Legal Review of Personal Data Regulations In The Personal Data Protection Law

Mardisontori

{mardisontorirajulan@gmail.com}

Universitas Borobudur

Abstract. Protecting personal data has become crucial in today's era of rapid technological advancement and information systems. Legal requirements to safeguard personal data reflect efforts to uphold human rights, as mandated by the Indonesian constitution. The numerous issues in data and information management highlight the growing importance of legal frameworks in personal data protection to defend Indonesian citizens from data breaches and cybercrimes, while reinforcing Indonesia's sovereignty internationally. Technological progress has led to widespread data-related issues across various social groups, making robust Personal Data Protection regulations crucial for Indonesia. This article explores the principles of personal data protection and examines the regulatory framework provided by the Personal Data Protection Law. The research utilizes a normative juridical approach, covering topics like the definition of personal data, rights of data owners, duties of data controllers and processors, data handling procedures, as well as the role of data protection authorities.

Keywords: Personal data protection, regulation, human rights

ICL-C 2023, November 11, Jakarta, Indonesia
Copyright © 2025 EAI
DOI 10.4108/eai.11-11-2023.2351324

1 Introduction

The Preamble of the Indonesian Constitution Year 1945 (UUD NRI Year 1945), the 4th paragraph, implies that The Government of Indonesia is constitutionally obligated to protect the entire Indonesian nation, promote the general welfare, educate its people, and contribute to a world order grounded in independence, lasting peace, and social justice. Amid the significant expansion of information and communication technology, this national purpose extends to safeguarding every Indonesian resident's and its citizens' personal data.

In its evolution, particularly following the 1945 amendment of the Indonesian Constitution, the right to privacy—including personal data protection—has been acknowledged as citizens' constitutional right. This aligns with the dedicated section on Human Rights within the constitution, specifically in Chapter XA, Articles 28A-28J. Indirectly, the assurance of personal data protection is embedded in Article 28G, paragraph (1) of the 1945 Constitution, which states "Everyone has the right to protection for the protection of himself, his family, his honour, dignity and property under his control, and to security and protection from the threat of fear to do or not to do something which is a human right".

Beyond its constitutional guarantees, Indonesia's role as a state party to the International Covenant on Civil and Political Rights (ICCPR) further emphasizes the government's duty to safeguard the privacy and personal data of its citizens. This aligns with Law No. 39 of 1999 on Human Rights (Human Rights Law), which includes articles that ensure the right to privacy for citizens. For example, Article 29, paragraph (1) of the Human Rights Law acknowledges an individual's right to personal protection, family honor, dignity, as well as property. This protection extends beyond direct interactions to cover personal information and data. In addition, Article 31 of the Human Rights Law states that privacy in electronic communications is safeguarded, except when disclosure is authorized by a judge or other lawful authority, as per legal provisions.[1]

Information and communication technology, as a form of innovation, nowadays enables the collection, storage, sharing, and analysis of data. These advancements have led to the widespread application of information and communication technology across some sectors, including e-commerce in trade and business, e-government in governance, social media platforms, search engines, smartphones with mobile internet. Also, the growth of the cloud computing industry.

The need for regulations on personal data protection gained prominence as the number of mobile phone as well as internet users grew, that directly or indirectly led to a rise in personal data breaches. These breaches have resulted in various non-criminal issues. For example, fraud and pornography. This trend highlights the important need for comprehensive legislation to safeguard personal data.

Personal data protection arrangements is actually based on the philosophical foundations of each country. The philosophical foundation is important because it has justifiable reasons, if thought deeply, especially on the way of life of a nation that contains the moral and ethical values of the nation.[2]

Privacy laws in the USA focus on repairing consumer losses and damage also balancing privacy with effective commercial transactions. While in Europe, privacy is positioned as a principle right that can trump interest of others.[3] Indonesia is also physiologically different from America and countries in Europe, however, there are universal standards that must be met while still paying attention to the content material applicable in Indonesia. The philosophical basis of the Law on Personal Data Protection is based on the legal ideals of the preamble to the 1945 NRI Constitution, namely the purpose of the formation of the state is to protect the entire Indonesian nation, and all Indonesian bloodshed. This implies that the State is obliged to provide protection human rights and guarantee them, that includes the protection of personal data, as mandated by paragraph (1) Article 28G of the Indonesian Constitution of 1945.

