TIRTAYASA JOURNAL OF INTERNATIONAL LAW
Volume 2 Nomor 1, June 2023, hlm. (15-30)
Fakultas Hukum, Universitas Sultan Ageng Tirtayasa, Serang-Banten, Indonesia
P-ISSN: 2961-8355 | e-ISSN: 2961-8061
https://jurnal.untirta.ac.id/index.php/tirtayasatjil

# PERSONAL DATA PROTECTION IN THE ERA OF GLOBALIZATION (INDONESIA PERSPECTIVE)

**Yogi Muhammad Rahman**[1]
[1]*Galuh Ciamis University*
*Jl. R.E Martadinata No. 150, Ciamis 46274, Jawa Barat*
*yogi@unigal.ac.id*

**Aflah Haora**[2] **Elsa Nurfitriani Sutansi**[3]
[2,3]*Universitas Sultan Ageng Tirtayasa*
*Jl. Raya Palka KM 3, Sindangsari, Pabuaran, Kab. Serang Provinsi Banten*
[2]*1111210181@untirta.ac.id*
[3]*1111210188@untirta.ac.id*

**Info Artikel**
|**Submitted**: 03-04-2023 |**Revised**: 10-06-2023 |**Accepted**: 15-06-2023

How to cite: Yogi Muhammad Rahman, Aflah Haora, *et al*, "Personal Data Protection in The Era of Globalization (Indonesia Perspective)", *Tirtayasa Journal of International Law*, Vol. 2 No. 1, (June 2023)", hlm. 15-30.

***ABSTRACT:***

*This journal explores the topic of securing personal data in the era of globalization, focusing on the legal framework of International Law and existing laws and regulations in Indonesia, especially the provisions stipulated in Law Number 27 of 2022 concerning Data Protection. The main objective of this study is to provide readers with knowledge regarding the personal data protection regulatory landscape at both national and international levels. This research uses juridical-normative and juridical-empirical methodologies to collect, compile, and research research data. This approach includes the study of legal theories and concepts related to the legal principles of laws and regulations, especially those contained in Law Number 27 of 2022, through journal references or legal materials through electronic media. The goal is to gain theoretical insights that can serve as a foundation for research. Furthermore, this research gave birth to a discourse on individual information governance within the framework of global jurisprudence and regulatory framework in Indonesia, especially Law Number 27 of 2022, along with the consequences caused after its implementation.*

***Keywords****; Personal Data, Data Protection, the Era of Globalization*

## A. Introduction

Technology has developed rapidly in this era of globalization, with new developments constantly being made to improve the quality of life of the people. It has garnered significant public interest and engagement. Undoubtedly, this progress will have both beneficial and detrimental effects. One of the positive effects is the facilitation of information exchange, which in turn creates many opportunities for development based on the information obtained.

It is imperative to enhance privacy policy as an integral component of human rights-related laws, and the safeguarding of personal data through special measures is a means of

upholding the right to privacy, which is an integral component of human rights.[1] Law of the Republic of Indonesia No. 27 of 2022 concerning Personal Data Protection highlights the importance of the above. The main purpose of the personal data protection regulation is to safeguard and ensure the fundamental rights of citizens regarding the protection of personal data.[2] In addition, public access to government services, corporations, business actors, and other institutions is the purpose of this law. In addition, encouraging the expansion of economic sectors and helping the local manufacturing sector become more competitive are also important goals.[3]

In today's era, there are prerequisites that require the fulfillment of the use of the chosen social networking platform. It involves creating an account, which mandates the provision of personal information that is subsequently stored and leaves a digital footprint on all pages visited. Privacy of personal data is exclusive to its owner. Advances in information and communication technology have resulted in reduced privacy restrictions, making it easier to disseminate personal data. Undoubtedly, this will result in adverse consequences that stimulate the emergence of new commercial frameworks centered on trading individual data. Indonesia has experienced many incidents of data leakage, as observed in recent years.

