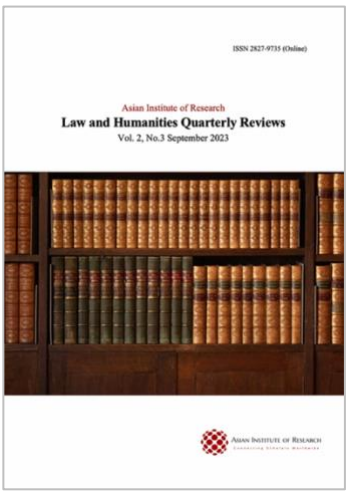

Law and Humanities Quarterly Reviews

Sitabuana, T. H., Adhari, A., Sanjaya, D., & Amri, I. F. (2023). The Importance of Personal Data Protection Act for The Protection of Digital Society in Indonesia. *Law and Humanities Quarterly Reviews*, 2(3), 128-141.

ISSN 2827-9735

DOI: 10.31014/aior.1996.02.03.77

The online version of this article can be found at:
https://www.asianinstituteofresearch.org/

Published by:
The Asian Institute of Research

The Asian Institute of Research Law and Humanities Quarterly Reviews is a peer-reviewed International Journal of the Asian Institute of Research. The journal covers scholarly articles in the interdisciplinary fields of law and humanities, including constitutional and administrative law, criminal law, civil law, international law, linguistics, history, literature, performing art, philosophy, religion, visual arts, anthropology, culture, and ethics studies. The Law and Humanities Quarterly Reviews is an Open Access Journal that can be accessed and downloaded online for free. Thus, ensuring high visibility and increase of citations for all research articles published. The journal aims to facilitate scholarly work on recent theoretical and practical aspects of law.

ASIAN INSTITUTE OF RESEARCH
Connecting Scholars Worldwide

The Asian Institute of Research
Law and Humanities Quarterly Reviews
Vol.2, No.3, 2023: 128-141
ISSN 2827-9735

DOI: 10.31014/aior.1996.02.03.77

The Importance of Personal Data Protection Act for The Protection of Digital Society in Indonesia

Tundjung Herning Sitabuana[1], Ade Adhari[2], Dixon Sanjaya[3], Ibra Fulenzi Amri[4]

[1] Faculty of Law, Tarumanagara University, Jakarta, Indonesia. Email: tundjung@fh.untar.ac.id
[2] Faculty of Law, Tarumanagara University, Jakarta, Indonesia. Email: adea@fh.untar.ac.id
[3] Faculty of Law, University of Indonesia, Jakarta, Indonesia. Email: dixonsanjaya@gmail.com
[4] Faculty of Law, Tarumanagara University, Jakarta, Indonesia. Email: ibra.205220249@stu.untar.ac.id

Correspondence: Tundjung Herning Sitabuana, Faculty of Law, Tarumanagara University, Jakarta, Indonesia.

Abstract
The era of technological disruption is marked by massive use of digital services and devices which always require submission of personal data free of charge. Digital companies can use personal data to identify behavior of their users freely without supervision. This is exacerbated by vulnerability of personal data protection due to hacking, mining or misuse of personal data, as happened with Facebook, Yahoo, Tokopedia, Bukalapak. In this phase, government has to active to provide protection which in Indonesian context is realized through formation of PDP Act as mandated by 1945 Constitution of Indonesia. This research intends to examine importance of PDP Act and its developments in Indonesia for digital society protection. This normative-empirical research uses primary data (observations and interviews) and secondary data (regulation searches and textual literature) that are processed qualitatively by content analysis. The idea of protecting personal data originates from recognition of the right to privacy that has developed and been institutionalized in various legal documents, both national, regional and international. In Indonesia, prior to enactment of PDP Act, personal data protection arrangements were scattered sporadically and sectoral which caused personal data protection to not be optimal. PDP Act complements and refines previous regulations to provide certainty for protection of personal data in Indonesia. The existence of PDP Act gives important meaning as a manifestation of state's commitment to provide protection, guarantee order and security of digital society, optimize law enforcement and reform personal data processing practices and encourage changes in society's culture to respect personal data.

Keywords: Act, Digital Society, Indonesia, Personal Data Protection, Privacy Rights

1. Introduction

The development and progress of technology have transformed the civilization of society with various benefits and challenges faced due to the use of technology. Almost all aspects of life involve technology and are connected in a global information and communication system network, both in industrial, business, financial, banking, education, health, trade, transportation, and government sectors. Especially in Indonesia, this technological disruption and intervention has driven 4.0 industrial revolution towards 5.0 industrial revolution. These changes are generally marked by the increased use of Internet of Things (IoT)-based technology,

information and communication systems, and digital industry. By using internet and high-technology digital devices, everything can be connected and controlled remotely through digital applications or information system networks provided by digital companies (Kusnadi & Wijaya, 2021).

Large companies engaged in technology and digital devices, such as Facebook, Twitter, Instagram, TikTok, WhatsApp, YouTube, and others, work by providing services or using available features (both free and paid) on digital devices. Instead, digital companies obtain rights or permission to obtain and utilize specific information or data from its users. User-specific data or information is then collected, stored, and managed in a "big data" in "Cloud" network. The "Cloud" network is a new metaphorical term that describes a digital data storage system in a non-physical space that can process collection, arrangement, storage, and processing of data resulting from engineering computer technology. In simple terms, “Cloud” is explained as a system for storing and processing or distributing data, applications, services for all internet users that don’t require physical data storage instruments (Sudibyo (a), 2021). Digital device user data is collected and obtained from all digital platforms and applications that are connected to internet network.

Although in general, all services for digital devices and applications are provided free of charge to users, this doesn’t mean that there are no consequences. There are no digital services that are completely free but are always bartered by submitting personal data for free as well. Philips N. Howard stated that in the IoT era, advances in digital technology raise serious problems related to privacy security, social engineering, and public behavior manipulation. The flow of internet users' personal data collected by digital companies through digital devices and services has provided space for monitoring and controlling people's behavior (Sudibyo (a), 2021). In line with that, Foucault emphasized that technology present since industrial era has become a means to control people's behavior. Technological capabilities in supervising community without being watched by public (to see without being seen) and monitoring movements of community without the opposite has become a new form of power in modern era (Sudibyo (a), 2021). This vulnerability has an impact in the form of potential misuse of personal data for purposes that are detrimental to personal data owners. In the last decade, cases of illegal personal data mining through cybercrime to leakage of personal data (intentional or unintentional) have become a widespread problem in public sphere. In particular, cases of personal data leakage by digital companies have raised a number of concerns. Several digital companies have failed to protect their users' personal data, as illustrated in Table 1 below: (Lesmana et.al., 2022; Annur, 2021; Mediana, 2023)

