UNNES LAW JOURNAL

Challenges in Ensuring Personal Data Protection for Society in The Era of Society 5.0: Indonesia's Case Study

Tegar Islami Putra, Waspiah, Indriana Firdaus, Fitria Damayanti, Bintang Rafli Ananta

Cite this article as:
Putra, Tegar Islami, Waspiah, Indriana Firdaus, Fitria Damayanti, and Bintang Rafli Ananta. "Challenges in Ensuring Personal Data Protection for Society in The Era of Society 5.0 Indonesia's Case Study". *Unnes Law Journal* 11, no. 2 (2025): 223-254. https://doi.org/10.15294/ulj.v11i2.8928.

AIMS AND SCOPE

The Unnes Law Journal has taken a broad and visionary approach to legal scholarship in Indonesia since its beginnings in 2012. The Unnes Law Journal has committed to become a law journal that foster a knowledge of law in empowering justice in Indonesia and global context. The Unnes Law Journal has since established itself as a leading journal for theoretical, interdisciplinary, comparative, and other conceptually oriented inquiries into law and law reform in Indonesia and global context, as well as comparative legal issues in Southeast Asia. The Journal **regularly published articles related to Indonesian legal studies in various perspective of legal philosophy, law and economics, legal history, criminology, justice and crime, gender and feminist analysis of law, law and literature, political aspects in law, and law and culture in contemporary global context**. The Unnes Law Journal is currently one of the leading law journals in Indonesia. The Journal also received the reputable ranking for journal quality from the Ministry of Education, Research and Technology of Republic of Indonesia.

EDITORIAL TEAM

UNNES LAW JOURNAL

Challenges in Ensuring Personal Data Protection for Society in The Era of Society 5.0: Indonesia's Case Study

Tegar Islami Putra, Waspiah, Indriana Firdaus, Fitria Damayanti, Bintang Rafli Ananta

ABSTRACT. Personal data protection is crucial in realizing cybersecurity in the Industrial Revolution 5.0 era in Indonesia. The regulation of cybercrime and personal data protection is to provide protection to victims of cybercrime and provide legal sanctions to perpetrators. The implementation of this regulation is not an easy thing, there are various challenges faced, especially in order to face the Era of Society 5.0. This research utilizes normative legal research which examine all regulations (positive law, principles, and legal doctrines) that are applicable in Indonesia and will not overlook the comparison of regulations in other countries to correlate various legal behaviors resulting from the said regulations in an effort to find answers to the research questions. The results show that there are several challenges faced in ensuring personal data protection for society in the era of society 5.0 with a case study of Indonesia, including low public awareness, political patronage, and the need for competent officials hindering effective law enforcement. In addition, there are implementation challenges in the form of regulatory weaknesses that are not matched by implementing regulations and specialized agencies, low public awareness and understanding of the importance of personal data protection, lack of competence of human resources managing personal data, as well as sectoral ego and lack of moral responsibility of officials.

KEYWORDS. Challenges; Personal Data; Protection; Society; Indonesia.

Challenges in Ensuring Personal Data Protection for Society in The Era of Society in The Era of Society 5.0: Indonesia's Case Study

Tegar Islami Putra[1*], Waspiah[2*], Indriana Firdaus[3*], Fitria Damayanti[4*], Bintang Rafli Ananta[5*]

Introduction

The advancement of technology in the era of the Industrial Revolution 5.0 is progressing rapidly. Information and communication technology is becoming increasingly important in everyday life (Guntur, et.all, 2020: 12-15).[2] Society now lives alongside technology, and according to data released by the Central Statistics Agency (BPS) in 2021, the number of internet users in Indonesia reached approximately 196.7 million people, or about 72.3% of Indonesia's total population of 272.1 million (BPS, 2021: 104). Additionally, the number of social media users continues to rise, with around 170 million people using social media in Indonesia in 2021. Moreover, the use of other information technologies such as smartphones, laptops, and computers is also becoming more widespread in Indonesia. According to a survey conducted by the Ministry of Communication and Informatics in 2020, smartphone

* Universitas Negeri Semarang, Semarang, Indonesia. Corresponding email: tegarislami44@students.unnes.ac.id. The authors would like to express their gratitude to the Research and Community Services Institute of UNNES (LP2M) for funding this research through the Student Organization Research Funding Scheme. Our sincere thanks to the Faculty of Law, Universitas Negeri Semarang, for being the home institution of the authors. We also extend our appreciation to the Communication and Informatics Agency (Diskominfo) of Central Java for the opportunity to engage in discussions and gather empirical data.

Special thanks to Mrs. Waspiah, S.H., M.H., as the supervisor of UKM Lex Scientia, for her guidance. We are also deeply grateful to Mr. Laga Sugiarto, S.H., M.H., for the assistance and enlightenment provided to the authors in the development and refinement of this research.

[2] Guntur et al., Perkembangan Teknologi Informasi Di Indonesia Menghadapi Industri 5.0. (Surabaya: CV Jakad Media Publishing, 2020).

penetration in Indonesia reached approximately 62.4% of the total population, while laptop and computer users accounted for about 8.4% and 2.4% of the total population, respectively. These data indicate that the use of information technology in Indonesia is rapidly increasing and is spreading across all segments of society.[3]

In its development, information and communication technology is like a double-edged sword that brings significant positive and negative impacts, especially in the field of cybersecurity. Cybersecurity in Indonesia is considered weak, with numerous cases reported; there were 6,388 cases of cybercrime reported in Indonesia throughout 2019-2020. Cybercrime is a criminal act committed through or related to the use of information and communication technology (Nancy E. Marion & Jason Twede: 2020, 16).[4] Cybercrime can take various forms, such as hacking, identity theft, fraud, phishing attacks, spreading computer viruses, and other criminal activities involving digital technology (Bahtiar, 2020, 18). The emergence of changes in human life also creates new problems. One example is the problem of personal data security that often occurs for users of digital technology.[5] Cybersecurity issues are becoming increasingly serious and require serious attention from the government and society. Cybercrimes can cause significant material and non-material losses, including financial losses, loss of personal or business data, damage to reputation, and even threats to national security (Amrozi, et.all., 2021: 7).[6]

