of implementing ethics in data use is the principle of transparency. Organizations must clearly communicate to users how data will be used, stored, and protected. This includes providing easily understandable information about privacy policies and obtaining explicit consent before collecting or processing personal data. Transparency creates an environment where users feel more secure and empowered in managing their personal information, while also encouraging more responsible practices on the part of data managers.

In addition to transparency, the principles of fairness and non-discrimination must be upheld in the use of personal

data. Collected data should not be used for purposes that discriminate against individuals based on race, gender, religion, or other protected characteristics. Algorithms and artificial intelligence models that use personal data should be designed to prevent bias and ensure fair outcomes for all users. By prioritizing fairness, organizations can prevent data misuse that could disadvantage certain groups and create a more inclusive digital ecosystem.

Ethical practices also include a commitment to maintaining data security. Organizations should implement robust security measures to protect personal data from unauthorized access, leaks, and cyberattacks. This includes data encryption, strict access controls, and continuous monitoring of security systems. In addition to technical measures, it is also important to build a data security culture within the organization, where every employee understands the importance of protecting personal data and acts in accordance with ethical principles. By integrating ethics into every aspect of data use, individuals can ensure that technology is used for the good and that individual privacy is respected throughout.

In practice, personal data can be taken by people who intend to commit crimes by taking data from websites, social media, personal data spread on the internet and also taken from marketplaces because nowadays there are many buying and selling transactions through marketplaces. Efforts or methods taken to minimize or suppress or even prevent misuse and sale of personal data are by limiting their presence on the internet, being selective in publishing personal data on the internet, understanding personal data protection regulations and preferably using a data security application system (Wismantoro, Aryanto, & Andono, 2020) [54]. In addition, methods that can be done to protect personal data from being used by irresponsible parties include (Clinten & Nistanto, 2019) [9]:

1. Use complex passwords. User accounts can be hacked if the password is weak. Once hacked, unscrupulous individuals are free to do whatever they want with the data contained in the account. Use slightly complex passwords for accounts that request personal data, such as social media accounts, email accounts, and so on. You can also utilize password manager apps, which can be downloaded for free from the Play Store or App Store.
2. Use a VPN or private browser. Unscrupulous individuals often exploit the target's location to carry out malicious activities. This is especially true when using public connections like Wi-Fi, making it easier for them to exploit security holes in the user's device, as data shared over Wi-Fi is often insecure.
3. Avoid uploading photos of documents or personal identification. Photos can be a target for unscrupulous individuals, especially personal documents. Therefore, it's important to avoid uploading images related to personal information online. If an application requests a photo of your ID, ensure that the application is trustworthy and useful.
4. Download applications from official sources. Apps downloaded from unofficial sources are often embedded with malware and adware. Both of these malicious programs can infect devices and then steal all the information stored on the phone. Therefore, it's recommended to only download apps from the Play Store (for Android phones) and the App Store (for iOS phones).
5. Research the company you're applying to. Nowadays, job applications are usually submitted online. Many companies also post job openings online to make them more accessible to applicants. On the other hand, there are individuals who sell personal data using the guise of offering job openings to users. Therefore, it's recommended to research the company offering the job and find out more information about its legitimacy.
6. Limit personal information on social media. Social media is essentially an individual's online portfolio, allowing others to learn a thing or two about each individual. Therefore, each individual is expected to avoid posting personal information, such as phone numbers, email addresses, and other details, on social media platforms. If necessary, individuals can change their social media visibility from public to private.
7. Pay attention to app permissions. Smartphone apps can do anything, such as collect personal information from their users, if authorized by the user. This allows unscrupulous individuals to exploit this vulnerability to steal personal data and then sell it. Therefore, individuals are expected to read the entire agreement and the data collected by the app before using it.
8. Don't click on random links. Besides using the internet, data thieves can use SMS offers to offer lucrative information, such as easy online loans. To obtain these benefits, individuals simply click on the link in the SMS, which usually comes from a random number. In this situation, individuals are advised not to click on such links. This is because they don't know the contents of the link and the source of the SMS is unknown. Individuals can Google the sender's phone number online to determine whether the number is a scam.