Furthermore, personal data protection is recognized as a human right in both regional human rights frameworks and international, with Indonesia legally bound by the 1966 ICCPR and the Association of Southeast Asian Nations. In addition to that, personal data protection is addressed in international cooperative frameworks involving Indonesia, like the 2004 APEC Privacy Framework. Sociologically, Indonesian society is now part of the global information society, existing in an interconnected world. Moreover, safeguarding personal data privacy is important to ensure security and protection for both foreign nationals and Indonesian citizens in Indonesia concerning the collection, processing, management, then sharing of personal data.

Legally, Indonesia has many laws and regulations that partially address personal data protection; but, these have yet to provide maximum protection and legal certainty for personal data. Around 30 laws and regulations touch on aspects of personal data protection but still fall short of ensuring legal certainty and security for the public. Some regulations include: Law No. 19 of 2016 amending Law No. 11 of 2008 on Electronic Information and Transactions, Law No. 14 of 2008 on Public Information Transparency, Government Regulation No. 82 of 2012 on the Operation of Electronic Systems and Transactions, and Ministry of Communication and Information Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems.[4]

The Personal Data Protection Law aims to protect the fundamental rights and freedoms of citizens, particularly regarding personal data. It seeks to make it sure that governments, businesses, and organizations adhere to personal data protection standards, fostering legal certainty and promoting growth within the technology, information, as well as communication sectors. Indonesia as a populous democratic nation, addressing personal data protection issues has become an urgent necessity for its country.

1.1 Problems

The problems to discuss what are the principles of implementing personal data protection? what are the substances of the personal data protection regulations in the Personal Data Protection Law?

1.2 Purpose

As for the aim of this paper, it is to understand the principles of implementing personal data protection, as well as understand the personal data protection regulations in the Law concerning Personal Data Protection.

2 Method

The writing employs a normative juridical method that uses a statutory approach, focusing on literature related to personal data protection and the issues that arise, by analyzing primary, secondary, as well as tertiary data sources.[5] The problems and analysis in this paper are presented in a descriptive analytic manner, which provides a clearer picture of the law concerning Personal Data Protection and content material that regulated therein. To gain a more comprehensive understanding, a comparative study of secondary data relating to personal data protection arrangements was conducted in other countries such as the Philippines, South Korea, and the European Union.

3 Result and Discussion

3.1 Conceptual Framework

3.1.1 Problems in the Field of Personal Data Protection

Sideways with the advance of information and communication technology that is increasingly massive, several problems in relation to personal data are increasing. In recent years globally there have been many cases of personal data leakage affecting Indonesia. The latest problem that is most horrendous is of course the case of the leak of President Joko Widodo's Identity Number (NIK) on the internet some time ago. It was stated that the NIK was obtained from the official website of the General Elections Commission on the form of the Indonesian presidential candidate for the 2019 election. This problem was certainly troubling, because NIK is very important personal data and must be kept confidential, because NIK can be used to access and abuse many things, including various applications that exist. In addition, it is unfortunate that the relevant agencies actually threw responsibility for this incident on each other.[6] Another incident that is quite worrying is the leak of 15 million personal data of users of Tokopedia, one of the leading e-commerce platforms in Indonesia. Even worse, the party who leaked the personal data also claimed to have and would sell 91 million Tokopedia user data and then traded for USD 5,000 or around 70 million rupiah, even the data can now be downloaded freely.[7]

This data leak case is the second time it has occurred on an e-commerce platform, after in 2019 there was also a data leak of 13 million Bukalapak user accounts. Personal data leaked in the form of emails, usernames, passwords, salts, hashed Facebook, emails, user addresses, to phone numbers. At that time, the personal data was sold separately with a total value of 1.2431 Bitcoin or about USD 5,000 or equivalent to 70. 5 million rupiah.[8] This shows that structuring regulations in the personal data protection sector is crucial for Indonesia to have at this time. The potential violation of the right to privacy of personal data not only exists in online activities, but also off-line ones. Possible online violations include activities such as mass collection of personal data (digital dossiers), direct marketing, social media interactions, the execution of electronic ID card programs, the implementation of e-health initiatives, as well as cloud computing operations.