Recent cybercrime cases in Indonesia include a hacking attack on BPJS Kesehatan in 2021, which resulted in the personal data of BPJS Kesehatan participants being hacked and stolen by hackers. The stolen personal data included names, BPJS Kesehatan card numbers, phone numbers, email addresses, and home addresses of millions of BPJS Kesehatan participants (Saleh, 2021: 92). In November 2021, a data breach involving the e-HAC (Electronic Health Alert Card) application of the Indonesian Ministry of Health occurred (Djafar & Komarudin: 2014). It was reported that the

[3] BPS, "Statistik Telekomunikasi Indonesia 2021," Telecomunication Statistics in Indonesia 2021 (Jakarta, September 7, 2022).
[4] Nancy E. Marion and Jason Twede, *Cybercrime: An Encyclopedia of Digital Crime* (Santa Barbara, California: ABC-CLIO, 2020).
[5] Waspiah Waspiah et al., "Model Perlindungan Hukum Data Pribadi Di Era Digital Guna Menjamin Hak Warga Negara Atas Perlindungan Data Pribadi," *Syntax Literate: Jurnal Ilmiah Indonesia* 8, no. 9 (2023): 5165–79.
[6] Yusuf Amrozi et al. "Tantangan Security Dan Kehandalan Sistem Dalam Aplikasi Bergerak," *Jurnal Pendidikan Teknologi Informasi (Jukanti)* 4, no. 2 (2021):

personal data of more than 1 million users of the application leaked online, including names, NIK numbers, email addresses, phone numbers, and health information such as medical history and COVID-19 test results (Solehudin & Ruhaeni, 2022: 983).[7] Additionally, in the same year, a shocking data breach involved the life insurance company BRI Life in Indonesia. Despite the frequent occurrence of cybercrime cases in Indonesia, the country still does not have laws regarding personal data protection. On the other hand, citizens still have rights to legal protection, as enshrined in Article 28G (1) of the 1945 Constitution of the Republic of Indonesia *(Pasal 28 G, Undang-Undang Dasar Negara Republik Indonesia tahun 1945*), and the state threatens criminal penalties for perpetrators of cybercrime under criminal law regulations to reflect legal certainty and the principle of legality. Legal regulations on cybercrime and personal data protection aim to provide protection for cybercrime victims and impose legal sanctions on perpetrators of these crimes. Personal data protection is crucial in realizing cybersecurity in the era of Industrial Revolution 5.0, especially in Indonesia, with the increasing use of information technology and the internet (Sagala, et.all., 2021: 98-120).[8]

Based on the review of previous research publications, various related studies conducted by different authors have been identified. These studies differ from the current research objectives of this author. In other words, the various analyses or studies related to legal protection of personal data conducted by previous researchers and authors have yielded different results, as it can be said that their research tends to have a more general scope of discussion. Below, the author will explain several studies by previous authors, thereby showing that this research is new and interesting for further investigation, such as: a) A study conducted by Timotius & Rasji titled "*Personal Data Protection as Fulfillment of Privacy Rights in the Digital Era*" in 2023. Their research explains that personal data protection is clearly regulated in Law No. 27 of 2022, ensuring legal certainty for the owners of personal data regarding their privacy rights. b) Another study was conducted by Ayumi, titled "*Legal Aspects of Personal Data Protection as Privacy Rights for Social Media Users*" in 2023. Ayumi explains that, so far, there is

[7] Herlan Solehudin and Neni Ruhaeni, "Perlindungan Hukum Atas Kebocoran Data Pribadi Ditinjau Dari Undang Undang Nomor 19 Tahun 2019 Tentang Informasi Dan Transaksi Elektronik Dan Implementasinya Terhadap Kebocoran Data Pengguna Electronic Healcth Alert Card," in *Bandung Conference Series: Law Studies* (Bandung: Unisba, 2022), 981–88.
[8] Mesias Sagala et al., *Hukum Dan Cybercrime* (Medan: Penerbit Kita Menulis, 2021).

no law protecting the personal data of Indonesian citizens, and many articles in the ITE Law still contain ambiguous terms. Therefore, the government needs to create clear regulations to protect personal data. c) Lastly, a study by Yuniarti titled "*Legal Protection of Personal Data in Indonesia*" in 2019. In this paper, Yuniarti reveals that with the advancement of technology and the increasing number of people using technology, privacy regarding citizens' data needs legal guarantees and protection from the government. However, currently, there is no explicit legal product regulating personal data protection. Therefore, the concept of data protection is highly relevant to individual privacy.[9]

From the summaries of the research above, it can be seen that the protection of personal data for Indonesian citizens is important for further research. This is done because the protection of personal data is one of the keys to successful law enforcement in Indonesia.

Within the framework of other's country law, international law, national law, and empirical studies, this research is directed towards the question: "*How is the Overview of Personal Data Protection for Indonesian Society in the Era of Society 5.0?*" In this section, the author will elaborate on the political efforts made by the government to ensure data security for society in the era of Society 5.0. Additionally, the author will compare the legal constructions and regulations currently implemented in Indonesia with those applied in international law and several developed countries to understand the measures they take to protect their citizens' personal data. Moreover, this question will lead to the second research question: "*What are the Possible Challenges in Ensuring Personal Data Protection for Society in the Era of Society 5.0 in Indonesia?*" In this section, the author will outline various issues that arise as data security risks in the era of Society 5.0. Furthermore, the author will explain the risks in this context that society may face as a result of political efforts and regulations in Indonesia.

[9] Tegar Islami Putra, Akbar Jihadul Islam, and Abdullah Mufti Abdul Rahman, "Integrating Islamic Laws into Indonesian Data Protection Laws: An Analysis of Regulatory Landscape and Ethical Considerations," *Contemporary Issues on Interfaith Law & Society* 4, no. 1 (2024): 89.

Method

This research utilizes normative legal research. As stated by Peter Mahmud Marzuki (2019: 35), normative legal research is a series of processes undertaken by researchers to find a legal rule, legal principle, or relevant doctrine that can be used to address a legal issue encountered in a study. Meanwhile, in this research, the researcher will examine all regulations (positive law, principles, and legal doctrines) that are applicable in Indonesia and will not overlook the comparison of regulations in other countries to correlate various legal behaviors resulting from the said regulations in an effort to find answers to the research questions.[10] Additionally, the approach used in this research is an empirical legal approach, which positions the study within its core focus as law conceptualized as actual behavior in every societal relationship to identify and test the effectiveness of a law in societal life (Abdulkadir Muhammad, 2004: 52).[11]

Based on these research methods and approaches, the research data sources for this study are identified into two sectors: primary data sources, which consist of interviews with informants from Diskominfo Jateng, and secondary data sources based on literature, which involves reviewing literature from books, journal articles, websites, relevant legislation, principles, norms, doctrines, regulations implemented in comparative countries, and other relevant data sources. The data collected and inventoried will then be processed by reducing and sorting the data deemed relevant. The next step is to analyze the processed data, which will then be used to answer the research questions in the form of a written presentation.