Protecting data and information security encompasses efforts to maintain the confidentiality, integrity, and integrity of company information. These efforts also encompass various aspects, such as the hardware or software and data collections that make up the information system. Here are some steps that can be taken (Zebua *et al*. 2023) [59]:

1. Data encryption. Data encryption is a way to hide data. The encrypted data can only be read or accessed by authorized individuals and the encryption key, which acts as a lock.
2. Using a firewall. A firewall acts as a barrier between a computer network and the internet. A firewall, either a software or hardware system, blocks unauthorized access to a company's computer network.
3. Regulating access. By controlling access to data, individuals can limit who can see certain data and when. For example, a company can restrict access to confidential information to a select group of unauthorized employees or limit access to data during specific periods.
4. Maintaining physical data security. Measures that include physical security against attacks are designed to protect the physical security of data. This can be done by securing servers in locked rooms or monitoring sensitive areas with security cameras.
5. Performing regular backups. Data backups are essential and should be performed routinely and regularly. Ideally, previously backed up data can be recovered in the event of data loss due to hardware failure, natural disasters, or

other unforeseen events. Someone has the ability to recover sensitive and important data.

6. Create a data disposal SOP. If the data is truly no longer needed, ensure it is disposed of securely, by completely destroying it and making it inaccessible to prevent it from falling into the wrong hands. This can be done by destroying physical documents with a paper shredder. For digital data, special software may be required.

In the increasingly advanced digital era, the urgency of protecting personal data has become increasingly important. Personal data, which includes information such as identity, address, medical history, and financial data, is highly valuable. When this data falls into the wrong hands, the impact can be devastating, ranging from identity theft to financial fraud. In recent years, incidents of data breaches and cyberattacks have increased significantly, demonstrating that many organizations are not fully prepared to face these threats. Therefore, protecting personal data must be a top priority for governments, companies, and individuals alike.

The future of personal data protection will also be influenced by technological developments such as artificial intelligence (AI) and the Internet of Things (IoT). While these technologies offer numerous benefits, they also pose new risks to data security. AI can be used to analyze and exploit personal data in previously unimaginable ways, while internet-connected IoT devices can become a gateway for hackers. Therefore, strict regulations and advanced security technologies must be implemented to ensure that personal data remains secure amidst rapid technological advancements.

Strict regulations are a crucial foundation for protecting personal data in the digital era. Regulations not only grant individuals specific rights regarding their data, such as the right to access, correct, and delete data, but also impose severe penalties on companies that violate them. Strict regulations force companies to be more careful in managing personal data and ensuring it is protected from cyber threats. In addition to stringent regulations, advanced security technologies must also be implemented to protect personal data. Technological advancements such as data encryption, multi-factor authentication, and intrusion detection systems can provide an additional layer of protection for personal data.

Governments around the world are beginning to recognize the importance of personal data protection and have taken steps to regulate its use and storage. This is considered crucial for building public trust and ensuring that personal data is not misused. In the future, it is hoped that more countries will follow suit and introduce similar regulations to protect their citizens. However, regulation alone is not enough. Public education and awareness regarding the importance of personal data protection must also be increased. Individuals need to understand the risks associated with carelessly sharing personal information and how to protect themselves online. Companies must also commit to protecting their customers' data by implementing best security practices and being transparent in their data management. A combination of strong regulations, advanced technology, and high awareness can create a safer digital environment in the future. Broadly speaking, implementing strict regulations and advanced security technology requires a strong commitment from all parties, including governments, companies, and individuals. Governments need to ensure that these regulations are implemented effectively and adapt them to technological developments. Companies must continue to invest in the latest security technologies and adopt best practices in data management. Individuals must also be more aware of the importance of protecting their personal data and follow basic security practices, such as using strong passwords and not sharing personal information carelessly. With collective efforts, personal data can remain secure amidst rapid technological advancements.