Table 1: Cases of Personal Data Leakage in Indonesia

Year	Digital Platform	Amount Data Leaked
2019	Alibaba	1.1 billion accounts
2020	Tokopedia	91 million user data 7 million seller records
2020	Bhineka.com	1.2 million user data allegedly leaked and traded by a group of Shiny Hunters hackers on the dark web for USD 12,000
2020	Bukalapak	12,957,573 user data
2020	Kreditplus	890,000 customer data allegedly leaked and traded on Raid Forum
2020	*RedDoorz*	5.8 million user data is traded
2020	*Facebook*	130,000 user data
2022	Bank of Indonesia	Hack by Conti Ransomware Group
2020	Sina Weibo	538 million accounts
2021	*LinkedIn*	700 million accounts

The efforts to compete to obtain and control personal data aren’t only carried out in civil and private spheres, but also occur in state realm. Competition between countries has moved away from traditional patterns involving weapons of mass destruction or means of physical warfare towards competition using data to influence direction of state policy. For example, competition for data control related to using TikTok (owned by a company from China) which is growing from 65 million accounts (2017) to 1 billion accounts (2021). This sparked concern from United States government which pushed for a ban on using TikTok for security reasons and hacking of

personal data. Even United States is pushing for TikTok to leave its parent company, ByteDance or release all TikTok shares owned by Chinese citizens to entrepreneurs from other nations. This is due to United States' concern over geopolitical competition, especially after Cyberspace Administration of China (CAC) issued a policy ordering submission of digital technology algorithms for all Chinese companies to prevent anti-government content, and content that is contrary to Chinese socialism values. This policy sparked concerns in a number of countries that China would do same to TikTok user data in other countries. A number of countries have banned applications or social media from China, including India, United States, United Kingdom and New Zealand (Anwar, 2023).

The phenomena and developments of competition, hacking, and personal data theft show that is the tip of iceberg which has become a national to international issue. Cases of leaking personal data of users of digital technology that have been revealed are only a small part of possible reality. This happens because digital systems are very complex and limited, so it isn't easy to find out whether or not there is a hack or leakage of personal data for users of digital devices and services. To respond to these phenomena, continuous efforts to update personal data protection laws are being made by various countries. The principle of protecting personal data is the recognition of individual privacy and personal safety as part of human rights. In Indonesia, protection of citizens' personal data is one of constitutional obligations and responsibilities of the state which is explicitly contained in Paragraph IV of the Preamble of 1945 Constitution of Republic Indonesia (1945 Constitution of Indonesia), which emphasizes that state protects the entire Indonesian nation. Indonesia nation's recognition and guarantee of personal data protection urgency as part of human rights is clearly contained in Art. 28G p. (1) of 1945 Constitution, which states that everyone has right to personal protection and right to feel safety and protection from threat of fear to do or not do something that is a human right. Therefore, personal data must be protected, respected, maintained, and mustn't be ignored, reduced, or confiscated by anyone (Considerations of Human Rights Act No. 39/1999). In Indonesia, as a consequence of the state being based on law and constitution, protection of personal data should be actualized by laws and regulations. Since the Indonesia Independence (77 years ago), Indonesian government has only had a special law regulating personal data protection with the issuance of Law Number 27 of 2022 concerning Personal Data Protection (PDP Act). PDP Act is legal basis for governance and implementation of personal data protection in Indonesia. By paying attention to phenomenon of failure to protect people's personal data, developments in formation and ratification of PDP Act, to the emergence of various forms of digital crimes against personal data, it's necessary to carry out comprehensive research on PDP Act in order to respond to phenomena and legal needs of society and technological developments that very dynamic.

The latest research has an urgency to find out the development, scope, and potential legal loopholes that can be misused, misinterpreted or misused so as to cause harm to the public in efforts to protect personal data. Apart from that, it is also necessary to explore the importance of existence of the PDP Act as a special legal instrument for society protection in this digital era. Previous research has taken a lot of pictures and explained the urgency of protecting personal data from various perspectives. In general, previous research can be grouped into 5 (five) aspects, namely: ***First,*** research conducted by Yunarti (a) (2019), and Mirna, et al. (2023) which outlines various laws and regulations and basic principles that contain arrangements regarding protecting personal data in Indonesia prior to enactment of PDP Act. The research also contains foundations and factors that drive urgency of establishing PDP Act. ***Second,*** research conducted by Ramadhan & Wijaya (2022) and Tsamara (2021) which explains conception of a personal data protection commission, and a comparison of personal data protection in in other countries and international legal instruments against Indonesia before PDP Act.

Third, research by Afiudin, et al. (2022) and Setiawan, et al. (2020) which examines personal data protection arrangements prior to enactment of PDP Act on certain aspects/fields such as personal data protection related to online loans, e-commerce, and marketplace, as well as other electronic and digital devices. ***Fourth,*** research by Mangesti, et al. (2021) and Marune & Hartanto (2021) which examines personal data protection from a legal ethical perspective, and studies increasing public participation in strengthening personal data protection in general. ***Fifth,*** research by Manurung & Thalib (2022) and Kristanto (2023), who conducted a juridical review and outlined provisions in PDP Act in general and implementation of PDP Act related to legal phenomena in

certain aspects/fields. Both of these studies are descriptive in nature to provide an overview of PDP Act but haven't conducted a critical review of systematic norms.

By taking into account various previous research analyzes and developments, this research uses a different perspective because the research focus is directed at examining development of concept and regulation of PDP Act (including conducting a critical study of norms) and exploring importance of PDP Act to protect Indonesian digital society. This research was conducted to provide a more proportional description and critical analysis of PDP Act in order to complement and enrich literature studies that haven't been carried out much research after enactment of PDP Act. Based on background, main issues in this research are: (1) how is the development and regulation of personal data protection in Indonesia; and (2) what is the importance of PDP Act existence for digital society in Indonesia?

2. Method

This research focuses on examining the development of legal politics and regulation of personal data protection in various laws and regulations that apply systematically as an integrated legal system. It also analyzes and explores the importance of the PDP Act in responding to legal phenomena and developments in society related to personal data protection. This research attempts to provide a description and critical analysis of the importance of PDP Act in a comprehensive systematic description. The data used are in form of: (1) primary data obtained from observations (mass media and social media) and interviews with cyber law and telematics experts, namely: (a) Luluk Awaludin (Lecturer and Researcher at Faculty of Law, University of Bhayangkara Bekasi); (b) Tomy Prihananto (Analyst and Lecturer at Indonesia National Cyber and Code Agency); and (c) Dr. Andi Widiatno (Lecturer at Faculty of Law, Trisakti University); and (2) secondary data obtained from 1945 Constitution of Indonesia, PDP Act, and laws and regulations related to personal data protection, books, journals, and other supporting literature. The research data is processed based on validity and reliability of data to be studied and tested qualitatively using content analysis techniques. To deepen analysis, several perspectives and interpretations of laws are used.