[10] Peter Mahmud Marzuki. *Penelitian Hukum Edisi Revisi.* (Jakarta: Kencana, 2019). pp. 25.
[11] Abdulkadir Muhammad. *Hukum dan Penelitian Hukum*. (Bandung: Citra Aditya Bakti, 2004).

The Overview of Personal Data Protection for Indonesian Society in the Era of Society 5.0

a. Addressing Personal Data Protection Problems in Indonesia's Society 5.0

"What is Society 5.0? Why is this concept often discussed nowadays? Is it important to discuss it?" These questions frequently populate journal article pages today and have become research inquiries. However, answering these questions is not as simple as saying, "*Society 5.0 is a concept where society adopts technological and informational advancements to support their lives*." When this concept is juxtaposed with current issues, it necessitates a comprehensive analysis and validation through several variables. In this research, the urgency of personal data protection for Indonesian society in the era of Society 5.0 will also examine the social aspects of the government's political efforts to meet this need and the legal constructs implemented.

Based on the Japanese government's statement in Faruqi (2019:67), it can be understood that Society 5.0 is a new concept supporting technological advancement centered on humans in its application to social life. The resolution of social problems will always consider humanistic aspects by integrating "cyberspace" with "physical space." According to him, the birth of the Society 5.0 concept partly stems from the nature of instant gratification, which is a tendency to desire everything needed instantly without much effort. Thus, technology comes to facilitate their affairs more instantly and gradually reduces the effort they put into performing tasks. However, before the era of Society 5.0, technological advancements tended to overlook humanistic aspects, ultimately leading to the concept of "bringing distant things closer while distancing those that are near," or essentially creating antisocial attitudes resulting in social gaps within society. Regardless, the concept of Society 5.0 must be understood in the context of its development from current societal situations to comprehend social conditions and attitudes at each stage of its progress. Faruqi has illustrated the development of this revolution with the following image:

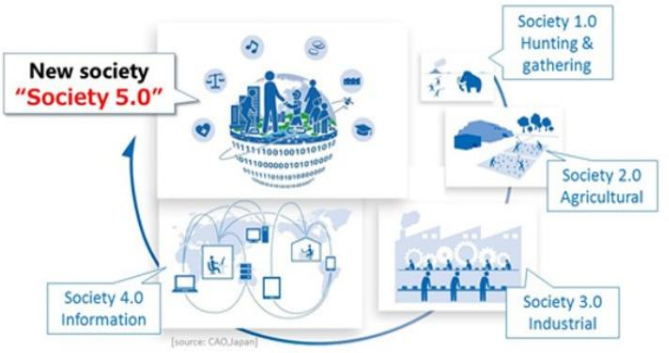

Figure 1: *Illustration of Revolution (Society 1.0-Society 5.0)*
Source: *Faruqi (2019: 68)*

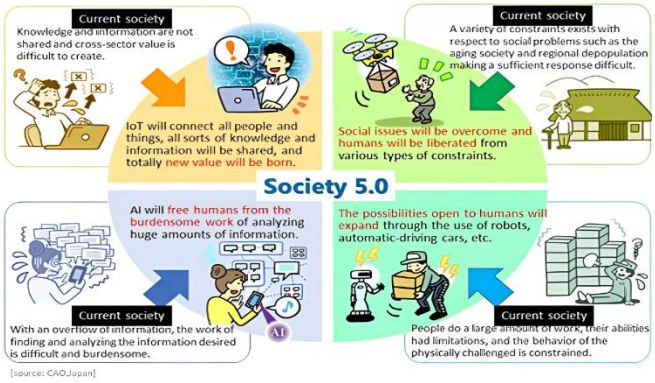

Figure 2: *Illustration of the Current Situation of Society toward the Desired Situation*
Source: *Faruqi (2019: 69)*

Reviewing the image presented, it can be seen that society is now transitioning to the Society 5.0 model with significant changes or radical improvements that began in the era of information development in Society 4.0 (see Fig. 1). In this era, human connectivity knows no bounds and occurs very rapidly. The consequence of this is the blurring of demographic boundaries, especially in terms of communication, which becomes a new change for society. Ultimately, when entering Society 5.0, society begins to explore the development of Artificial Intelligence, Big Data, Robotics, IoT, and Automation with a humanistic paradigm. In principle, the concept of Society 5.0 is to integrate "*cyberspace*" with "*physical space*", where user information and data on activities in various aspects are stored using technology. Responding to the alignment between the digital world and the physical world, Faruqi (2019: 78) argues that Society 5.0 can be considered successful if the aspect of future service in various sectors is fulfilled, namely, a strong technological capability and competent human resources in their respective fields to achieve a super smart society.[12]

[12] Umar Faruqi, "Future Service in Industry 5.0," *Jurnal Sistem Cerdas* 2, Vol. 1 (2019): 67–79.

Based on this argument, we realize that when entering the Society 5.0 era, user data collection has indeed occurred because this era fundamentally views data as the core of technology such as the development of artificial intelligence and other cyber technologies. The consequence is that the data collected by such technology can be processed according to the user's wishes or misused by third parties. These consequences sometimes have to be accepted by society in their efforts to keep up with this era's developments, which they may not even realize. As a result, the data available in society is sometimes known by irresponsible third parties who use it for personal gain. In fact, Djafar (2019) states that data collection and processing should be conducted with ethical guidelines respecting users' privacy rights and not disregarding the privacy rights of the community.[13]