On April 17, 2020, Tokopedia discovered a breach of confidential information relating to no less than 12,115,583 user accounts. Shortly after the event, an additional data breach occurred at Bhineka.com, a company specializing in *e-commerce*. *Shiny Hunters*, a hacking group, is said to have obtained the user data of 1.2 million people from Bhinneka.com. The information is marketed at a price of 12,000 US dollars or equivalent value in Indonesian Rupiah, which is 17,800,000. Previously, Bukalapak, an additional *e-commerce* platform, experienced a data leak. According to records, a total of 12,957,573 user accounts on the platform were exchanged.[4]

---

1 Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, "*The European Union General Data Protection Regulation: What It Is and What It Means*", Information & Communications Technology Law, Vol. 28, No. 1, 2019, pp. 66.

2 Rosalinda Elsina Latumahina, "*Aspects Law Protection Data Personal in Cyberspace*", Journal Echo Actuality, Vol. 3, No. 2, 2014, pp. 23.

3 Law of the Republic of Indonesia Number 27 of 2022 concerning Personal Data Protection.

4 ELSAM and Commission I DPR RI, Term of Reference (TOR) Representative Secretariat Commission I DPR and Team Assistance PDP Bill Secretary-general House of Representatives of the Republic of Indonesia, "*Discussion InventoryList Problem (DIM) Bill Protection Data Personal Focus Group Discussion*", Jakarta: Century Park Hotels Wednesday 22 July 2021 hit 10.00- 17.00.

The rise of personal data breaches in Indonesia shows that the privacy rights of its citizens are very vulnerable to exploitation, which has the potential to cause social harm. Therefore, it is imperative to establish a legal framework that governs the trajectory of technological progress to prevent deviant treatment of individuals during the era of globalization.

The legal system plays an important role in shaping the lives of individuals and develops in response to changing norms and values of society. Article 1 (3) of the 1945 Constitution affirms that Indonesia is a state of law. The assertion argues that the law serves as the highest standard for addressing any problem. Despite the different technological and legal nature, they have the same goal of improving the well-being of individuals. International law refers to a comprehensive set of principles and regulations governing the behavior of states with each other, which they are expected to adhere to universally.[5] Law could serve as a tool for social *engineering* and *social controlling*.

Social engineering refers to the deliberate application of legal measures to establish a desired order or structure of society that is in line with predetermined goals. The concept of[6] *social controlling* involves legitimate interventions aimed at preventing deviant behavior in society. It can be concluded that legal instruments are used in *a social engineering* capacity to produce positive change and are reinforced by *social controlling* actions that seek to force individuals to comply with established norms and values.

The study has significant relevance to the current situation, given the ubiquitous use of social networking services in individuals' daily routines. The preparation of this journal is expected to provide enlightenment to the public about the importance of caution in using social media platforms. This journal will discuss the problems that have been described, namely:

1. Safeguarding personal information in the context of globalization from the point of view of international law in Indonesia.
2. The legal framework governing the management of personal data in Indonesia is stipulated by Law No. 27 of 2022.

## B. Research Method

[5] J.G. Starke, "*Introduction Law International*", Jakarta: Sinar Graphicsthing, 2010, pp. 3.
[6] Satijpto Rahardjo, "*Law Progressive: A Synthesis Law Indonesian*", Yogyakarta: Bell Publishing, 2019, pp. 128.

There are social and judicial aspects to this issue that need to be investigated. The researchers chose to use theoretical and empirical legal approaches to data collection and analysis. Juridical-normative studies examine precedents, such as theories, concepts, legal principles, and laws and regulations, which are in direct contact with the problem at hand. An empirical approach is a form of sociological legal research that investigates legal provisions and their impact on individual experience. This methodology is commonly used in the field to explore the intersection of law and society.