3. Results & Discussion

3.1. Personal Data Protection: Development of Concept, Law, and Legislation in Indonesia

In digital society era, the benefits and economic value of user data for digital devices and services are very high, which has encouraged the behavior of mining personal data for certain purposes. In reality, not all parties are able to process and manage personal data of digital device users according to generate competitive advantage. On this basis, the collection and processing of personal data is very vulnerable to causing interference with a person's privacy. Privacy interventions occur because personal data can easily be arbitrarily transferred, and cause harm to society. In addition, so far, the public doesn't know how the management of their personal data works by digital.

With potentially violations of privacy, in a welfare state perspective, it's necessary to have an active role of state to oversee various activities of processing personal data and provide legal protection for potential misuse of personal data. In Indonesian context, the philosophical foundation of personal data protection is reflected in second precept of the Pancasila which states "just and civilized humanity". This philosophical basis emphasizes that personal data protection is necessary to create justice and form a human civilization that respects other people's personal data. Meanwhile, responsibilities and obligations of state in providing protection for security of personal data are stated in Paragraph IV of the Preamble 1945 Constitution of Indonesia, "Indonesian state government was formed to protect the entire Indonesian nation and all of Indonesia's bloodshed".

Discussions about personal data protection in Indonesia have only begun to be intense in last decade, although the problem of personal data protection in general isn't a new issue. The issue of protecting personal data globally developed in early 2003 in line with emergence of cybercrimes such as pornography, money laundering, hacking, malware (virus), carding crimes, and others. Technological advances have led to emergence of

technology-based crime and made demarcation between private and public space very thin. As a result, personal data becomes vulnerable to being stolen, shared, and misused for purposes that can harm society (Lesmana et.al., 2022). Before the phenomenon of cybercrime and the issue of protecting personal data surfaced, the idea of guaranteeing the right to privacy had been put forward by Samuel D. Warren and Louis D. Brandeis in 1890 as a development of the right to life. Warren and Braindes stated "Privacy is the right to enjoy life and right to be left alone and this development of law was inevitable and demanded legal recognition." There are 5 (five) arguments underlying importance of protecting privacy rights, namely: (Kusnadi & Wijaya, 2021)

1. As an individual, one needs time to be alone.
2. As a social being, a person needs to cover part of his private life to maintain his position at a certain level.
3. In domestic (family) relations, a person fosters marriage and family so that other people don't need to know about these personal relationships.
4. In terms of concept, privacy is a right that stands alone and doesn't depend on other people so that this right will disappear with publication to the public.
5. Violation of a person's right to privacy creates an impact that allows him to suffer losses due to disruption to a person's private life.

Starting from this idea, protection of right to privacy includes the right to feel comfortable in social interactions, and right to confidentiality of data or personal information. In its development, the scope of right to privacy has been expanded to include 4 (four) basic principles, namely: (1) right to privacy for information (collection and processing of personal information); (2) right to privacy for body (physical protection); (3) right to privacy for communication (security and confidentiality of any forms of communication); and (4) right to privacy for territory (Rianarizkiwati, 2022).

Today, the increasing need for privacy rights protection, especially for personal data, is caused by 3 (three) main factors, namely: (1) further development of human rights; (2) technological advances that give rise to cybercrimes, and result in vulnerabilities to personal data security; and (3) global competition in controlling data causes illegal data mining and misuse of public personal data. These conditions are dominant factors that encourage countries to establish regulations that specifically provide personal data protection. Several international documents have initiated and become guidelines for formation of personal data protection regulations, in various countries, both regionally and internationally, including: (Djafar & Santoso, 2019)

1) The OECD'S Privacy Guidelines 1980 and 2013 (revision).
2) European Union General Data Protection Regulation (EU GDPR).
3) UN Guidelines for the Regulation of Computerized Personal Data Files 1995.
4) Asia Pacific Economic Cooperation Privacy Framework 2004.
5) ASEAN Framework on Personal Data Protection.

Meanwhile, until now (2022), 132 of 193 countries has have laws that specifically regulate personal data protection. In particular, countries that are based on democracy place personal data protection as a human right and constitutional right of citizens, such as Portugal, Armenia, Timor Leste, Philippines, Colombia and Argentina, including Indonesia (Mangku, 2021). The following are development of formation of personal data protection regulations in several countries:

Table 2: Personal Data Protection Settings by Countries (Niffari, 2020; Kusnadi & Wijaya, 2021)

Country	Year	Name of Regulation
Europe Union	1984	*Data Protection Act*
	1998	*Data Protection Act 1998*
	2000	*Charter of Fundamental Rights of the European Union*
	2016	*General Data Protection Regulation*
United Stated	1974	*United State Data Privacy Act 1974*
	1988	*Computer Matching and Protection Act of 1988*
Hongkong	1995	*Personal Data Privacy Ordinance of 1995*
Japan	2003	*Personal Information Protection Act No. 57*

Russia	2006	*Federal Law on Personal Data*
South Korea	2011	*Personal Information Protection Act*
Malaysia	2010	*Personal Data Protection Act 2010*
Singapore	2012	*The Personal Data Protection Act No. 26 of 2012*
Philippines	2012	*Data Privacy Act 2012*
Laos	2017	*Law on Electronic Data Protection 2017*
Australia	2018	*Notifiable Data Branches Scheme*
China	2021	*Personal Information Protection Law*
Thailand	2019	*Personal Data Protection Act 2019*
India	2022	*Digital Personal Data Protection Bill 2022*
Indonesia	2022	*Law on Personal Data Protection No.27 of 2022*

As data shown in Table 2 above, Indonesia has just regulated personal data protection in a legal instrument that is specific through PDP Act in 2022. Previously, the arrangements of personal data protection were spread out in various laws and regulations. Several regulations that contain norms regarding personal data protection, prior to the enactment of PDP Act are described in Table 3 as follows:

Table 3: Personal Data Protection Arrangements Prior to PDP Act

Regulation	Chapter	Main Provision	Lack
Banking Act No. 10/1998 and the Amandement	Art. 40 p. (1)	Banks have an obligation to keep information about depositors and their deposits confidential	Doesn't include a description of the type of "information about depositors" which must be kept confidential. In addition, these obligations are sectoral banking affairs
Hospitals Act No 44/2009	Art. 32 letter I, 38, and 44 p. (1)	Patient own right on protection medical data privacy and hospital must save and reject disclose confidential of medical	Explanation of "medical data" or "confidential data/records". only regulated in Regulation of the Minister of Health No. 24/2022 and No. 36/2012 but the criteria for "patient identity" which must be kept confidential aren't further elaborated.
Practice Medical Act No. 29/2004	Art. 47 p. (2), Art. 48 p. (1), and 51 letter c	Doctors are obliged to keep confidential rights related to patients (medical records and medical secrets)	
Health Workers Act No. 36/2014	Art. 58 letter c, 70 p. (4), and 73	Health workers are obliged to store and maintain the health secrets of service recipients	
Nursing Act No. 38/2014	Art. 38 letter e	Users of nursing services have the right to maintain the confidentiality of their health conditions	
Openness Public Information Act No. 14/2008	Art. 2 p. (4) and Art. 17 letter h	This provision guarantees that personal data regarding history, health, finances, intellectual evaluation results, and personal records are exempt from disclosure	There is no definitive definition of personal data, only providing the types of personal data that must be protected.
Administration Population Act No. 23/2006 and the Amandement No. 24/2014	Art. 1 p. (22), Art. 8 p. (1) letter e, Art. 79 p. (1), and Art. 85 p. (3).	The state is obliged to protect, store and maintain correctness and security of personal data and population documents	There are significant differences regarding personal data that must be protected (Art.84) and the regulations aren't comprehensive enough.
Electronic Information dan Transaction Act No. 11/2008 and the Amandement	Art. 16, Art. 26 p. (1), and Art. 32 p. (3).	Overall, this rule contains arrangements to ensure protection against misuse of electronic technology and information	Doesn't contain specific arrangements regarding personal data protection
Trade Act No. 7/2014 and Government	Art. 91 Trade Act, and Art. 2, 33, 58, and	Trading data and information is open, unless otherwise specified. The government regulations	The definition and scope of "personal data" aren't regulated

Regulation concerning Trading Through Electronic Systems	59 Government Regulation	regarding trading through electronic systems contain obligations for business actors to store personal data and set standards for protecting personal data	
Government Regulation No. 71/2019 concerning Implementation of Electronic Systems and Transactions and Regulation of Ministy of Communication dan Informatics No. 20/2016 concerning Personal Data Protection	Art. 1 p. (29) Government Regulation and Art. 1 p. (3) Minister Regulation	This regulation contains a definition of personal data. This rule also explains quite fully the protection of personal data, both in the process of obtaining and collecting, processing and analyzing, storing, and destroying it.	There are different definitions and terms of "personal data" and "individual data". In addition, sanctions are only administrative penalties.

The various laws and regulations that contain norms for obligation to protect personal data that were in effect before PDP Act have several obstacles that impact the implementation of personal data protection, namely:

1) The definition and scope of personal data don't have fixed and clear parameters, so types of personal data that require to be protected become vague and ambiguous.
2) The obligation to provide protection for personal or confidential data is sectoral and sporadic because only applies to certain aspects.
3) Weaknesses of sectoral and sporadic regulation of personal data protection, impact on law enforcement process that isn't optimal, partial, and not systematically integrated. The sanction differentiated in various forms (administrative, criminal and non-sanctioned sanctions) are relatively weak for law enforcement.

Some of weaknesses in sectoral regulations are one of reasons for the need regulations urgency that specifically and comprehensively for personal data protection. In general, the PDP Act contains substance of personal data protection norms which can be described in Table 4 below:

Table 4: Norm Systematics of PDP Act (Yuniarti (b), 2022)

Indicator	Chapter	Explanation
General Terms	Art. 1 and 2	Definition of Personal Data: - Data about natural persons. - Identified or can be identified separately or combined with other information directly or indirectly. - Through electronic or non-electronic systems.
Principle	Art. 3	- Principles of protection, legal certainty, public interest, expediency, prudence, balance, accountability and confidentiality.
Types of Personal Data	Art. 4	- Specific Personal Data: (a) Health data and information; (b) Biometric data; (c) Genetic data; (d) Crime records; (e) Child data; (f) Personal financial data; (g) Other data according to the provisions. - General Personal Data: (a) Full Name; (b) Gender; (c) Citizenship; (d) Religion; (e) Marital Status; (f) Other Personal Data to identify a person.
Personal Data Subject Rights	Art. 5-15	- Right to information; to complete, update and correct errors or inaccuracies; to gain access; to end processing, delete, or destroy; to withdraw consent; to submit objections to automatic decision-making; to delay or limit data processing; to sue and receive compensation; and to use and

		send personal data from and to personal data controllers.
Personal Data Controller	Art. 1 and 19	- Individuals. - Public bodies. - International organizations.
Scope of Personal Data Protection Processing	Art. 16 – 18	- Acquisition and collection. - Processing and analysis. - Storage. - Fixes and updates. - Appearance, announcement, transfer or disclosure. - Deletion or destruction.
Basis for Personal Data Processing	Art. 20 (2)	- Explicit valid consent. - Fulfilment of agreement obligations. - Fulfilment of legal obligations. - On the basis of public interest, public service, or exercise of authority. - Fulfilment of other legitimate interests.
Obligations of Personal Data Controllers and Processors	Art. 19-54	- General requirements. - Obligations of data controllers. - Responsibilities of data processors. - Official or officer of personal data protection.
Transfer of Personal Data	Art. 55-56	- Within and outside Indonesian Jurisdiction.
Sanctions Arrangement	Art. 57, 65, and 67-72	- Administrative sanction. - Criminal penalties.
PDP Agency	Art. 58-61	- Duties and Authorities
International Cooperation	Art. 62	- Governments of other countries. - International organizations
Public Participation	Art. 63	- Directly and indirectly. - Through education, training, advocacy, outreach, and/or supervision.
Dispute resolution	Art. 64	- Courts, arbitration, and other dispute resolution institutions
Prohibition of Use of Personal Data	Art. 65	- Prohibition to unlawfully collect, disclose, use, or falsify personal data that does not belong to them.
Transitional and Closing Provisions	Art. 74-76	- Adjustment period of 2 (two) years. - Other regulations that are not contradictory still apply.

From a normative perspective, provisions in PDP Act have several positive aspects for efforts to protect digital society in Indonesia, namely:

1) The PDP Act was formed and formulated quite comprehensively and sufficiently to complement deficiencies or weaknesses of previous regulations.
2) The PDP Act provides clarity regarding definition and scope of personal data, rights and principle of personal data protection, responsibilities of controllers and processors, law enforcement procedures and dispute settlement, PDP agency, and existence of officials or officers of personal data protection.
3) The PDP Act provides an alternative as a basis for processing personal data as stipulated in Article 20 paragraph (2) letters a-f which is a cumulative alternative. With this format, the law doesn't place an excessive burden on controllers and processors of personal data to use and process the data (Ramli, 2023).