Scholarly views on Society 5.0 essentially indicate that in the era of Society 5.0, humans are forced to live with rapid technological advancements, as currently every aspect of human life involves such technology (Sintiya & Yulianto, 2024: 5).[14] For example, in the paradigm of bureaucratic modernization, society is forced to transition from paper-based bureaucracy to online form filling, although digital disparities still frequently occur in Indonesia (Hanasi, 2024: 69).[15] Based on these facts, we want to convey that personal data protection when entering the Society 5.0 era becomes crucial for the government to accommodate within a legal framework as legal protection. Satjipto Raharjo (2000) states that legal protection must be expedited to provide protection for human rights for anyone harmed by others. Moreover, the urgency of personal data protection in the Society 5.0 era can also be viewed from the demand to fulfill the aspect of human security.[16] Chenoy (in Sintiya and Yulianto, 2023: 6) states that human security is an effort to protect individuals from all risks that can threaten individual security in physical, psychological, dignity, or welfare corridors. Human security fundamentally also includes personal security, wherein the Society 5.0 paradigm, cyber security is also part of personal security, useful for protecting information security. Furthermore, regarding

[13] Djafar, W. (2022, September 1). *Hukum Perlindungan Data Pribadi di Indonesia.* Retrieved from learninghukumonline.com.
[14] Tiyas Sintiya and Retnandika Yulianto, "Analisis Kebijakan Indonesia Terkait Dengan Perlindungan Dta Diri Warga Indonesia," *Case Law: Journal of Law* 5, no. 1 (2024): 1–16.
[15] Raihan Hanasi, "Peran Teknologi Informasi Dalam Modernisasi Administrasi Publik," *Jisosepol: Jurnal Ilmu Sosial Ekonomi Dan Politik* 1, no. 1 (2024): 64–70.
[16] Satjipto Rahardjo, Ilmu Hukum, ed. Awalludin Mawan (Bandung: PT. Citra Aditya Bakti, 2014).

personal data security, privacy rights become a fundamental human right that must be maintained and realized within the security concept.[17]

Violations of individuals' personal data in cyberspace are essentially part of cybercrime, which is a series of illegal activities that use and target computer systems and networks. Christianingrum & Aida (2021) state that from 2019 to 2021 in Indonesia, there were at least cyber anomalies in the form of data leak indices in the government sector amounting to 45.5% of 741.4 million or about 337.337 million anomaly traffic. It is reiterated that in the era of Society 5.0, data security is substantial because, in this era, the physical and virtual worlds are integrated, making the boundaries blurred.[18] Given the personal data leakage index previously mentioned, the government, responsible for collecting and managing the community's personal data, should be accountable. So far, in implementing electronic government (*e-government*), Iswandari (2022:81) states that the legal guarantee for personal data protection is still fragmented within each regulation and legislation, which could lead to overlaps between institutions in addressing these problems. Iswandari adds that ambiguity in guaranteeing personal data security in the context of e-government implementation could potentially affect public trust, as fundamentally, if this ambiguity is not immediately addressed, it cannot guarantee justice and certainty for the parties involved. The ambiguity in handling data breaches by the Indonesian government essentially indicates that the government has not been able to guarantee the security of the community's personal data and has not been able to provide tangible sanctions for cybercrime perpetrators.[19] Sintiya and Yulianto (2023: 12) also state that the government has not been able to maximize its power in ensuring the security of Indonesian citizens' data when referring to a top-down approach in the state's security conception.[20] On the other hand, the government's ineffectiveness in addressing data breach issues as contemporary problems indicates that the government has not successfully functioned in ensuring the security of society within the human security paradigm (Boer & Wilde, 2008).[21]

---

[17] Sintiya & Yulianto, Op. Cit., 6

[18] Christianingrum, R., & Aida, A. (2021). *Analisis RUU Tentang APBN: Tantangan Penguatan Keamanan Siber dalam Menjaga Stabilitas Keamanan Nasional*.

[19] Iswandari, B. (2022). "Jaminan Keamanan Data Pribadi Warga Negara dalam Penyelenggaraan Urusan Pemerintahan Berbasis Elektronik (E-Government)". *Dharmasisya: Jurnal Program Magister Hukum Fakultas Hukum Universitas Indonesia*, *2*(1), 75–86.

[20] Sintiya & Yulianto, Op. Cit., pp. 12

[21] Boer, M., & Wilde, J. *The Viability of Human Security*. (Amsterdam: Amsterdam University Press, 2008)

b. An Overview of Legal Politics of Personal Data Protection in Indonesia and Its Impact on Personal Data Protection in the Era of Society 5.0

Basically, the law functions to regulate all aspects of human life by norming human behavior. As stated by Arif Sidharta (1999) in his book titled *Reflection on the Structure of Legal Science*:

> "Many factors are related to efforts to realize effective law, including the substance of the law itself, law enforcement apparatus, and the legal culture of society, which are the most dominant factors in efforts to realize effective law, considering that legal culture encompasses all values, attitudes, feelings, behavior, and legal awareness."[22]

Essentially, the law is required to be an institution that works effectively within society to fulfill aspects of order and certainty in realizing the ideals of society as outlined in the preamble of the 1945 Constitution of the Republic of Indonesia. Therefore, when the Indonesian government commits to actively engaging in digital governance through the e-government framework, it must maximize efforts to protect personal data as a consequence of human civilization's progress. The recent incident that shocked Indonesian society on June 20, 2024, namely the Ransomware attack on the National Data Center, indeed endangered the security of Indonesians' private data because, in principle, Ransomware infections will ecrypt data in a data center unless the government, as the victim, pays a ransom (Hartono, 2023: 56).[23] However, through national news, the Deputy Minister of Communications and Information Technology, Nezar Patria revealed that this attack did not endanger the information and personal data taken over by the hackers. Consistent with this view, the Head of BSSN, Siburian, together with Telkom's Director of Network & IT Solution, Wijarnako, confirmed that the sensitive data of victims had been encrypted by the Ransomware itself, making the data unusable (CNBC: 2024).[24] The author believes that this issue further highlights the government's poor commitment to personal data protection because it has been unable to mitigate this problem despite its repeated occurrences. In fact, the presence of Law No. 27 of 2022 mandates in Article 16 that every personal data processing by anyone, including the government, must guarantee the rights of personal data subjects and be accountable through a series of data processing that protects against illegal access.