In addition, another form of neglect of privacy protection is the emergence of an advertising message commonly called Location-Based Messaging. The message will be sent automatically to someone if they are in a certain place. While on the other hand, not necessarily someone has agreed to an agreement with the provider and gave an agreement to record every activity. The subsequent potential breach regarding personal data is then the digital dossier. This process involves the large-scale collection of an individual's personal data through digital technology. The government began utilizing digital dossiers in the 1970s, particularly in European countries and the USA. Today, the private sector has also adopted digital dossiers through internet technology. These private-sector activities related to digital dossiers pose a risk of infringing on an individual's human rights concerning their personal data.[9]

The popularity of social media and friendship sites has resulted in many cases of privacy violations. Personal data belonging to a person can be easily accessed and disseminated without the knowledge of the data owner. In addition, potential violations of privacy can also arise from government programs involving private parties, such as e-KTP and e-health programs. By using the device in the e-KTP, every citizen can be tracked for his whereabouts and activities, which can potentially cause violations of citizens' human rights.

The issues mentioned above are not matched by a corresponding rise in public awareness regarding the protection of personal data. While some people object to their personal data being shared without consent and an increasing number of individuals and groups advocate for personal data protection laws, societal conditions reflect a different reality. In Indonesia, personal data is not regarded as something that requires safeguarding. This is evident in the extensive amount of personal data shared on social media. Moreover, the significant growth in e-commerce platforms over the past few years has not been accompanied by a clear understanding of privacy policies or terms and conditions in relation to personal data usage in these applications.[4]

The preparation of regulations in the field of personal data protection in the form of laws is expected to be able to answer various problems that occur in society. The preparation of comprehensive regulations governing personal data protection will provide personal data protection in Indonesia that is equivalent to other countries. Indirectly, this will encourage and strengthen Indonesia's position as a trusted country, especially in the economic sector which will become an important point in the Indonesian national economy.

In addition, regulations concerning personal data protection will help reduce the risk of personal data misuse in industries such as banking as well as on online social platforms. The aim of these regulations is to protect and ensure the rights of every individual, regardless of nationality, ethnicity, or residence, in relation to the storage and processing of personal data, as well as their rights and freedoms, specifically the right to privacy.

3.2.1 Conception and Theory of Personal Data Protection

Personal data protection law actually develops in tandem with the development of technology itself. This is because personal data is a dynamic aspect, which will continue to be influenced by technological advances as well as business practices. One of the factors for the emergence of crime and unlawful use of personal data is caused by the development of ICT. Currently, ICT has penetrated almost all aspects of life and changed people's behavior towards electronic and internet-based interaction.

The use of information technology and communication media has changed the behavior of society and human civilization globally and caused human interaction to be borderless. However, information technology is now a double-edged sword, because in addition to contributing to improving welfare, progress is also an effective means of unlawful acts. United Nations Resolution N0.68/167 on the right to privacy in the digital age, reminds of the many arbitrary and unlawful surveillance and interception practices of communication, including the arbitrary collection of personal data, which are violations of the right to privacy.

In addition, Article 17 of the ICCPR stipulates that the collection or storage of personal information on computers, databases, and other devices—whether by public authorities or private individuals and entities—must be governed by law. The state is required to implement effective measures to ensure that information concerning a person's private life is not accessed by individuals who are not legally authorized to receive, process, or utilize it.[10] Several regional organizations have started addressing personal data protection, including the establishment of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in 1981, which was revised in 2018. Additionally, the Organization for Economic Co-operation and Development (OECD) introduced guidelines on the protection of privacy and transborder data flows of personal data in 1980, which were updated in 2013. In the Asian region, APEC released the APEC Privacy Framework in 2004, which was also amended in 2015.