According to Bogdan and Taylor, qualitative research methods generate descriptive data in the form of interviews, focus groups, diaries, and other written and oral reports of people's experiences. Data collection techniques refer to the various methodologies that researchers can use to collect data. Researchers have the option of using a single or mixed methodology based on the challenges faced or being investigated.[7] Focusing on Law Number 27 of 2022, however international instruments such as the General Data Protection Regulation (GDPR), Universal Declaration of Human Rights (UDHR), International Covernant on Civil and Political Rights (ICCPR), European Convention on Human Right (ECHR), and the Charter of Fundamental Rights of the European Union (CFREU) are also referenced by researchers. This study uses qualitative data analysis to examine a number of legal theories and ideas related to the application of legal principles. This study utilizes journal references and legal materials accessed through electronic media to obtain theoretical insights as a basis for further research.

## C. Discussion

### 1. Safeguarding personal information in the context of globalization from the point of view of international law in Indonesia

From the point of view of international law, the safeguarding of personal data relating to privacy falls under the umbrella of human rights protection. The concept has its roots in the 1948 Universal Declaration of Human Rights (UDHR), which stood as the first international instrument to protect the right to privacy of individuals. Article 12 of the UDHR specifically regulates this aspect. The notion of privacy was originally formulated by Warren

[7] Rachmatul, "*Engineering Collection Data Deep Research Quantitative and Qualitative*", IAIN Sheik Nurjati Cirebon, 2013.

and Brandeis in their article entitled "*The Right to Privacy*" published in the Scientific Journal of Harvard University School of Law.

The journal argues that technological advances and advances in the era of globalization have the potential to increase public awareness of the right of every community to live a fulfilling life, or more specifically, the right of individuals to safeguard their personal lives from interference by the state or others.[8] So, safeguarding and recognizing the right to privacy requires legal action, thereby underscoring the urgency of regulations relating to the privacy of personal data.

On the contrary, EU regulations can serve as a benchmark for other countries, as they provide a thorough and meticulous framework for protecting personal data, particularly the General Data Protection Regulation (GDPR). The regulation outlines basic principles and guidelines for protecting personal data, serving as a valuable reference for countries wishing to establish or refine their own data protection policies. The application of this regulation may result in the imposition of penalties under the GDPR for unauthorized disclosure of data to external entities without the explicit consent of the data owner.

Currently, international law allows individual countries to establish their own laws that protect the privacy and confidential information of individuals. However, International Law has also undertaken various initiatives to standardize regulations in this regard.

1. The right to privacy is governed by Article 17 *of the International Covenant on Civil and Political Rights* (ICCPR). However, the ICCPR does not specifically state that privacy rights include the protection of a person's personal information from unauthorized access. The United Nations Human Rights Committee (HRC) has issued comprehensive guidelines to describe the extent of the right to privacy as described in CCPR General Declaration No.16: Article 17. As per[9] *General Comment*, it is imperative that individuals are given the right to understand the personal data stored in automated data files, along with the purpose for which they are stored. In addition, individuals should be able to identify public authorities,

[8] Richards, Neil and Hartzog Woodrow. "*Taking Trust Seriously in Privacy Law*". Stanford Technology Law Reviews, Vol. 19, No. 431, 2016, pp. 434.

[9] Christopher Kuner, "*The European Union and the Search for an International Data Protection Framework*", Groningen Journal of International Law, Vol. 2, 2014, pp. 76.

individuals or private entities that may have control over their data. Individuals have the right to request deletion or correction of their data if it includes inaccurate personal information or is unlawfully collected, processed, or used.[10]

2. Safeguarding the right to privacy is a concern *of the Council of Europe*, a regional international organization. To that end, the organization has made a number of agreements, including Article 8 of the ECHR, which forms the basis for a convention that comprehensively regulates the handling of personal data. The Convention is the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, adopted by the Council of Europe. Individuals have the right to privacy in their homes, in their communications with others, and in their private and family lives, as stated in Article 8, paragraph 1 of the European Convention on Human Rights. This includes protection of the personal life and correspondence of a person hacked. With exceptions in cases of national security, public security, economic prosperity, prevention of crime and harassment, protection of morals and health, and protection of the rights and freedoms of others, states are prohibited from interfering with the right to privacy of individuals under Article 8, paragraph 2 of the European Convention on Human Rights.[11]
3. In addition to the *Council of Europe*, there are other international organizations operating in the European region, such as the European Union. The latter has established an international legal framework aimed at protecting the right to privacy and ensuring the protection of personal data.
4. *The Charter of Fundamental Rights of the European Union* (CFREU) contains provisions relating to the right to privacy. Specifically, Article 7 of the CFREU
5. Establishes that every individual has the right to protection of their personal life, home, and communications. Article 8 deals with the regulation of securing personal information. Article 8 paragraph 1 guarantees everyone the right to privacy. The OECD Guidelines on Privacy Protection and Cross-Border Flow of Personal Data are referred to in paragraph 2 to ensure that data are handled fairly and transparently, for limited purposes, with the consent of data subjects, and in accordance with OECD Guidelines. For the first time, universal rules, and minimum requirements for