Even the formation of PDP Act has a positive image for efforts to protect digital society in Indonesia, after carrying out a critical normative review of PDP Act using an a contrario paradigm, it can be found notes that need to be prevented or reviewed so that enactment of PDP Act doesn't have a negative impact, that is: (Djafar, 2022; Awaludin, 2023)

1) Placement of crime records and child data categorized as specific personal data that must be protected doesn't have a rational juridical basis because: (a) related to crime records it can be used by the public as considerations that will affect social acceptance or social reintegration); and (b) regarding child data isn't yet specific because for certain parts are generally used for administrative or procedural requirements.

2) The PDP Act emphasizes full responsibility for personal data protection to controllers and processors of personal data. These obligations and responsibilities have the potential to be neglected if the norms aren't immediately complemented by the existence of a PDP agency.
3) The PDP agency, as sole organ of personal data protection, doesn't have law enforcement authority to resolve disputes over personal data protection violations. In addition, the appointment of an institution that is given the authority to supervise personal data protection hasn't been confirmed so that the effectiveness of implementation of PDP Act can't be implemented. This will have an effect if: (a) the establishment of a new institution creates a burden on the state budget; or (b) attached to or assigned to an existing institution, it is necessary to readjust or restructure the organization (Luluk, 2023).
4) There is a potential for injustice/inequality in law enforcement between the public and private sectors. It is only possible for the public sector to be subject to administrative sanctions (Art. 57 p. (2)), while private sector, in addition to administrative sanctions, can also be subject to administrative fines of 2% of annual income (Art. 57 p. (3) and its explanation) and criminal threats (Art 57, 67-70). Andi Widiatno emphasized that the 2% fine also applies to public institutions because it will affect performance appraisal and budget management capabilities of government institutions/agencies.
5) Exceptions to the obligations of processors and controllers of personal data for purposes stipulated in Art. 50 have potential to create loopholes for irregularities to misuse personal data. The state can use this reason to obtain personal data from controllers and processors for non-legal or extra-legal purposes.
6) With regard to issue of sentencing, practice in Indonesia shows the settlement of cases prioritizes corporal punishment. While protecting personal data, data owners often experience material losses. In this case compensation and other actions (account recovery, localizing data leaks that may occur, and others) aren't an option because the conversion of value of loss (personal data leakage) doesn't yet have a reference.
7) Data transfer involving data managers abroad, even though it has been regulated, has practical/technical problems because it requires Mutual Legal Assistance (MLA) which complicates and makes handling data protection increasingly complex and time-consuming. The government also needs to know about countries that have the potential to have personal data of Indonesian citizens to open or move their data centers to Indonesia, which in practice isn't easy to do.
8) The setting for an adjustment (transition) period of 2 (two) years in Art. 74 is less rational transition time due to several reasons, namely: (1) complexity of regulations synchronization; (2) preparation of implementing regulations; (3) establishment of a PDP agency; (4) internal reform of personal data controllers and processors; and (5) socialization and advocacy for regulations. This is important because it will have consequences for the public and legal obligations stipulated by PDP Act haven't been fulfilled.

Based on that analysis, normatively there is still disgrace from PDP Act. This at least includes gaps for misuse and abuse of personal data, potential for neglect and neglect of legal obligations by processors and controllers of personal data, conflicts of interest and injustice in law enforcement, to norms that require further regulation. The dependence of the PDP Act on implementing regulations is still very large to prevent the occurrence of elements that bias implementation of the law Andi Widiatno explain that PDP Act still requires guidelines or regulations at a more technical, procedural, and implemented level. Example: regulations related to cooperation and interconnection mechanisms between countries, complaint mechanisms, presidential regulations regarding PDP agency. The detail and quality depth of implementing regulations will determine effectiveness of PDP Act in providing personal data protection for Indonesia digital society.

3.2. The Importance of the Personal Data Protection Act for Protection of the Digital Society in Indonesia

As described in previous section that PDP Act provides the main foundation for general comprehensive personal data protection nationally to protect the public from negative impacts of technological developments. The next question is "is it still important and relevant to protect personal data in digital society era?". This can't be separated from the fact that personal data is distributed freely and widely on various digital platforms, both by irresponsible parties, digital companies, the government, and even by the owner (personal data) himself. In this digital era, the state and society unconsciously exist and live in a cycle of global supervision and control. The consequence is that personal data is very easily exposed and accessed in cyberspace, whether uploaded

intentionally or misused (Anonymous (a), 2023). In general, misuse of personal data can be caused by mining and illegal cyber activities. It can be proven that the intensity of cyber-attacks which are always increasing and getting more massive has occurred even after enactment of PDP Act. Safenet data shows that in 2022 there were 302 digital security incidents (54% increase from 2021 of 193 incidents). (Anonymous (b), 2023). While the National Cyber and Code Agency (BSSN) noted that in the period January-July 2023, there were 204,686,669 detections of cyber-attacks which included 53.54% malware activity, 29.7% Trojan activity, and 6.84% leaked data or information (Dewi, 2023).

This condition is in accordance with Zuboff's estimation which illustrates that in digitalization era, digital society is directed at the gateway to a new order of life that negates privacy. Public personal data that is confidential and private is easily exposed and exposed by other parties (Sudibyo (a), 2021). By entering a global digital system network, society has become an object of personal data mining as well as an object of unconscious monitoring and control. The practice of mining personal data occurs latently, automatically and continuously to produce very detailed user profiles for the benefit of certain parties. This condition is called "Panopticon Society". Panopticon society is a term used to describe a society that lives in a world full of surveillance and control over personal data. In this era, discussions about personal data and privacy rights are less or no longer relevant (Sudibyo (b), 2023). In panopticon society era there is no guarantee that digital companies are able to provide protection for the personal data of users of digital platforms. These digital companies also utilize their users' personal data to predict and influence user behavior for the benefit of the digital business economy to practical political needs, such as formulating advertisements, product offers, being traded to monetizing personal data. This phenomenon, according to Schiller and Zuboff, has occurred as an exclusive violation because they have penetrated private spaces without permission. This is exacerbated by the absence of other parties who have power to intervene in behavior that violates propriety (Sudibyo (a), 2021).

In addition to what was stated by Schiller and Zuboff, accessibility to personal data which is very vulnerable in digital society era which can have a detrimental impact on society is also influenced by various factors, including: (Sugihartati, 2023; Attidhira & Permana, 2022)

1) The shrewdness of perpetrators of theft or hacking of personal data to take advantage of the victim's personal condition by mapping victim's social network and environment to carry out information espionage and manipulation.
2) The ability of privacy literacy and digital literacy is low which causes people to be easily deceived. Research by Hootsuite and We Are Social in 2021 estimates that no more than 25% of internet and social media users are digital media literate. Digital device users tend to be driven by a great desire for curiosity but low caution.
3) The low quality of Indonesian cyber facilities. Analysis of National Cyber Security Index (NCSI) in 2022 shows that Indonesia's cybersecurity ranks 83 out of 160 countries globally and sixth among ASEAN member countries (38.96/100), far behind Malaysia (79.22), Singapore (71.43), and Thailand (64.9) (Yuniarto, 2022). The low level of cyber security is related to indicators of the rule of law, the presence of government agencies, cyber cooperation, and public evidence.
4) Inadequate law enforcement capacity against cyber threats and personal data protection. BSSN stated that compliance and response of ministries and government agencies in following up cybersecurity infection efforts was still low. In 2021, out of 1,261 cyber threat notifications sent to ministries and government agencies (an increase in 2022 by 1,433 notifications), only 6% or 72 notifications were responded to. The Executive Director of the Institute for Community Studies and Advocacy (ELSAM), Wahyudi Djafar stated that cyber-attacks that occurred in ministries and institutions had an impact on leakage of citizens' personal data (Anonymous (c), 2023.