A major advancement in personal data protection law took place when the European Union enacted the EU GDPR (General Data Protection Regulation) in 2016, that became effective in 2018. The GDPR is extensive, as it unifies data protection laws and encompasses nearly all aspects of personal data processing. Its implementation impacts not only data controllers and processors located in the European Union but also entities that provide goods or services to, or track the behavior of, individual EU citizens. By the end of 2019, over 125 countries had enacted their own data protection laws.

a. Privacy Concept

Personal data is a component of privacy that requires protection. It is recognized in various international, regional, and national legal frameworks. But, there is no universally accepted definition of privacy or personal data, as their scope is highly dynamic and evolves with societal context and technological advancements in daily life. Additionally, Edmon Makarim outlines three essential principles regarding personal rights: the right to be free from interference in one's personal life, the right to keep sensitive personal information confidential, and the right to control how one's personal data is used by others. In terms of personal rights as human rights, it is noted that safeguarding personal or private rights enhances human values, fosters better relationships between individuals and their communities, promotes independence and autonomy in managing personal data, and encourages tolerance while reducing discriminatory treatment and limiting governmental power.[11] In general, there are six concepts of privacy that develop in international debates, namely:[12]

In general, there are six concepts of privacy that develop in international debates, namely:

i. The right to privacy is understood as the right to be left alone, that has formed the foundation for contemporary privacy law concepts.

ii. The right to privacy is viewed as restricted access to oneself, highlighting the individual's desire for seclusion from others. But, this notion of limited access does not equate to solitude, isolation, or withdrawal. While solitude is a part of this concept, it encompasses a broader understanding that includes freedom from government interference and intrusion by the media and others.

iii. The right to privacy is framed as secrecy, which involves keeping certain aspects hidden from others. One common understanding of privacy is the confidentiality of specific information. This idea of privacy as confidentiality can be seen as a facet of limited access to oneself.

iv. The right to privilege is characterized as the control over personal information. This notion is one of the most influential theories of privacy, defining it as the ability to determine when and by whom aspects of oneself can be perceived by others. The essence of privacy lies in controlling who can see, hear, touch, smell, or feel us.

v. The right to privacy is conceptualized as personhood, focusing concerning the protection of individuality, personality, and dignity. This understanding safeguards a person's identity and autonomous actions, serving as a coherent framework against degrading treatment, insults to personal dignity, and attacks on human personality while supporting the individual's interest in being and remaining a person.

vi. The right to privacy is seen as intimacy, which involves controlling limited access to one's relationships and aspects of life. This concept acknowledges that privacy is crucial for both personal identity and human relationships. One strength of this perspective is that it extends the moral personality beyond mere rational autonomy, viewing privacy as involving some form of limited access or control, as well as emphasizing its importance in fostering personal connections.[13]

b. Concept of Personal Data

Personal data is often synonymous with the term "personal data" in Europe and "personal information" in the USA. According to the Big Indonesian Dictionary (KBBI), personal data encompasses information related to a person's characteristics, such as name, age, gender, education, occupation, address, and family role. In paragraph (1) Article 4, of the GDPR, personal data is defined as information connected to an identified or identifiable natural person. The GDPR intentionally uses a broad definition of personal data, allowing European legislators to include any data that could potentially relate to an individual.[14] Orla Lynskey identifies two distinct concepts within personal data and privacy. Firstly, unlike "privacy intrusion," the concept of personal data is not context-dependent. Secondly, the definition of personal data includes data related to individuals who are unknown but identifiable. This narrows the scope of personal information to data specifically connected to individuals. Personal data protection is a human right, that is part of the broader right to privacy, safeguarded by both international legal instruments and national constitutions. This implies that an identifiable person is someone who can be directly or indirectly recognized based on an identification number or specific physical, psychological, mental, cultural, or social characteristics. Personal data protection mechanisms cover natural persons, not legal entities .