[10] United Nations, 1988, General Comment No. 16 of Article 17 ("The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation"), pp. 1.

[11] Milton Themba, 2016, "*The Right to Privacy and Identity on Social Network Sites: A Comparative Legal Perspective*", thesis, University of South Africa, pp. 137.

protecting personal information in all member states were established. Article 38(1) of the Statute of the International Court of Justice is consistent with the OECD classification on personal data security as a *general principle of law*.

6. According to Article 8 of the Convention on Human Rights, public entities are obliged to safeguard the privacy of individuals and related data. Individuals must have the ability to carry out appropriate storage or processing of personal data.

Data privacy security is an integral aspect of privacy rights in the realm of information technology. Law Number 27 of 2022 which has just been promulgated in Indonesia regulates the security of users' personal information. In Indonesia, various regulations contain provisions on safeguarding privacy and personal data.

1. According to Article 28G (1) of the 1945 Constitution, everyone has the right to defend himself, his loved ones, his reputation, his honor, and his property. In addition, they deserve to feel a sense of security and protection from any form of intimidation that may affect their actions or inaction. Something that is considered as a fundamental right or privilege that every individual has for being human.
2. This text relates to the legal framework of ITE Law Number 19 of 2016, which aims to protect data privacy and privacy rights. Specifically, Article 26 of the Act discusses:
    a. If there are no legal provisions to the contrary, it is mandatory to obtain the consent of the person concerned for the use of personal information through electronic means.
    b. Persons who have violated their rights as referred to in paragraph (1) may seek compensation through the courts to obtain financial compensation.
    c. To comply with the court's determination, each Electronic System Operator must delete, at the request of the affected party, any Electronic Information and/or Electronic Documents that are considered irrelevant and under the control of the operator.
    d. In accordance with the provisions set forth in the relevant laws and regulations, each Electronic System Operator must provide a way to delete outdated Electronic Information and/or Electronic Documents.

3. According to Article 8 paragraph (1) letter e of Law Number 23 of 2006 concerning Population Administration, the organizer must guarantee the confidentiality and security of information related to population events and other important matters.

**2. The legal framework governing the management of personal data in Indonesia is stipulated by Law No. 27 of 2022**

The notion of privacy is often associated with Western (European) ideology in public discourse in Indonesia, like the concept of human rights. The reasons behind the limited public awareness of privacy, particularly with respect to the protection of personal information, are supported by this statement. In Indonesia, individuals can easily disclose their residential location, date of birth, and family relationships to others in public spaces. In addition, it is customary in Indonesia to provide identity cards (KTP) or other forms of personal identification to third parties that include a person's personal information.[12]

The Constitution, as the supreme legal authority for all legislative provisions, does provide security measures for individual data. The preservation of human rights is guaranteed by the Fourteenth Amendment to the 1945 Constitution, which can be seen in the articles of human rights, especially Articles 28, 28A, and 28J. Article 28G paragraph (1) of the Constitution of the Republic of Indonesia which came into force in 1945 contains provisions on the protection of individual rights of residents. The rights to self-defense, family, honor, dignity and property are guaranteed to all persons covered by this document. In addition, people have the right to be free from fear that may prevent them

from exercising their civil rights. The operationalization of norms relating to data protection requires their incorporation into organic legislation and regulations in accordance with the established hierarchy of legal and regulatory frameworks.