The various fundamental loopholes that cause various violations of personal data of digital device users, even though digital society era is marked by the loss of demarcation between public and private spheres, it will eventually cause losses, both physical, material and psychological. In this case, existence of PDP Act has an important meaning in providing protection for digital community in Indonesia to prevent losses arising from the use of digital device. The significance of PDP Act can be traced in 3 (three) aspects which, according to Soerjono Soekanto, also influenced the enactment of PDP Act), namely: (Sitabuana, 2017)

1) The philosophical aspect, that the PDP Act seeks to provide protection for Indonesian nation from the dangers of hacking, theft, misuse and dissemination of personal data against law. The Second and Third Precepts of Pancasila provide guidelines and encourage the need for a legal basis to provide security guarantees for personal data of Indonesian citizens and to foster public awareness of recognition and respect for other personal data owner (being a civilized human being).
2) The juridical aspect, that PDP Act was born as a form of state responsibility to provide protection for Indonesian nation as contained in Paragraph IV of Preamble and Art. 28G p. (1) of 1945 Constitution of Indonesia. The nature and construction of 1945 Constitution norm are adaptive and futuristic, it has been proven capable of being realized and manifested in PDP Act as a means of protecting the threats to constitutional rights of personal data owner/subject. Tomy Prihananto (2023) added, the legal formality of PDP Act has answered the political will of Indonesian nation for an urgent and non-delayed need for national interests.
3) The sociological aspect, that PDP Act was born on basis of a legal need in society to create order and progress in a digital society. Therefore, the importance of PDP Act in a sociological aspect includes 3 (three) things, namely: (a) guaranteeing protection, security and order in a digital society in relation to processing of personal data; (b) fostering and increasing public's sense of trust in providing personal data without misusing or violating their personal rights; and (c) contribute to smooth running and growth of the digital economy.

The importance of PDP Act in a more practical and implementable sense as stated by the Director General of Informatics Applications of the Ministry of Communication and Informatics, Semuel Abrijani Pangarepan, includes: (Rizki, 2022)

1) Means of providing protection for the fundamental rights of society.
2) A comprehensive legal umbrella to encourage reform of personal data processing practices.
3) Responding to the needs and demands of public law, especially consumers.
4) Promote responsible innovation and respect for human rights from a personal data protection perspective.
5) Development of new ecosystems and talents in protecting personal data and strengthening Indonesia's leadership in governance and global relations.
6) Growing public habits and awareness in personal data protection.

Meanwhile, Andi Widiatno (2023) gave an explanation of importance of PDP Act from a juridical aspect that the presence of PDP Act caught up with Indonesian people from other countries that had previously owned and provided personal data protection, complemented and perfected the gaps in legal construction of existing laws and regulations previously applied, and law enforcement more optimal and complete, especially implementation of sanctions (administrative, civil, and criminal penalties).

The meaning of PDP Act existence for digital community in Indonesia as previously explained will only provide benefits if it can be implemented and applied properly and thoroughly to protect the interests of the community. For this reason, it is important to identify the factors that influence the operation of the PDP Act based on Soerjono Soekanto's opinion (Soekanto, 2007; Satwiko, 2021), namely: ***First,*** legal factors (legal substance) through the integration of personal data protection laws in various laws and regulations. This is necessary to ensure that there is no legal vacuum and more complex arrangements, both in the material and procedural context. ***Second,*** law enforcement factors (legal structure). In this case the government must guarantee the implementation of protection of personal data by establishing and implementing policies, promotion and education, advocacy, and supervision, also set up supervisory and regulatory units on a small scale. Law enforcement officials need to follow and understand the flow of changing times and technology development, so they need to receive special training and education to increase their capacity and competence in dealing with and preventing cases of violations of personal data protection. ***Third,*** the factor of facilities and amenities. To increase effectiveness of personal data protection, the availability of qualified technological facilities and devices is needed. So far, relatively complete and modern cyber facilities have tended to be concentrated in big and strategic cities. In addition, in the event of a breach of personal data protection, channels and facilities that are affordable and easy to access for victims must be provided and communicated to the public.

Fourth, the society factor. The problem that often occurs is the low public awareness of the importance of protecting personal data. Therefore, socialization and education to improve digital literacy must be carried out massively. Collaborative governance needs to be encouraged to accelerate personal data protection goals so that society can benefit from digital developments and digitization processes. The state in this context is responsible for providing equal and equitable education or knowledge for every citizen. ***Fifth,*** cultural factors (legal culture). This can be done by providing legal outreach and training to the community, especially those who are left behind by technological advances. This process can be carried out in 2 (two) forms, namely: (1) formal socialization including socialization formed by the government and the community through institutions that have a special task in disseminating values, norms and the roles of community in ensuring personal data protection; and (2) informal socialization, including socialization to instill mutual respect for personal data and right to privacy among community members (Marune, 2021). To fight hegemony and potential theft of personal data, it is necessary to develop what is called deleuze as a control society, namely a society that is no longer part of being regulated and controlled by digital systems and technology but becomes a society that is not trapped in the manipulation of desires and pleasures offered by digital technology.

Andi Widiatno (2023) provided guidance regarding the steps to maximize the potential for personal data protection, especially after the PDP Act, namely: (1) an educational aspect approach that is provided to all stakeholders and interested parties through an education and outreach process of increasing digital literacy and cybersecurity literacy. This stage is the basis for the public to have awareness in protecting their personal data; (2) a system approach charged to personal data processors and controllers (electronic system operators) to provide reliable software and hardware; and (3) a legal approach as the final step in personal data protection in the event of violations that are detrimental to the interests of personal data protection (generally the losses incurred are material). Therefore, the transition or transition period becomes a momentum for all stakeholders to accelerate and optimize efforts to make the law effective. This is done solely to provide and increase public confidence in the capacity of the state to guarantee and ensure the protection of the personal data of all its citizens as mandated by the 1945 Constitution of Indonesia.