---

[22] Sidharta, A. (1999). *Refleksi tentang Struktur Ilmu Hukum*. Mandar Maju.
[23] Hartono, B. (2023). "Ransomware: Memahami Ancaman Keamanan Digital". *Bincang Sains Dan Teknologi*, *2*(2), 55–62.
[24] CNBC. (2024, June 24). *Asing Sorot Pemerintah RI Ogah Bayar Rp 131 M ke Hacker PDN*. Retrieved from cnbcindonesia.com:

CHALLENGES IN ENSURING PERSONAL DATA PROTECTION

The legal basis applicable in Indonesia for the implementation of electronic information is generally regulated by Law No. 19 of 2016 concerning Electronic Information and Transactions, known as the ITE Law, along with its derivative regulations. However, specifically to address the issue of personal data protection, the government enacted Law No. 27 of 2022 concerning Personal Data Protection in 2022. The enactment of this law arose from a collective awareness following a series of cyberattacks targeting citizens' data. The initial awareness formed when the government realized that personal data security is a vital aspect of advancing technology utilization, requiring a robust concept to accommodate privacy rights as part of human rights protection (Fauzi & Shandy, 2022: 451).[25] Regarding the concept of personal data protection as the basis for the Personal Data Protection (PDP) Law, Warren and Brandeis in their essay *The Right to Privacy* posited in 1890 that rapid technological advancement ignites awareness that everyone has the right to enjoy life. According to them, this right is categorized as inviolable, not to be interfered with by individuals, groups, or the state. Thus, the state, through legal instruments, must be able to accommodate the protection of these privacy rights (Ferera, 2004: 271).[26]

The nomenclature of privacy rights as "inviolable rights" intersects with the definition of Non-Derogable Rights in Human Rights, as recognized through Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which implies that the state protects personal integrity, honor, dignity, property, and so on inherent to an individual. However, in it's application in Indonesia, Article 15 of the PDP Law mentions that privacy rights and personal data protection are placed as derogable rights, meaning their fulfillment can be restricted or even reduced by the state within certain limits (Fauzi & Shandy, 2022: 455). Thus, legal protection efforts for personal data cannot be separated from the government's legal politics as a cohesive unit. So what are the government's efforts through legal politics for personal data protection?

Regarding legal politics *rechtpolitiek*, Prof. Soepomo in his book "The History of Adat Law Politics in Indonesia" volumes 1 and 2 discusses the legal politics implemented by the Dutch East Indies colonial government towards the indigenous population. However, his book does not include a conceptual definition or theoretical framework on legal politics. The conceptual definition of legal politics is mentioned by Bagir Manan as "Policy behind the legal policy," dividing it into two types: *first*, the law-making process and *second*, legal politics in law

[25] Fauzi, E., & Shandy, N. (2022). 'Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi". *Lex Renaissance*, *3*(7), 445–461.
[26] Ferrera, G. *CyberLaw Text and Case*. (Bostono: South-Western Cengage Learning, 2004)

enforcement (Anggoro, 2019: 81).[27] In line with this, Mahfud MD in (Latif & Ali, 2010: 19) defines legal politics as the legal policy carried out by the government, discussing how political policy influences law by observing the configuration of forces behind the law-making process. Therefore, legal politics can influence the formulation of legal content in its implementation.[28]

Regarding personal data protection in Indonesia, Pancasila serves as the philosophical foundation for the establishment of the PDP Law, as mentioned in its academic manuscript. Additionally, there is a constitutional obligation for the government to protect all Indonesian citizens and promote general welfare as stated in the 1945 Constitution. Therefore, as mentioned in the academic manuscript for the establishment of the PDP Law, the PDP Law aims to: "(1) protect and guarantee the basic rights of the community related to personal data protection processes; (2) increase legal awareness in society to respect each person's privacy rights, including privacy rights over personal data; (3) ensure that the community receives services from the government within the e-government framework, business actors, and community organizations; (4) prevent the Indonesian nation from cyber exploitation by other nations regarding Indonesian citizens' personal data; (5) increase the growth and progress of the technology, information, and communication industry." Thus, the objectives and goals of establishing the PDP Law inherently contain philosophical, sociological, and juridical reasoning. This is because the PDP Law aims to protect personal data on par with recognizing and protecting fundamental human rights, as stated in several international, regional, and national legal instruments. Furthermore, the current paradigm shift views personal data protection as a basic necessity in managing personal data, an urgency that needs to be addressed promptly to build public trust when entrusting their personal data to the government. Therefore, the presence of the PDP Law enables the government to accommodate broader public interests without worrying about policy ambiguity and widespread data misuse.

Besides seeing to the philosophical and constitutional perspectives, we will also examine the legal politics of personal data protection in Indonesia through Friedman's Legal System Theory, which views law implementation must meet three components: legal structure, legal substance, and legal culture. Briefly, in terms of legal substance, the government has accommodated personal data protection through legal instruments, namely Law No. 27 of 2022, which generally contains 76 articles, including principles of personal data protection; recognition of personal data subjects' rights; basic guidelines for personal data processing; basic obligations

[27] Anggoro, S. (2019). “Politik Hukum: Mencari Sejumlah Penjelasan. *Jurnal Cakrawala Hukum”*, *10*(1), 77–86.
[28] Latif, A., & Ali, H. *Politik Hukum*. (Jakarta: Sinar Grafika, 2010)

that must be fulfilled by controllers in processing personal data; regulations on personal data transfer; administrative sanctions; institutional structure; international cooperation; public participation in personal data protection; dispute resolution and legal procedures; prohibitions on using and abusing personal data; and criminal provisions related to personal data protection. Thus, the PDP Law's presence can address the challenges of internet penetration growth.

On the other side, based on data reported by the Indonesian Internet Service Providers Association (APJII) in Fauzi & Shandy (2022: 458), it is known that in 2021-2022, 210 million Indonesians were connected to the internet, or in other words, 77.02% of the total population had embraced the internet as part of progress in the Society 5.0 era. However, the increasing number of internet users in society is not accompanied by public attention to the urgency of personal data protection.[29] Delpiero et al. (2021: 1) state that the public currently lacks concern about data leakage issues. This problem stems from the public's lack of awareness, knowledge, and initiative regarding the vulnerability of their private data. This is evidenced by the continued voluntary provision of personal data on various online services like marketplaces without understanding the potential misuse of personal data.[30] Moreover, Usman (2014: 52) reveals that legal awareness among the Indonesian public is still considered low due to a lack of understanding of legal provisions, lack of appreciation for the law enforcement process, and low morality. Consequently, law enforcement efforts cannot run optimally.[31] The correlation found in the scholars' presentations indicates that the initiative for personal data protection and legal awareness will influence the implementation and enforcement of the PDP Law as a legal culture issue. This issue can be considered a legal culture problem because, according to Friedman (1977), legal culture is a set of values and attitudes that influence how law operates. Friedman adds that legal culture serves to bridge legal regulations with the legal behavior of the entire society. Thus, the public's low initiative for personal data protection affects their compliance with the values contained in the PDP Law.[32]