Closing

Conclusion

1. Regulations on personal data protection under Law Number 27 of 2022 concerning Personal Data Protection demonstrate that the legal purpose of enacting Law Number 27 of 2022 concerning Personal Data Protection in cases of criminal acts of buying and selling personal data on digital platforms is to ensure that personal data collected by companies or institutions is processed fairly, securely, and in accordance with applicable law. Furthermore, it aims to ensure that all personal data processing is conducted fairly, transparently, and responsibly; to ensure that all entities, both governmental and private, process personal data in a fair, legal, and transparent manner; and, as a legal basis for personal data processing, to introduce stricter concepts regarding whether and how consent must be obtained and documented. Legal protection for the public related to the criminal act of buying and selling personal data on digital platforms, from the perspective of Law Number 27 of 2022 concerning Personal Data Protection, is considered the overall effort to protect personal data throughout the personal data processing chain to guarantee the constitutional rights of personal data subjects.
2. Misuse of personal data protection includes: submitting false administrative requirements, creating fake accounts, impersonating others, illegally buying and selling data, bullying and sexual harassment, and information theft.
3. Future regulation of personal data protection can be achieved through several means. First, tightening regulations, indicating that in the face of challenges to data protection and privacy, regulations are expected to become increasingly stringent. Countries and regions will implement stricter laws to protect personal data, such as regulations similar to the General Data Protection Regulation (GDPR) being extended to various jurisdictions. Second, increasing awareness and education, where public awareness of the importance of privacy and personal data protection will continue to grow. More individuals will become involved in understanding their privacy rights and how to protect their own data. Third, the development of privacy technology, indicating that in an effort to maintain a balance between innovation and privacy protection, new technologies designed to enhance privacy will emerge. This is evident in the use of more secure encryption technology, data anonymization, or personal control tools that provide more options to users. Fourth, enhanced international cooperation. Facing a globally interconnected digital environment, stronger international cooperation on data protection and privacy will be essential. Countries will work together to develop

consistent frameworks and standards for data protection. Fifth, ethics in data use, which demonstrates that fair, transparent, and non-discriminatory data use will be a primary focus, with efforts to avoid bias and discrimination in data-driven decision-making.

Suggestion

1. The government and relevant authorities are expected to take firm, swift, and transparent action against individuals who engage in the crime of buying and selling personal data on digital platforms.
2. Public campaigns are needed to raise public awareness about the importance of personal data protection and the risks of buying and selling personal data on digital platforms. These campaigns can be conducted through mass media, social media, and educational programs in schools and universities.
3. The government and relevant parties can increase international cooperation through bilateral and multilateral agreements governing the extradition of cybercriminals, the exchange of information, and cooperation in cross-border investigations. This will strengthen Indonesia's ability to handle cases of buying and selling personal data involving perpetrators from abroad.