4. Conclusion

Various cases of leakage, hacking, abuse leading to cybercrimes have caused a lot of harm to Indonesian nation. This phenomenon is related to the development of industrial era and digital society, which underlined the rise of data mining and ownership as a commercial commodity. The idea of personal data protection developed from embryo of right to privacy which was then formulated and standardized in various legal documents, both national, regional and international. Today, various countries have domestic regulations to provide protection for personal data of their citizens. In Indonesia, the obligation to provide protection (personal data) is a constitutional mandate based on 1945 Constitution of Indonesia and Indonesian government has issued regulations of personal data protection. Before PDP Act enactment, personal data protection arrangements are scattered in various laws and regulations that are sporadic and sectoral that impact to law enforcement aren't optimal. With enactment of PDP Act, it will complement other regulations. The PDP Act normatively has a positive impact because it provides clarity regarding the scope of personal data generally and systematically. However, several issues that have the potential to add the complexity of protecting personal data include issues of independence and authority of PDP agency, overcriminalization and discrimination in the application of the law, potentially abuse of law, irrational transition times, and dependence on implementing regulations.

Apart from dynamics of normative regulation, the formation of PDP Act gives important meaning to the protection of digital society in Indonesia, namely: (1) fulfilling constitutional responsibility and obligation to provide protection for all citizens as mandated by 1945 Constitution of Indonesia; (2) responding to legal needs, especially in digital era to guarantee order and security for community; (3) foster public trust in the state to provide reliable protection of people's personal data; (4) encouraging digital economic growth in Indonesia; (5) catching up with laws regarding the protection of personal data in global relations; and (6) fostering public awareness and culture of recognition and respect for personal data. Therefore, in order for the goals and implementation of personal data protection to be correlated and coherent, need to be done, namely:

1. Synchronize laws and regulations and accelerate the process of forming of implementing regulations for the

PDP Act.
2. Conduct advocacy, assistance, and outreach, both formal and informal to all stakeholders, especially the general public.
3. Increase the capacity and qualifications of officials, processors, controllers and law enforcement officials to ensure reliable and responsible personal data protection through a system (technology) approach.

Acknowledgments

The Research Team would like to thank Mr. Tomy Prihananto, Mr. Luluk Awaludin, and Dr. Andi Widiatno, as an expert in technology and cyber law, and specially to Research and Community Service Institute, Tarumanagara University (LPPM UNTAR) who supported and funded this research.

References

Afiudin, U.T.A., Novera, A., Adisti, N.A., & Puspasari, A. (2022). "Pelindungan Hukum Terhadap Korban Penyalahgunaan Data Pribadi Dalam Pinjaman *Online*" [Legal Protection for Victims of Misuse of Personal Data in Online Loans]. *Repertorium: Jurnal Ilmiah Hukum Kenotariatan, 11* (1), 104-113. Doi: 10.28946/rpt.v11i1.1822.

Annur, C.M. (October 24, 2020). "Inilah 10 Kasus Kebocoran Data Terbesar di Dunia" [These are the 10 Biggest Data Leak Cases in the World]. Accessed April 27, 2023. https://databoks.katadata.co.id/datapublish/2021/10/24/inilah-10-kasus-kebocoran-data-terbesar-di-dunia.

Anonymous (a). (February 23, 2023). "Data Pribadi Semakin Tak Aman" [Personal Data is Increasingly Unsecured]. *Kompas.*

Anonymous (b). (February 25, 2023). "Tahun Politik Rawan Serangan Digital" [Political Year Prone to Digital Attacks]. *Kompas.*

Anonymous (c). (February 21, 2023). "Satgas BSSN Hadapi Tren Ancaman Siber" [National Cyber and Code Agency Task Force Faces Cyber Threat Trends]. *Kompas.*

Anwar, L.A. (March 23, 2023). "AS Berencana Larang TikTok Sepenuhnya" [US Plans to Ban TikTok Completely]. *Kompas.* Accessed May 1, 2023. https://www.kompas.id/baca/internasional/2023/03/23/as-berencana-larang-tiktok-sepenuhnya.

Attidhira, S.W., & Permana, Y.S. (2022). "*Review of Personal Data Protection Legal Regulations in Indonesia*". *Awang Long Law Review, 5*(1), 280-284. https://doi.org/10.56301/awl.v5i1.562.

Awaluddin, L. (2023). The interview was conducted online via a zoom meeting on Friday, August 18, 2023.

Dewi, I. R. (July 2, 2023). "Bohong Internet RI Aman, BSSN Beberkan Buktinya" [Lie that Indonesian Internet is Safe, National Cyber and Code Agency Reveals Proof]. *CNBC Indonesia.* Accessed July 14, 2023. https://www.cnbcindonesia.com/tech/20230712162824-37-453708/bohong-internet-ri-aman-bssn-beberkan-buktinya.

Djafar, W. (September 20, 2022). "Pengesahan RUU Pelindungan Data Pribadi: Terancam Menjadi Macan Kertas" [Ratification of the Personal Data Protection Act: Threatened to Become a 'Paper Tiger']. *Lembaga Studi dan Advokasi Masyarakat.* Accessed May 2, 2023. https://elsam.or.id/siaran - pers/pengesahan-ruu-pelindungan-data-pribadi-teran cam-menjadi-macan-kertas.

Djafar, W., & Santoso, M.J. (2019). *Pelindungan Data Pribadi: Konsep, Instrumen, dan Prinsipnya* [Personal Data Protection: Concepts, Instruments and Principles]. Jakarta: ELSAM.

Kristanto, A.P. (2023). "Pelindungan Terhadap Data Pribadi Dalam Aplikasi Digital Sebagai Bentuk Pelindungan Hak Asasi Manusia" [Protection of Personal Data in Digital Applications as a Form of Human Rights Protection]. *Unes Law Review, 5*(3), 955. https://doi.org/10.31933/unesrev.v5i3.

Kusnadi, S.A., & Wijaya, A.U. (2021). "Pelindungan Hukum Data Pribadi Sebagai Hak Privasi" [Legal Protection of Personal Data as a Privacy Right]. *Jurnal Al-Wasath. 2*(1), 20. https://doi.org/10.47776/ alwasath.v2i1.127.

Lesmana, T., Elis, E., & Hamimah, S. (2022). "Urgensi Undang-Undang Pelindungan Data Pribadi Dalam Menjamin Keamanan Data Pribadi Sebagai Pemenuhan Hak Atas Privasi Masyarakat Indonesia" [The Urgency of the Personal Data Protection Law in Guaranteeing the Security of Personal Data as a Fulfillment of the Indonesian People's Right to Privacy]. *Jurnal Rechten: Riset Hukum dan Hak Asasi Manusia, 3*(2), 1-7. https://doi.org/10.52005/ rechten.v3i2.78.