Another issue related to the legal system for personal data protection in Indonesia is the legal structure. Article 53 paragraph (2) of the PDP Law mandates appointing officials or officers responsible for implementing personal data

[29] Fauzi, E., & Shandy, N. (2022). Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Lex Renaissance*, *3*(7), 445–461.
[30] Delpiero, M., Reynaldi, F., Ningdiah, I., & Muthmainnah, N. (2021). Analisis Yuridis Kebijakan Privasi dan Pertanggungjawaban Online Marketplace dalam Pelindungan Data Pribadi Pengg. *Padjadjaran Law Review*, *9*(1), 1–22.
[31] Usman, A. (2014). Kesadaran Hukum Masyarakat dan Pemerintah Sebagai Faktor Tegaknya Negara Hukum di Indonesia. *Jurnal Wawasan Hukum*, *30*(1), 26–53.
[32] Friedman, L. M. *The Legal System a Social Science Perspective*. (New York City: Russel Sage Foundation, 1975)

protection functions within a merit system paradigm. The merit system is used because the appointed officer must possess professionalism, legal knowledge, practical understanding of personal data protection, and all other abilities to fulfill their duties. However, problems arise when political patronage plays its role. Political expert Lely Arrianie, in an interview with Kompas (2023), mentions that the appointment of Budi Arie Setiadi, who has a social sciences background, as Minister of Communication and Informatics (Menkominfo) can be seen as political patronage by President Joko Widodo because no true model of political communication is found (Yahya, 2023).[33]

In addition, Article 58 paragraph (2) of Law No. 27 of 2022 mandates the establishment of a personal data protection institution established by the president and responsible to the president with the authority as stipulated in Article 60. However, until now, the personal data protection institution has not been established by the government. This personal data protection institution is important to maintain the protection of personal data belonging to personal data subjects in Indonesia. So this is a problem for the supervision of personal data protection in Indonesia. As a matter of impact and need to be considered is the personal data owned by the subject of personal data owned by consumers who use e-commerce services with personal data described in Article 4 paragraphs (1), (2), and (3). In the explanation of Article 4 para- graph (3) letter f, it states that IP (Internet Protocol) Address and cellular phone number are personal data combined to identify a person and are general Personal Data.[34] The personal data requested and used by this E-Commerce service provider is in the form of a full name with a general personal data classification and a telephone number as a type of personal data combined with a special personal data classification. In addition, to access additional features, the E-Commerce service provider will request additional personal data such as facial images and dactyloscopy as biometric personal data, and credit card number data as personal financial data. Especially for data protection of cellular phone numbers as one type of combined personal data, it still has a recht vacuum status to be further regulated for its protection as personal data after the issuance of Law Number 27 Year 2022. In e-commerce transactions, there are basically consumers who purchase goods. Indirectly, consumers in e-commerce transactions are also subjects of personal data.[35] Ditambah lagi, domestic trade manuevers are increasing complex. As domestic data up third quarter of 2022, there are 2,987 Micro, Small,

[33] Yahya, A. (2023, July 17). *Pengangkatan Budi Arie Jadi Menmkominfo Dinilai sebagai Politik Balas Budi Jokowi*. Retrieved from Kompas.com:

[34] Tegar Islami Putra and Nurul Fibrianti, "Threats and Legal Protection of Personal Data Combined in E-Commerce Transactions Based on Personal Data Protection Law in Indonesia," *Lambung Mangkurat Law Journal* 9, no. 1 (2024): 67.

[35] Tegar Islami Putra, (2024) "Data Protection Impact Assessment Indicators In Protecting Consumer E-Commerce Platforms," *The Indonesian Journal of International Clinical Legal Education*, 6, (1): 12.

and Medium Enterprises (MSMEs) and companies registered as vendors with 21,018 procurement transactions that have been completed with a transaction value of IDR 41,6 billion and will continue to grow.[36]

c. Taking a Look to International Regulation and Overseas Law About Personal Data Protection

Violation of privacy rights is not only experienced by Indonesia. Several individuals, legal entities, companies, and countries outside Indonesia have also faced similar issues. Some famous cases include the personal data breach experienced by Facebook, which was caused by Cambridge Analytica misusing the personal data of 87 million Facebook users through illegal access for the benefit of the 2016 US Presidential campaign (Zaelany & Putranti, 2023: 126).[37] Additionally, Google, USA also had a similar experience for not providing a simple mechanism for rejecting the use of cookies for data subjects. As a result, Google USA was fined 60 million euros by the French Data Protection Authority. Furthermore, the *Bundesverfassungsgericht* (BVG) or the German Constitutional Court once ruled that local police and intelligence officers had excessive access to individuals' private data. In their defense, the relevant parties argued that intercepting private data of mobile phone and internet users through access to private mobile phone traffic data was necessary as an effort to combat major and organized crimes, such as terrorism. However, the BVG rejected this exception and decided that any interception of private data constitutes a violation of the state constitution (Sutrisna, 2021: 8).[38] These cases show that personal data protection (privacy rights) must be fulfilled through legal instruments and the political will of the government. So how does the international community regulate the protection of personal data?

The focus on personal data protection is not only experienced by the Indonesian government. The international community has also paid special

[36] Tegar Islami Putra & Nurul Fibrianti, (2024) "Criminalization of Consumers for Criticism Given to Companies Through Cyberspace in Theoritical Studies," *Annual Review of Legal Studies* 1, (2): 181.

[37] Zaelany, F., & Putranti, I. (2023). "Pelanggaran Privasi dan Ancaman Terhadap Keamanan Manusia dalam Kasus Cambridge Analytica". *Journal of International Relations Diponegoro*, *9*(1), 125–137.