The implementation of Law No. 27 of 2022 on October 17, 2022, has clarified the regulations surrounding Personal Data in Indonesia. Therefore, everyone in Indonesia can rest assured that their personal information will be safe. The total number of provisions in Law Number 27 of 2022 is 75. The General Provisions are followed by section Types of Personal Data, Rights of Personal Data Owners, Personal Data Processing, Dispute

[12] Revelation Djafar, *"Law Protection Data Personal in Indonesia Landscape"*, Urgency and Necessity Updates, pp. 6.

Resolution, and Internal Dispute Resolution.[13] The upcoming discussion will explore certain aspects of Law No. 27 of 2022 concerning Personal Data Security, commonly referred to as the PDP Law.

Before the PDP Law was promulgated in Indonesia, there were at least thirty legal provisions related to the responsibility to ensure the security of personal data, according to a study by the Institute for Community Studies and Advocacy (ELSAM).[14] The Population Administration Law is a law that provides special arrangements for the categorization of personal data. The Population Administration Law, especially Law No. 23 of 2006 as amended by Law No. 24 of 2013, initially defines the scope of personal data including KK Number, NIK, date/month/year/birth, information related to physical and/or mental disabilities, Mother's NPWP, Father's NPWP, and select the contents of records about important events. The Population Administration Law has broadened the scope of personal data to include various categories such as information relating to physical and/or mental disabilities, fingerprints, irises, signatures, and other data elements that can be considered a source of shame for a person. The scope of the Population Administration Law is limited to the regulation of the Population Administration. In other words, the Population Administration Law lacks comprehensive provisions related to the procurement, manipulation, and storage of individual information. The legal framework that provides more protection of data owners' rights is Law No. 11 of 2008 concerning Electronic Information and Transactions which was later amended by Law No. 19 of 2016. Article 26 of the ITE Law establishes the foundation for securing personal data obtained through electronic systems, as outlined in the law. Article 26 paragraph (1) of the ITE Law emphasizes the importance of obtaining the consent of the data owner in utilizing his personal data. Failure to comply with this requirement may result in a violation of civil law rights, as stipulated in Article 26 paragraph (2) of the same law, so that the affected party can bring legal proceedings. The ITE Law also accommodates the right to be forgotten through the provisions of Article 26 paragraph (3) which gives data owners the right to ask electronic system operators to delete irrelevant personal data. Although the ITE Law regulates the handling of personal data, it does not provide a precise description of the term

[13] *Ibid*, pp. 12.

[14] Revelation Djafar, Sumigar Bernhard Ruben Fritz, S. B. L, "*Protection of personal data in Indonesia*", 2016, Available on website: http://weekly.cnbnews.com/news/article.html?no=124000, Accessed March 31th, 2023.

"personal data". Lexicons related to individual information are regulated in legal frameworks such as PP 18/2012 concerning the implementation of electronic systems and transactions, and Permenkoinfo 20/2016 concerning Security of Personal Data in Electronic Systems. The foregoing requires the implementation of sector-specific regulations, such as SEOJK 014/2014, relating to the confidentiality and security of personal data and/or consumers, as stipulated in OJK Circular Letter No.014/SEOJK.07/2014.[15]

According to Article 1 point 2 of Law No. 27 of 2022 concerning Personal Data Protection, "Personal Data" means any and all information relating to an identified or identifiable natural person, whether obtained directly from the subject or indirectly from other sources, whether recorded intangible or intangible media. In line with the provisions of Article 1(2), the protection of Personal Data in the processing chain is a comprehensive effort aimed at protecting the constitutional rights of the Personal Data subject concerned.

In accordance with Article 12(1), a person whose personal data is processed improperly may, in accordance with applicable law, file a claim with the court and demand compensation for the losses suffered. Therefore, in the event of a breach of the processing of personal data, both individuals and corporations have the right to seek legal recourse and claim compensation.

Law no. 27 of 2022 outlines the role of personal data controllers and personal data processors. Individuals, public entities, and international organizations that determine the purposes and supervise the handling of personal data are referred to as personal data controllers. The term "personal data processor" refers to an individual, public entity or international organization that processes personal data on behalf of a personal data controller, either independently or in cooperation.