Mangesti, Y.A., Suhartono, S., & Mahyani, A. (2021). "Ethico-Legal Aspects of Personal Data Protection in Indonesia". *International Journal of Educational Research & Social Science, 2*(5), 1030-1037. https://doi.org/ 10.51601/ijersc.v2i5.160.

Mangku, D.G.S., Yuliartini, N.P.R., Suastika, I.N., & Wirawan, I.G.M.A.S. (2021). "The Personal Data Protection of Internet Users in Indonesia". *Journal of Southwest Jiaotong University, 5*(1), 204. 10.35741/issn.0258-2724.56.1.23.

Manurung, E.A.P., & Thalib, E.F. (2022). "Tinjauan Yuridis Pelindungan Data Pribadi Berdasarkan UU Nomor 27 Tahun 2022" [Juridical Review of Personal Data Protection Based on Law Number 27 of 2022]. *Jurnal Hukum Saraswati, 4* (2), 143. https://doi.org/10.36733 /jhshs.v4i2.

Marune, A.E.M.S., & Hartanto, B. (2021). "Strengthening Personal Data Protection, Cyber Security, and Improving Public Awareness in Indonesia, Progressive Legal Perspective". *International Journal of Business, Economi, and Social Development, 2* (4), 143-152. https://doi.org/10.46336/ijbesd.v2i4.170.

Mediana. (February 7, 2023). "Masa Transisi UU PDP, Kepastian Hukum Tetap Diperlukan" [Transition Period to the PDP Law, Legal Certainty is Still Required]. *Kompas*. Accessed May 1, 2023. https://www.kompas.id/baca/ekonomi/2023/02/07/jaminan-kepastian-hukum-tetap-diperlukan-selama-masa-transisi-uu-pdp.

Mirna, M., Judhariksawan, & Maskum. (2023). "Analisis Pengaturan Keamanan Data Pribadi di Indonesia" [Analysis of Personal Data Security Regulations in Indonesia]. *Jurnal Living Law, 15* (1), 16-30. https://ojs.unida.ac.id/livinglaw/article/view/4726.

Niffari, H. (2020). "Pelindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Pelindungan Data Pribadi (Suatu Tinjauan Komparatif Peraturan Perundang-undangan Negara Lain)" [Protection of Personal Data as Part of the Human Right to Protect Personal Data (A Comparative Review of Legislation in Other Countries)]. *Selisik, 6* (1), 10-11. https://doi.org/10.35814/ selisik.v6i1.1699.

Prihananto, T. (2023). Written statement submitted on Sunday, August 20, 2023.

Ramadhan, K.R., & Wijaya, C. (2022). "The Challenges of Personal Data Protection Policy in Indonesia: Lesson Learned from the European Union, Singapore, and Malaysia". *Techicum: Social Sciences Journal,* 36, 18-28. https://doi.org/10.47577/tssj.v36i1.

Ramli, A.M. (March 23, 2023). "Pemrosesan Data Pribadi Menurut UU PDP dan Status Eksisting" [Processing of Personal Data According to the PDP Act and Existing Status]. *Kompas*. Accessed May 1, 2023. https://nasional.kompas.com/read/2023/03/23/11333391/pemrosesan-data-pribadi-menurut-uu-pdp-dan-status-eksisting.

Rianarizkiwati, N. (2022). "Ius Constituendum Hak Atas Pelindungan Data Pribadi: Suatu Perspektif Hak Asasi Manusia" [Ius Constituendum the Right to Protect Personal Data: A Human Rights Perspective]. *Jurnal Hukum Sasana, 8* (2), 328-329. https://doi.org/10.31599/sasana.v8i2.1604.

Rizki, M.J. (November 1, 2022). "Kominfo Paparkan Beragam Manfaat Penting Kehadiran UU PDP" [The Ministry of Communication and Information Explains Various Important Benefits of the PDP Act]. *Hukumonline*. Accessed August 21, 2023. https://www.hukumonline.com/berita/a/kominfo-paparkan-beragam-manfaat-penting-kehadiran-uu-pdp-lt6360ac5d1f1e3/.

Satwiko, B.S. (2021). "Privacy and Data Protection: Indonesia Legal Framework". *Corporate and Trade Law Review, 1* (2), 106-108. https://journal.prasetiyamulya.ac.id/.

Setiawan, H. et al. (2020). "Pelindungan Hukum Terhadap Data Pribadi Konsumen Dalam Transaksi E-Commerce" [Legal Protection of Consumer Personal Data in E-Commerce Transactions]. *Merdeka Law Journal, 1* (2), 102-111. https://doi.org/10.26905/mlj.v1i2.5496.

Sitabuana, T.H. (2017). *Berhukum di Indonesia [Legal in Indonesia]*. Jakarta: Konpress.

Soekanto, S. (2007). *Faktor-faktor yang Mempengaruhi Penegakan Hukum [Factors Affecting Law Enforcement]*. 7th Printed. Jakarta: Raja Grafindo Persada.

Sudibyo, A (a). (2021). *Jagat Digital: Pembebasan dan Penguasaan [The Digital Universe: Liberation and Mastery]*. 2nd Printed. Jakarta: Kepustakaan Populer Gramedia.

Sudibyo, A (b). (February 30, 2023). "Manusia Digital dan Ke(tidak)bebasan" [Digital Man and (un)Freedom]. *Kompas*.

Sugihartati, R. (January 30, 2023). "Kejahatan Siber di Era Masyarakat Berisiko" [Cybercrime in the Era of a Risk Society]. *Media Indonesia.*

Tsamara, N. (2021). "Perbandingan Aturan Pelindungan Privasi Atas Data Pribadi Antara Indonesia dengan Beberapa Negara" (Comparison of Privacy Protection Rules for Personal Data Between Indonesia and Several Countries]. *Jurnal Suara Hukum, 3* (1), 53-85. https://doi.org/10.26740/jsh.v3n1.p53-84.

Widiatno, A. (2023). The interview was conducted online via a zoom meeting on Monday, August 21, 2023.

Yuniarti, S (a). (2019). "Pelindungan Hukum Data Pribadi" [Legal Protection of Personal Data]. *Jurnal Becoss, 1* (1), 147-154. https://doi.org/10.21512 /becossjournal.v1i1.6030.

Yuniarti, S (b). "Protection of Indonesia's Personal Data After the Ratification of the Draft Personal Data Protection Law". *Progressive in Law, 4* (2), 57-60. https://doi.org/10.36448/plr.v4i02.85.

Yuniarto, T. (September 30, 2022). "Kasus Bjorka dan Keamanan Data di Indonesia" [The Bjorka Case and Data Security in Indonesia]. *Kompas*. Accessed May 1, 2023. https://kompaspedia.kompas.id/baca/paparan-topik/kasus-bjorka-dan-keamanan-data-di-indonesia.