c. Principles of Implementation of Personal Data Protection

The implementation of personal data protection has to be carried out on various important principles, because the implementation of personal data protection must be carried out without violating human rights. Some principles in the implementation of personal data protection implemented based on the law are:

i. Principles of lawfulness and transparency

This principle is based on each individual being informed and knowing clearly how their data will be processed, and by whom it is processed and stored. The individual should also be aware of whether the data will be shared with third parties. If an individual is not clearly informed or unaware of this fact, it is likely that their personal data was not collected transparently or fairly. A person's information should not be processed or gathered in an unfair or unlawful way, nor should it be used for purposes that go against humanity principles.

ii. Principle of purpose limitation

The purpose of this principle is to ensure that personal data handlers collect, use, or disclose an individual's personal data only for legitimate purposes. All personal data must be collected for specific and lawful purposes. The data's processing and use must be clearly defined and communicated to the data subject, and personal data should not be disclosed, provided, or used for purposes beyond those specified. Nevertheless, exceptions apply if the data owner consents; such consent must be unconditional, free from hidden intentions, as well as carried out by authorized legal entities.

iii. The principle of data minimization

This principle of data minimization requires the party processing the data to consider the minimal data essential to attain the objectives of the data processing. Data processors cannot receive and collect additional data due to the possibility of useful or other reasons. In the era of rapid technological progress in recent times, this principle is needed because technological advances and capabilities massively improve analytical techniques to seek and collect to develop intelligence and knowledge.

iv. Accuracy principle

The accuracy principle implies that personal data must be correct and up-to-date to meet its intended purpose. This principle obligates those collecting and storing personal data to periodically verify the data's accuracy and relevance, ensuring that records are as complete as possible to prevent errors or omissions. Moreover, data should be periodically updated or reviewed whenever the information is accessed, for as long as it is being processed.

v. Storage limitation principle

The storage limitation principle holds that personal data should only be retained in a form that is essential for processing purposes. Data may be stored for extended aeras solely for archiving in the public interest, or for scientific, historical research, or statistical drives.

vi. Principles of confidentiality and security

These principles emphasize that personal data must be handled with strict confidentiality. In addition it must be handled with implementing suitable organizational, administrative, physical, and technical measures to safeguard data security. These measures should protect against unauthorized or accidental access, damage, loss, or any other risks associated with data processing. Moreover, personal data must be shielded from risks such as unauthorized access, usage, or disclosure, as well as from loss, damage, or destruction.These principles emphasize that personal data has to be handled with strict confidentiality, implementing suitable organizational, administrative, physical, and technical measures to safeguard data security. These measures should protect against unauthorized or accidental access, damage, loss, or any other risks associated with data processing. Moreover, personal data must be shielded from risks such as unauthorized access, usage, or disclosure, as well as from loss, damage, or destruction.

vii. Principle of accountability

The accountability principle is vital to enforcing personal data protection, as it encompasses responsibility and obedience to data protection practices. The data controller, who manages personal data, must be able to demonstrate compliance with legally established data processing principles. This accountability includes both legal approvals and adherence to ethical standards. Personal data should be processed fairly, with the data owner's consent and in their best interest.[15]

2. Subject Matter In The Personal Data Protection Law

Broadly speaking, there are some basic things that are very significant in the Law on Personal Data Protection. By regulating some of these substances as content material, Indonesia will make Indonesia a country that is considered equal in the international world in terms of data protection and will become a country that is friendly to investors. It is hoped that the achievement of this goal will make Indonesia's national economy stronger, but in contrast, state sovereignty in the digital field is also progressively maintained. This procedure will protect individuals' personal data against misappropriation when the data is of high value to commercial interests. They include:

a. Definitions and Types of Personal Data

   An important element in the protection of personal data is the definition of personal data itself. In Indonesia, the definition of personal data can be found in Government Regulation Number 82 year 2012 concerning the Implementation of Electronic Systems and Transactions (PP concerning PTSE). According to The Government Regulation on PTSE, personal data is defined as "certain individual data that is stored, maintained, and kept true and protected confidentially".[16]

b. Processing of Personal Data

   The processing is the next content material that is important to be regulated in the Law on Personal Data Protection. Data processing activities will describe how individual personal data is treated by both the data controller also the data processor. Then the definition of personal data processing should be broad, in order to encourage Indonesia

to innovate and progressively respond to technological advances in data analysis methods. In addition, it is very important to include data integration activities in the processing definition.[16]

c. Controllers and Processors of Personal Data

Personal data controllers and processors are parties concerned with personal data processing activities. According to the EU GDPR, personal data controllers are "a natural or legal person, public authority, agency or other body that alone or jointly with another person, determines the purposes and means of processing personal data, where the purposes and means of such processing are determined by EU or member state law". [16]