[38] Sutrisna, C. (2021). "Aspek Hukum Perlindungan Data Pribadi dan Kondisi Darurat Kebocoran Atas Data Pribadi di Indonesia". *Wacana Paramarta Jurnal Ilmu Hukum*, *20*(5), 1–10.

attention to this issue following the Universal Declaration of Human Rights (UDHR). Article 12 states, "No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." Therefore, Article 12 of the UDHR can be considered an umbrella term because it regulates the protection of other rights, namely family, home, honour, and reputation. In terms of privacy rights, according to Eide & Gudmur (1992: 188-214), Article 12 of the UDHR has a very broad scope. These include: a) Physical Privacy, which protects an individual's privacy related to their residence. b) Decisional Privacy, which protects an individual's right to determine their own life path, including their family life. c) Dignity as an instrument in protecting a person's self-esteem, including their name and reputation. d) Informational Privacy, which is referred to as the right of individuals to determine how to manage and store their information. Thus, the UDHR comprehensively regulates fundamental human rights, one of which is the right to privacy that frees individuals to determine how to manage and store their personal information, termed as the "common standard of achievement for all peoples and all nations".[39]

Not only does the UDHR focus on the protection of privacy rights, but the 1966 International Covenant on Civil and Political Rights (ICCPR) also regulates the protection of personal data as privacy rights through Article 17, which states: "(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, nor to unlawful attacks upon his honour and reputation. (2) Everyone has the right to the protection of the law against such interference or attacks." Jayawickrama in Sinta Dewi Rosadi (2020: 50) mentioned that in Article 17 of the ICCPR 1966, the terms "arbitrary and unlawful" were added to ensure that privacy rights must be protected and prohibit the state from violating them.[40] Bygrave (1998: 4) stated that the regulation of privacy through Article 17 of the ICCPR 1966 constitutes the strongest legal basis in international law for the protection of personal data. This opinion was proposed because, essentially, Article 17 of the ICCPR requires a state to

[39] Eide, A., & Swinehart, Theresa. *The Universal Declaration of Human Rights: A Commentary*. (Oslo: Scandinavian University Press, 1992)
[40] Rosadi, S. *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022)*. (Jakarta: Sinar Grafika Offset, 2023)

protect citizens' privacy regarding personal information through legislation. In implementing the values and spirit of the ICCPR, Indonesia responded by ratifying the ICCPR through Law No. 12 of 2005 on the Ratification of the International Covenant on Civil and Political Rights, which is the precursor to the Personal Data Protection Law. By ratifying the ICCPR, Indonesia is obligated to protect the personal data of its citizens as part of fulfilling the state's obligations as stipulated in the ICCPR.

The enforcement of legal provisions in other countries also focuses on the issue of personal data security. Several mature legal instruments are applied multilaterally, regulating recognized data privacy principles through international legal instruments, and serving as a foundation for modern national data protection laws. For instance, the Organization for Economic Cooperation and Development (OECD) Privacy Guidelines. Although not a legal instrument, the OECD Privacy Guidelines have inspired several regimes worldwide to establish regulations on personal data protection. This influence is because the OECD Privacy Guidelines contain statements of norms that construct personal data. Therefore, these guidelines can mobilize all OECD members and private organizations under them to formulate policies regarding personal data protection (Rosadi, 2022: 58).[41] Generally, the OECD Privacy Guidelines contain guidelines and principles that members must follow in managing personal data. Some of these principles include: 1) Limiting access and efforts in collecting personal data. 2) Prioritizing data quality. 3) Specifying the purpose of data collection and management. 4) Limiting data disclosure. 5) Security guidelines and procedures. 6) Transparency principle. 7) Individual participation. 8) Accountability in data management.

Besides the OECD Privacy Guidelines that function as norms, principles, and guidelines, the international community also recognizes the General Data Protection Regulation (GDPR), which is applied multilaterally in the European Union. The metamorphosis of the GDPR cannot be separated from privacy rights enshrined in Article 8, Section 1 of the European Convention on Human Rights of 1950, which refers to the right of every individual to respect for their private life. Over time, the GDPR emerged, replacing the European Union Directive (EU Directive) 95/46/EC: The Data Protection Directive and local personal data protection laws within the European Union.

[41] Ibid., 58

The substance of the GDPR related to personal data management principles is regulated through Article 5 of the GDPR, which includes: 1) Transparency, Legality, and Fairness in Management. 2) Purpose Limitation in Management. 3) Data Minimization. 4) Storage Limitation. 5) Enforcement of Confidentiality and Integrity Principles. 6) Accuracy Principle.

Unlike Indonesia, the government's attention to personal data protection for its citizens in Singapore and Malaysia started much earlier. The Singaporean government regulates the protection of its citizens' personal data through The Personal Data Protection Act No. 26 of 2012 Singapore, which contains three main values: 1) Consent, which stipulates that an organization is allowed to manage an individual's personal data if there is an agreement from the data subject. 2) Purpose, which includes protocols for the collection, use, and disclosure of a person's personal data in any situation, provided that the personal data management organization must inform the data subject about the data management. 3) Reasonableness, which grants authority to an organization to manage an individual's personal data if done for a reasonable purpose. Meanwhile, Malaysia regulates personal data protection through the Personal Data Protection Act No. 709 of 2010, which contains seven general principles of personal data protection: 1) management of personal data based on the consent of both parties. 2) Disclosure. 3) Security. 4) Notification. 5) Data management integrity. 6) Providing options. 7) Retention and accessibility principles.

d. What is Personal Data Protection Problems in Era of Society 5.0? Comparative Cases of Southeast Asian Countries

Personal data leakage is a serious problem faced by many countries around the world, including Southeast Asian countries. Therefore, personal data protection has become an important issue in the ASEAN region, especially with the increasing use of the internet and digital technology in the region.[42] However, there are still challenges in developing this legal framework. Some countries in Southeast Asia still do not have strong enough laws for personal data protection, and the implementation of existing laws still needs to be improved. In addition, cybersecurity issues such as hacking

[42] D. G. S Mangku et al., (2021) "The Personal Data Protection of Internet Users in Indonesia," *Journal of Southwest Jiaotong University,* 56 (1), 202-209.

and identity theft are still significant threats to personal data privacy in the region. On the other hand, the development of a robust legal framework for personal data protection in Southeast Asian countries also presents significant opportunities for the region. In the era of globalization and digitalization, the region can gain a competitive advantage by attracting investors and businesses that require strong personal data protection guarantees to expand their operations in the region.[43]