This law regulates the duties of controllers and processors of personal data. Articles 20 to 50 of the regulatory framework outline the responsibilities of the personal data controller. Included in this duty is the obligation to protect the privacy of personal data and to take reasonable measures to prevent its disclosure or use by any third party without the prior permission of the data subject. The responsibilities of personal data processors range from Article 51 to Article 52. These obligations include, inter alia, the obligation to process

[15] Siti Yuniarti, *"Legal Protection of Personal Data in Indonesia"*, Journal Business Economics, *Communication, and Social Sciences*, 2019, pp. 152.

personal data solely based on orders from the personal data controller, and the necessity to obtain written consent from the personal data controller before engaging in additional processing of personal data.

According to Law no. 27 of 2022, the rights of persons whose personal data are processed, as described in Articles 8, 9, 10, and 13 (paragraphs 1) and (2), may be waived in certain situations. Defense concerns the security and safety of a nation. Concerns with the criminal justice system. Theories of public interest concerned with government policymaking. Financial services, such as money, payment methods, and financial system stability, fall within the scope of state administration. Individuals express a tendency towards statistical pursuits and scientific investigations.

Article 58 paragraph of this law stipulates that the government is responsible for the implementation of Personal Data Protection measures. (1). The implementation of Personal Data Protection is responsible for the implementation of Personal Data Protection as referred to in paragraph (1). Furthermore, the determination of the institution in question is carried out by the President and the accountability lies with the President.

The business entity in Article 58 paragraph (2) undertakes: a. Development and establishment of Personal Data Protection safeguards policies and strategies, which serve as directions for Personal Data Subjects, Personal Data Controllers and Personal Data Processors. Supervise the implementation of Personal Data Protection measures. Implementation of administrative measures to enforce compliance with this law. The act of facilitating the resolution of disputes outside the court system.

In addition to the institution as referred to in Article 58 paragraph (2) authorized to: a. Develop and implement regulations relating to the security of personal data. Oversee the Personal Data Controller's compliance with regulatory requirements. In the event of a breach by the Personal Data Controller or Personal Data Processor of Personal Data Protection, administrative sanctions shall be imposed. The purpose of this law is to assist law enforcement in investigating and prosecuting crimes that may involve personally identifiable information. Work with similar organizations in other countries to investigate and remedy possible personal data protection violations at an international level. Examine whether the requirements for sending Personal Data outside the Unitary State of the Republic of Indonesia have been fulfilled or not. Instruct the Personal Data Controller and/or Personal

Data Processor in a way that enables you to track their progress because of your supervision. Report the results of your efforts to enforce rules designed to protect personally identifiable information. Complaints and/or reports about possible violations of the Personal Data Protection Act are reported to the relevant organization. Follow up on suspected violations of Personal Data Protection by investigating complaints, documentation, and/or tracking results. Find and notify all parties found to be involved in a Personal Data Protection breach claim. People are trying to get private and public organizations to hand over information, data, and documents related to privacy breaches they believe have occurred. Gather and display expertise necessary for investigations and investigations into possible violations of laws protecting personally identifiable information.

Article 62 of Law No. 27 of 2022 concerning international cooperation arrangements. The first paragraph explains that international cooperation measures are carried out by governments together with other governments or international bodies concerned with securing personal data. Paragraph (2) explains that the implementation of this Law through international cooperation is guided by established provisions and basic principles of international law. In addition, the public has the potential to contribute to the enforcement of Personal Data Protection, either through direct or indirect means. Education, training, advocacy, outreach, and supervision are examples of ways to engage in the community and follow the law.