While a personal data processor is "a natural or legal person, public authority, agency or other body that processes personal data on behalf of the personal data controller". Based on this definition, there are 3 elements that are key in defining personal data controllers and personal data processors, namely: parties, conducting alone or jointly, and determining the purposes and ways of processing personal data.

d. Rights of Personal Data Owners

The owner of personal data is the key subject in the implementation of personal data protection. Personal data protection arrangements in law will ensure that the rights of the owner of personal data are protected.

e. Transfer of Personal Data

In today's era of globalization, geographical boundaries are less relevant in terms of data sovereignty and security. Therefore, although the core purpose of the Law on Personal Data Protection is to maximally accommodate national interests and protection of citizens, it still takes into account the interests of other countries or the international community. Therefore, the regulations in the Law on Personal Data Protection at least meet global standards. This will facilitate international association and governance, including in terms of international trade, investment and financial activities.

f. Supervisory Agencies

One very important element in ensuring the effective implementation of a law is the existence of a supervisory authority. Some countries that apply the two concepts of the institution include:

1. Malaysia

Malaysia is one of the countries that has adopted the initial institutional typical. In Malaysia, the minister is legally empowered to appoint an individual as the personal data protection commissioner. The main role of the commissioner is to perform the functions and exercise the powers granted under Malaysia’s data protection law, as well as the commissioner is accountable to the minister.

2. The UK

The UK has The Information Commissioner's Office, an agency whose primary task is to uphold information rights and to ensure the protection of information rights in the public attention. The Information Commissioner's Office not only guarantees the rights

under the Data Protection Law, but also guarantees the information rights set out in the Privacy and Electronic Communication Regulations, the Environmental Information Regulation, the Freedom of Information Law, the INSPIRE Regulation, and the Re-Use of Public Sector Information Regulation.

3. Germany

In Germany, there is an institution called the Federal Commissioner for Data Protection and Freedom of Information. This institution is tasked with overseeing compliance with data protection, both carried out by public bodies, as well as postal and telecommunications service providers. This institution also has a very important role, because it is the only institution that is in the middle between industry and government.

4. Canada

Things are quite different in Canada, where both the privacy acts and the Personal Information Protection and Electronic Document Act (PIPEDA) are overseen by the Federal Privacy Commission of Canada, which is an official from parliament appointed by and must report to the Canadian parliament. The commissioner also has broad investigative powers, including to forcibly summon witnesses, enter a person's residence to obtain documents and conduct interviews, and to make recommendations, but is not authorized to issue orders or impose legal sanctions. PIPEDA also requires each organization to appoint one person as a data protection officer, the employee responsible for the organization's policies and practices and to whom criticisms and investigations can be forwarded.[17]

4 Conclusion

Indonesia as the world's fourth most populous democracy faces an increasingly urgent need for national regulations on personal data protection. Numerous issues have emerged within society and government administration, including widespread data leaks, personal data theft, misuse of personal information, and the lack of a unified, comprehensive national regulation on personal data protection. Personal data protection is an aspect of human rights safeguarded by the constitution.

In today's era of rapid technological and information advancement, the existence of a country's geographical borders is no longer an obstacle in the potential for international relations, increased international transactions, as well as potential destructions and crimes against Indonesian citizens. Some problems that often occur in the field of personal data include digital dossier activities, direct marketing, location-based messaging.

The Personal Data Protection Law now governs the content related to personal data, its processing, the errands of data controllers and processors, data transfers, and the institutions that oversee personal data protection. Comprehensive regulations in the digital field and the protection of citizens' personal data are anticipated to address various existing issues and strengthen Indonesia’s position alongside other countries internationally.