References

1. Advertorial. Penjual data di dark web tertangkap, polisi pastikan tidak bocor dari BCA [Internet]. Detik.com; 2023 [cited 2025 Oct 10]. Available from: https://news.detik.com/adv-nhl-detikcom/d-6876568/penjual-data-di-dark-web-tertangkap-polisi-pastikan-tidak-bocor-dari-bca
2. Akbar MA, Alam SN. E-Commerce Dasar Teori Dalam Bisnis Digital. Medan: Yayasan Kita Menulis; 2020.
3. Amir N, *et al*. Perilaku Konsumen Dalam Era E-Commerce. Badung: Intelektual Manifes Media; 2023.
4. Annur CM. Pengguna internet di Indonesia tembus 213 juta orang hingga awal 2023 [Internet]. Katadata.co.id; 2023 [cited 2025 Oct 10]. Available from: https://databoks.katadata.co.id/datapublish/2023/09/20/pengguna-internet-di-indonesia-tembus-213-juta-orang-hingga-awal-2023
5. Baskoro SE, Gamariyah F. Aspek Hukum Bagi Pelaku UMKM. Bogor: Ersa; 2022.
6. Bestari NP. Banyak data pribadi dijual di dark web, harganya bikin kaget [Internet]. CNBC Indonesia; 2021 [cited 2025 Oct 10]. Available from: https://www.cnbcindonesia.com/tech/20210907115829-37-274255/banyak-data-pribadi-dijual-di-dark-web-harganya-bikin-kaget
7. Bestari NP. 5 situs penjual data pribadi hasil curian, coba cek data kamu [Internet]. CNBC Indonesia; 2022 [cited 2025 Oct 10]. Available from: https://www.cnbcindonesia.com/tech/20220908073328-37-370246/5-situs-penjual-data-pribadi-hasil-curian-coba-cek-data-kamu
8. Christiawan R. Aspek Hukum Startup. Jakarta: Sinar Grafika; 2021.
9. Clinten B, Nistanto RK. Jual beli data pribadi marak, ini 8 tips untuk melindungi data anda [Internet]. Kompas.com; 2019 [cited 2025 Oct 10]. Available from: https://tekno.kompas.com/read/2019/08/02/16435557/jual-beli-data-pribadi-marak-ini-8-tips-untuk-melindungi-data-anda?page=all
10. Dahlan. Problematika Keadilan dalam Penerapan Pidana terhadap Penyalah Guna Narkotika. Sleman: Deepublish; 2017.
11. Erwin, *et al*. Bisnis Digital (Strategi dan Teknik Pemasaran Terkini). Jambi: PT Sonpedia Publishing Indonesia; 2023.
12. Faiki LO. Dasar-Dasar Hukum Pidana: Teori dan Praktik. Bantul: Mata Kata Inspirasi; 2023.
13. Gatra S. Penyalahgunaan data pribadi: Pinjol hingga doxing, 4 catatan UU pelindungan [Internet]. Kompas.com; 2022 [cited 2025 Oct 10]. Available from: https://nasional.kompas.com/read/2022/09/21/09512511/penyalahgunaan-data-pribadi-pinjol-hingga-doxing-4-catatan-uu-pelindungan?page=all
14. Hakim L. Asas-asas Hukum Pidana: Buku Ajar Bagi Mahasiswa. Sleman: Deepublish; 2020.
15. Harahap ARN, Soesi I, Kanti R. Perlindungan Hukum terhadap Sistem Pembayaran Transaksi Elektronik Lintas Batas Negara. Pekalongan: PT Nasya Expanding Management; 2022.
16. Hattu J. Pertanggungjawaban Pidana Pengambilan Jenasah Covid-19 Secara Paksa Berdasarkan Aturan Tindak Pidana Umum dan Tindak Pidana Khusus. Jurnal Belo. 2020;6(1).
17. Hernoko AY. Hukum Perjanjian Asas Proporsionalitas dalam Kontrak Komersial. Jakarta: Kencana; 2014.
18. Hutabarat SA, Praja SJ, Suhariyanto D, Paminto SR, Kusumastut D, Fajrina RM, *et al*. Cyber Law (Quo Vadis Regulasi UU ITE dalam Revolusi Industri 4.0 Menuju Era Society 5.0). Jambi: PT Sonpedia Publishing Indonesia; 2023.
19. Iskandar Y. Disrupsi Itu Seru: Menyingkap Transformasi Industri Keuangan Melalui Adaptasi dan Inovasi. Jakarta: PT Elex Media Komputindo; 2023.
20. Is MS. Aspek Hukum Informasi di Indonesia. Jakarta: Kencana; 2021.
21. Kojongian R. Tinjauan Kriminologis terhadap Pelacuran. Pekalongan: NEM; 2023.
22. Kominfo. Hindari penyalahgunaan data pribadi [Internet]. Kontan.co.id; 2021 [cited 2025 Oct 10]. Available from: https://kilaskementerian.kontan.co.id/news/hindari-penyalahgunaan-data-pribadi
23. Kominfo. Jual beli data pribadi, BRTI: Itu melanggar hukum [Internet]. Aptika.kominfo.go.id; 2019 [cited 2025 Oct 10]. Available from: https://aptika.kominfo.go.id/2019/05/jual-beli-data-pribadi-brti-itu-melanggar-hukum/
24. Lambi M. Sistem Informasi Manajemen AI (Artificial Intelligence) as the Future Management Information System (Untuk Mahasiswa Ekonomi Program Studi Manajemen). Ponorogo: Uwais Inspirasi Indonesia; 2023.
25. Maheswara IPYD. Penjualan Data Pribadi Ilegal Melalui NFT (Non-Fungible Token) dalam Perspektif Hukum Pidana Indonesia. Jurnal Kertha Desa. 2022;11(1):1430-43.
26. Manalu K, David N. Tinjauan Yuridis: Pertanggungjawaban Pidana istri yang Menerima Nafkah dari Hasil Pencucian Uang. Bekasi: CV Azka Pustaka; 2021.
27. Mauludi S. Socrates Cafe: Bijak, Kritis dan Inspiratif Seputar Dunia dan Masyarakat Digital, Media Sosial,