In Chapter XIII, Article 65, Paragraph (1), the law prohibits the use of personally identifiable information. In particular, no one is allowed to steal someone else's identity for financial gain or other purposes, as this may cause the victim's confidential information to be compromised. Violation of the rules and regulations outlined in this article may be subject to a fine of up to Rp. 5,000,000,000.00 and/or a maximum imprisonment of five years as referred to in Article 67 Paragraph 1. (1). Subsection (2) clarifies that no one may share another person's personal information without that person's consent. Article 67 paragraph 2 regulates criminal sanctions, including imprisonment for a maximum of four years and/or a maximum fine of Rp. 4,000,000,000.00 for acts contrary to the laws and regulations outlined in this article. (2). Pursuant to paragraph 3, no one shall use another person's Personal Information unlawfully. As mentioned in Article 67 Paragraph 1, criminal threats for ignoring the provisions and laws mentioned in this article can be threatened with imprisonment for a maximum of five years and/or a maximum fine of Rp. 5,000,000.000.00.

Article 66 of the regulation regulates the prohibition of falsifying or falsifying Personal Data. It is stated that people cannot perform these acts as they may cause harm to others and their participation in them is prohibited. Criminal penalties for violations of this rule include imprisonment for a maximum of six years and/or a maximum fine of Rp. The amount is Rp. 6,000,000,000.00 as required in Article 68. Additional penalties may be imposed through confiscation of profits and/or property obtained or obtained unlawfully, and the granting of restitution as referred to in Article 69, in addition to the penalties stipulated in Articles 67 and 68.

The potential legal consequences for business actors in the event of a data leak are regulated in Article 70 of Law Number 27 of 2022. In particular, the law recognizes companies as legal entities subject to personal data regulations.

According to Article 71 paragraph (1) of the court deed, the court that issued the fine gives time to the convicted person to pay the fine for one month, starting from the date the judgment has permanent legal force. As long as there is an urgent reason, the time referred to in paragraph (1) may be extended for a maximum of another month in accordance with the details in paragraph (2). If the fine is not paid within the period specified in paragraphs 1 and 2, the procuratorate may confiscate and sell the offender's property or income to cover the debt. If the confiscation and sale of property or income as referred to in paragraph (3) is insufficient or cannot be implemented, the unpaid fine is replaced by the maximum imprisonment for the crime concerned as referred to in paragraph (4). The period of detention as referred to in paragraph (4) is determined by the presiding judge and set forth in an official court decision, as described in paragraph (5) of the deed.

If the confiscation and sale of assets or income as referred to in Article 71 paragraph (4) is carried out against the convicted company and is considered insufficient to settle the crime, the corporation may be subject to other alternatives in accordance with paragraph (1) of Law No. Article 72 sanctions, including temporary suspension or for a maximum part or all of its business activities for a period of up to five years. In accordance with paragraph (2), the court determination must determine the period for stopping the Company's business activities, either temporarily or permanently, in accordance with paragraph (1). Additional criminal sanctions in the form of restitution are subject to the provisions in Article 71 and Article 72 as referred to in Article 73.

In the contemporary age of globalization, our individual information is stored in databases of corporate entities and government bodies. This is a direct result of our actions, such as registering in various applications and providing personal information traceable back to us. After looking at the provisions outlined in the PDP Law, what are the legal implications in case of a breach of personal data? Before further discussion, it is important to acknowledge that the personal data controller bears the responsibility for safeguarding and guaranteeing the security of personal data under the scope of its processing. This obligation requires the development and implementation of operational and technical measures aimed at protecting personal data from potential interference that may arise during the processing stage. In addition, it assesses the level of safeguarding of an individual's personal information considering the characteristics and potential dangers associated with personal data that require protection during the processing of such data. Within 72 hours of becoming aware of a breach of personal data security, the supervisor is required to notify affected individuals and institutions in writing. Personal data managers have a responsibility to notify the public if a security breach causes substantial disruption to public services or harms the interests of the community.

According to Article 47 of the PDP, the personal data controller is responsible for its processing and must demonstrate accountability by fulfilling its duty to respect the principles of personal data protection. In the event of a violation of Article 46 paragraphs (1) and (3) or Article 47 of the PDP Law, the relevant administrative authority may issue a written reprimand, temporarily suspend the violator's personal data processing activities, order the violator to delete or destroy the personal data in its possession, or levy administrative fines. The institution is authorized to impose administrative sanctions, which may be fines of up to 2% of the entity's annual income or income for various violations.