References

[1] Wahyudi Djagfar, “Personal Data Protection Law in Indonesia: Landscape, Urgency, and Need for Update,” 2023, [Online]. Available: https://law.ugm.ac.id/wp-content/uploads/sites/1043/2019/08/Hukum-Perlindungan-Data-Pribadi-di-Indonesia-Wahyudi-Djafar

[2] G. T. Suteki, “Legal Research Methodology (Philosophy, Theory, and Practice),” 2018.

[3] P. M. Schwartz and D. J. Solove, “Reconciling personal information in the United States and European Union,” *Calif. Law Rev.*, vol. 102, no. 4, pp. 877–916, 2014, doi: 10.2139/ssrn.2271442.

[4] Wahyudi Djagfar, “Personal Data Protection Law in Indonesia: Landscape, Urgency, and Need for Update,” *Postgrad. Program, Fac. Law, Gadjah Mada Univ.*, vol. 1, no. 1, pp. 147–154, 2019, [Online]. Available: https://law.ugm.ac.id/wp-content/uploads/sites/1043/2019/08/Hukum-Perlindungan-Data-Pribadi-di-Indonesia-Wahyudi-Djafar.pdf

[5] Soerjono Soekanto, “Introduction to Legal Research,” 2005.

[6] Ahmad Naufal Dzulfaroh, “When Jokowi’s KPT Number (NIK) Leaked...,” *Kompas*, 2023. [Online]. Available: https://www.kompas.com/tren/read/2021/09/04/170500165/saat-nomor-ktp-nik-jokowi-bocor-?page=all

[7] Rian Alfianto, “91 Million Tokopedia Account Data Leaked and Spread on Internet Forums,” *Jawa Pos*, 2023. [Online]. Available: https://www.jawapos.com/oto-dan-tekno/teknologi/05/07/2020/91-juta-data-akun-tokopedia-bocor-dan-disebar-di-forum-internet/

[8] Adhi Wicaksono, “13 Million Bukalapak Leaked Data Sold on Hacker Forum,” *cnnindonesia*, 2023. [Online]. Available: https://www.cnnindonesia.com/teknologi/20200506065657-185-500477/13-juta-data-bocor-bukalapak-dijual-di-forum-hacker

[9] Daniel J. Solove, “The Digital Person, Technology and Privacy in the Information Age,” *West Group Publication, New York: New York University Press*, p. 17, 2014.

[10] UN Human Rights Committee (HRC), “The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation,” *CCPR Gen. Comment*, vol. 16, no. 17, 1988, [Online]. Available: https://www.refworld.org/docid/453883f922.html,

[11] Jakarta: Rajawali Pers, “Legal Responsibility of Electronic System Operator,” 2010.

[12] D. Budhijanto, “Telecommunications, Broadcasting and Information Technology Law: Regulation and Convergence,” in *Bandung: PT. Rafika Aditama*, 2010, p. 4.

[13] D. J. Solove, “‘Part of the Law Commons Recommended Citation Recommended Citation Daniel J. Solove, Conceptualizing Privacy, 90 Cal,’” *L. Rev*, vol. 1087, p. 1087, 2002, [Online]. Available: https://scholarship.law.gwu.edu/faculty_publications

[14] W. D. dan M. J. Santoso, “Protection of Personal Data: Recognizing the Rights of Data Subjects, as well as the Obligations of Data Controllers and Processors,” *J. ELSAM Internet Hum. Rights Ed.*, p. 15, 2019.

[15] W. D. & M. J. Santoso, “Personal Data Protection: Its Concepts, Instruments, and Principles,” *ELSAM Journal, December*, p. 23, 2019.

[16] “European Union General Data Protection Regulation 2016/679, 2016”

[17] Andry Saputra, “Stag’s Personal Data Bill on Who Is the Supervisor, How Other Countries Are,” *news.detik.com*, 2023. [Online]. Available: https://news.detik.com/berita/d-5723232/ruu-data-pribadi-stag-soal-siapa-yang-jadi-pengawas-bagaimana-negara-lain