UU ITE hingga Cyber Crime. Jakarta: PT Elex Media Komputindo; 2018.
28. Mulyadi L. Bunga Rampai Hukum Pidana Umum dan Khusus. Jakarta: Alumni; 2023.
29. Muspiha. Platform Digital: Harga, Kualitas Pelayanan dan Kepuasan Pelanggan. Malang: Rena Cipta Mandiri; 2023.
30. Noventri AC, Noering RFFS, Sabrina IP. Juris Muda: Bunga Rampai Ilmu Hukum Jilid III Hukum dan Teknologi. Yogyakarta: Nas Media Pustaka; 2021.
31. Novika S. Marak kasus jual beli data pribadi, dijual ke mana [Internet]. Detikfinance; 2020 [cited 2025 Oct 10]. Available from: https://finance.detik.com/berita-ekonomi-bisnis/d-5263253/marak-kasus-jual-beli-data-pribadi-dijual-ke-mana
32. Nugroho AD, Ratnaning DS, Vibiantoro S. Hukum Administrasi Kependudukan Elektronik: Paradoks Perlindungan dan Pengakuan Status Pribadi serta Status Hukum terhadap Kontrol Kepatuhan Warga Negara di Era 5.0. Makassar: PT Nas Media Indonesia; 2022.
33. Nugroho A, Al Azam MN, Winardi S. Fundamental Komputer Era Digital Masa Depan. Surabaya: Narotama University Press; 2022.
34. Oktavia A, Efendi SM, Anisah BR, Setiawan D, Fathurrohman F, Winata FJ, *et al*. Antologi Esai Hukum dan HAM: Afiliasi Hukum dan HAM dalam Mewujudkan Perlindungan Hak Asasi Masyarakat Indonesia. Malang: Universitas Muhammadiyah Malang; 2020.
35. Perdana A. Data Analytics: Keteraampilan Teknis Akuntan dan Auditor di Era Digital. Batu: CV Madza Media; 2020.
36. Prameswati V, Nabillah AS, Kartika YN. Data Pribadi Sebagai Objek Transaksi di NFT pada Platform Opensea. Jurnal Civic Hukum. 2022;7(1).
37. Putra MN, Neni R. Jual Beli Data Pribadi Nasabah Bank Ditinjau dari Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Penegakan Hukumnya Dihubungkan dengan Unsur Penyertaan dalam Kitab. Prosiding Ilmu Hukum SPeSIA: Seminar Penelitian Sivitas Akademika Unisba. 2020;6(2).
38. Putra TW, Hamidah A, Achmad IH. Pertanggungjawaban Pidana terhadap Kejahatan Hacking. Pekalongan: PT Nasya Expanding Management; 2023.
39. Raharjo MM, Icuk. Manajemen Pelayanan Publik. Jakarta Timur: PT Bumi Aksara; 2021.
40. Rahayu K, Setianto WA, Adiputra WM, Monggilo ZM, Tania S, Prayitno RK, *et al*. Perempuan dan Literasi Digital: Antara Problem, Hambatan dan Arah Pemberdayaan. Yogyakarta: Gadjah Mada University Press; 2021.
41. Rahmaniar A. Bunga Rampai Isu-Isu Komunikasi Kontemporer. Jakarta: Proxy Media; 2023.