## D. Conclusion

In the perspective of international law, the protection of human rights towards the protection of personal data that is private originates from the Universal Declaration of Human Rights 1948 (UDHR) which is the first international instrument that protects a person’s right to privacy. On the other hand, there is the General Data Protection Regulation (GDPR) by the European Union which contains principles and rules for the protection of personal data that can be used as a reference by countries that will make or design rules on personal data protection. This is also supported by the creation of International Law rules in

harmonizing this matter, including International Convenant on Civil and Polittical Rights (ICCPR), Council of Europe, European Union, Charter of Fundamental Right of the European Union (CFREU).

When it comes to the protection of personal data in Indonesia itself, there are rules that are clearly regulated. It is regulated by Law No. 27 of 2022 on the Protection of Personal Data. The General Terms, Types of Personal Data, Rights of Data Owners, Personal Data Processing, Responsibilities of the Controller and Processor in the processing of personal data, Personal data Transfer, Prohibition in the Use of Personal Data, Establishment of Guidelines for the Conduct of the Personal Data Controller, Exception to Personal Data Protection, Dispute Resolution, International Cooperation, Public Role, Criminal Clauses, Transition Clauses and Closing Clauses.

## E. Suggestion

After conducting a thorough analysis of several scientific publications related to personal data, it has been determined that safeguarding personal data is the most important thing. It is anticipated that the public will be increasingly aware of the importance of protecting personal data in the current era of globalization, thus negating the need for inadvertent disclosure of such information. happen. Participation from both the public and the government is expected to increase in securing personal data, especially in the territory of Indonesia.

## References

### Books

Rahardjo, Satjipto. *Progressive Law: A Synthesis of Indonesian Lawa.* Yogyakarta: Genta Publishing, 2009;

Strake, J.G. "Introduction to International Law". Vol. 10. Jakarta: Sinar Grafika, 2010;

Themba, Milton. *The Right to Privacy and Identity on Social Network Sites: A Comparative Legal Perspective*. *thesis*, University of South Africa, 2009:

Soekanto, Soerjono. *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*, cet. 9. Jakarta, Rajawali Press, 2006;

### Journals

Kuner, Christopher. "The European Union and the Search for an InternationalData Protection Framework". Groningen Journal of International Law. Vol. 2;

Richards, Neil and Hartzog, Woodrow. Taking Trust Seriously in PrivacyLaw. *Stanford Technology Law Review*, Volume 19:431, 2016;

Yuniarti, Siti. "Legal Protection of Personal Data in Indonesia", *Journal of Business Economics, Communication, and Social Sciences*, Vol. 1 No. 1, 2019;

**Laws**

Law Number 12 of 2011 as amended by Law Number 15 of 2019 concerning the Establishment of Laws and Regulations stipulates that content material regarding criminal provisions can only be contained in the Law, Provincial Regional Regulations, or District/City Regional Regulations;

Law of the Republic of Indonesia Number 27 of 2022 concerning Personal Data Protection.

**Reports and Conferences**

Elsam and Commission I of the House of Representatives, Term of Reference (TOR) Representative of the Secretariat of Commission I of the House of Representatives and the PDP Bill Assistance Team Secretary General of the House of Representatives of the Republic of Indonesia "Discussion of the Problem Inventory List (DIM) of the Personal Data Protection Bill" Focus Group Discussion, Century Park Hotel, July 22, 2020;

Rachmatul, *Data Collection Techniques in Quantitative and Qualitative Research.* IAIN Syekh Nurjati Cirebon, 2013;

**Others**

Djafar, Wahyudi. " Personal Data Protection Law in Indonesia: Landscape, Urgency and Need for Update";

Wahyudi, Djafar and Sumigar Bernhard Ruben Fritz, S. B. L. 2016. *"Protection of personal data in Indonesia"*, Available on website:

http://weekly.cnbnews.com/news/article.html?no=124000, Accessed March 31th, 2023.