42. Raihan M. Perlindungan Data Diri Konsumen dan Tanggungjawab Marketplace terhadap Data Diri Konsumen (Studi Kasus: Kebocoran Data 91 Juta Akun Tokopedia). JIP: Jurnal Inovasi Penelitian. 2023;3(10).
43. Reza HK, Susanti M. Keuangan Digital. Cirebon: Yayasan Wiyata Bestari Samasta; 2019.
44. Rohman H. Hukum Jual Beli Online. Pamekasan: Duta Media Publishing; 2020.
45. Rosadi SD. Pembahasan UU Perlindungan Data Pribadi (UU RI No 27 Tahun 2022). Jakarta: Sinar Grafika; 2023.
46. Ruslan MT. Perlindungan Hukum: Bagi Wisatawan Dengan Kabupaten Banggai. Pasaman Barat: CV Azka Pustaka; 2022.
47. Santoso E. Hukum Siber: Permasalahan Hukum Bisnis di Bidang Teknologi Informasi dan Komunikasi. Jakarta: Kencana; 2023.
48. Sewaka KA, Denok S. Digital Marketing. Tangerang Selatan: Pascal Books; 2022.
49. Shalihah F, Putranti D, Putri UT, Marwa MH, Alwajdi MF. Equity Crowdfunding di Indonesia. Yogyakarta: UAD Press; 2022.
50. Situmeang SMT. Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna dalam Perspektif Hukum Siber. SASI. 2021;27(1).
51. Sugeng. Hukum Telematika Indonesia. Jakarta: Kencana; 2020.
52. Syafrial H. Literasi Digital. Makassar: PT Nas Media Indonesia; 2023.
53. Tempo PD. Untung Rugi Data Konsumen di Era Digital. Jakarta: Tempo Publishing; 2019.
54. Wismantoro Y, Aryanto VD, Andono PN. Literasi Fintech Melalui Pendekatan Marketing Sosial (Konsep, problem dan Studi Empiris). Yogyakarta: Kanisius; 2020.
55. Wulandari R. Perlindungan Hukum Pegawai Pemerintah dengan Perjanjian Kerja di Rumah Sakit Umum Daerah. Surabaya: Scopindo Media Pustaka; 2020.
56. Yahman, Nurtin T. Peran Advokat dalam Sistem Hukum Nasional. Jakarta: Kencana; 2019.
57. Yunus M, Fahmi FR, Satria H, Gusti K, Shofia. Tinjauan Fikih Muamalah terhadap Akad Jual Beli dalam Transaksi Online pada Aplikasi Go-Food. Amwaluna: Jurnal Ekonomi dan Keuangan Syariah. 2018;2(1).
58. Yusuf M, Irvan I. Praktik Jual Beli Jahe Menurut Hukum Islam: Studi Kasus di Usaha Dagang Areba Jahe Jakarta Timur. MIZAN: Journal of Islamic Law. 2021;5(1).
59. Zebua RSY, *et al*. Bisnis Digital (Strategi Administrasi Bisnis Digital untuk Menghadapi Masa Depan). Jambi: PT Sonpedia Publishing Indonesia; 2023.
60. Zulkifli, *et al*. Ekonomi Digital. Batam: Yayasan Cendikia Mulia Mandiri; 2024.