Based on empirical evidence, there have been several cases of personal data leakage in Southeast Asian countries in the past six years. Statistics show that in July 2019, the personal data of millions of users of Thailand's Lazada e-commerce platform was leaked due to a security breach in the server. The leaked data included users' full names, email addresses, phone numbers, and home addresses. Then, in August 2020, it was discovered that the personal data of millions of users of the Philippine government website was leaked. The leaked data included the user's name, email address, phone number, date of birth, and home address.[44]

Furthermore, in the same year 2020, a case of personal data leakage occurred in Vietnam, to be precise in October 2020, where the personal data of millions of users of the Tiki electronic commerce platform was leaked due to a cyber attack.[45] The leaked data included full names, email addresses, phone numbers, home addresses, and financial information. A few months later, in 2021, there were back-to-back incidents of personal data leaks in some countries. First, in February 2021, it was discovered that the personal data of millions of Malaysian citizens who registered for financial assistance during the COVID-19 pandemic was leaked.[46] The leaked data includes full name, national identification number, address, phone number, and financial information. Then, in March 2021, there was a case of employee data leakage

[43] Syafri Hariansah et al., "Personal Data Protection in Asean : Indonesia ' S Role in Developing Asean ' S Personal," *India Proceedings of International Seminar on Indonesian Lecturer Is Born to Report Regularly*, n.d., 453–465.
[44] Sofia Abrogar, "Over 1M Records from NBI, PNP, Other Agencies Leaked in Massive Data Breach," INQUIRER.net, 2023, https://newsinfo.inquirer.net/1758456/over-1-million-records-from-nbi-pnp-other-agencies-leaked-in-huge-data-breach.
[45] Luu Quy, "Vietnam Has Major Data Leak Problem, Citizens Suffer," e.vnexpress.net, 2022.
[46] R. Loheswar, "Major Data Breaches in Malaysia in The Past 24 Months," malaymail.com, 2022, https://www.malaymail.com/news/malaysia/2022/12/31/major-data-breaches-in-malaysia-in-the-past-24-months/47722.

in Singapore.[47] In addtiion, Thailand, Philippines and Brunei do not explicitly require data to be localized in the country, but certain obligations relating sensitive information and cybersecurity mandate companies to reach their standards for cross-border transfer which might affect the data storage.[48]

Challenges That May Be Face by the Indonesia Government in Ensuring Personal Data Protection for Society in the Era of Society 5.0

On several previous occasions, the author has stated that in the era of Society 5.0, society is forced to adapt to both physical and virtual environments as a consequence of the accelerating pace of development. Hence, the birth of Law No. 27 of 2022 or the Personal Data Protection Act (UU PDP) is expected to accommodate the protection of the personal data of Indonesian society in terms of legality. Although the legal idea (*Rechtsidee*) has been pursued through a lengthy process, does it make the UU PDP effective in meeting all potential challenges?

Based on a study of the Political Law of personal data protection through the UU PDP with the approach of Friedman's Legal System Theory, several issues are still found in the implementation process of the UU PDP. Therefore, on this occasion, the author will outline some issues of personal data protection in the era of Society 5.0. Among them are:

First is weak regulation. It is indeed true that the UU PDP has gone through a lengthy stage until its enactment and has met academic standards as quality control for a legal product (Rizqiyanto, et al., 2024: 7).[49] Although the UU PDP has been enacted, its existence in providing legal certainty is not clearly visible in providing legal protection to the public. This problem can

[47] Amit Roy Choudhury, "Singapore Public Sector Saw 178 Data Breaches in 2021," itnews.asia, 2022, https://www.itnews.asia/news/singapore-public-sector-saw-178-data-breaches-in-2021-583428.
[48] Supatsara Chaipipat, "ASEAN Governance on Data Privacy: Challenges to Regional ASEAN Governance on Data Privacy: Challenges to Regional Protection of Data Privacy and Personal Data in Cyberspace" (Chulalongkorn University, 2019).
[49] Rizqiyanto, N., Rohman, A., & Raya, F. (2024). "Politik Hukum Pembentukan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi". *Media Hukum Indonesia (MHI)*, *2*(2), 1–14.

be seen in its implementation, where components of protection are sometimes neglected by personal data managers, and there is no legal accountability afterward. This issue arises because the enactment of the UU PDP is not balanced with the presence of implementing regulations and a mandate to a specific institution that handles cases of personal data breaches. Additionally, the implementation of the UU PDP has not been able to accommodate guarantees for recovery for society as victims whose privacy rights have been violated. This is different from Singapore and Malaysia, which have regulations that accommodate society in setting preferences by providing options, management, and limitations on the personal data they manage. Even though Article 8 of the UU PDP gives society the right to terminate the processing of personal data, Indonesia's approach differs from Malaysia and Singapore, which impose more stringent civil and criminal sanctions. In contrast, Indonesia imposes only limited administrative and criminal sanctions on privacy rights violators without strict enforcement (Waspiah, et al., 2023: 5176-5177).[50]

Second, the low awareness and understanding of society about the urgency of personal data protection, coupled with the challenges of Indonesia's human resource intelligence, also pose challenges in the implementation of personal data protection in Indonesia. This opinion is put forward because, in essence, the UU PDP was born with the goal of increasing public legal awareness regarding the process of personal data protection and protecting and guaranteeing the fundamental rights of society related to the process of personal data protection as stated in the academic manuscript of the UU PDP formation. Thus, the UU PDP generally mandates active participation by society in personal data protection. As published by A.T Kearney (2018) in Witjacksono & Kriwibowo (2023: 35), it is stated that public awareness of cybersecurity in Indonesia is still very low and can be said to be at the nascent stage. This opinion is based on research conducted by the Communication and Information System Security Research Center (CISSReC) in 2017, which states that in 9 major cities in Indonesia, such as Jakarta, Semarang, Bandung, Yogyakarta, Medan, Surabaya, Palembang, Makassar, and Bali, only 33% of the population in these cities are aware of

[50] Waspiah, Sekar, N., Lies, A., Islami, T., Wida, S., & Widyaning, S. (2023). "Model Perlindungan Hukum Data Pribadi di Era Digital Guna Menjamin Hak Warga Negara Atas Perlindungan Data Pribadi". *Syntax Literate: Jurnal Ilmiah Indonesia*, *8*(9), 5165–5179.

the importance of cybersecurity, including personal data security. This is evidenced by respondents' reluctance to secure private assets connected to cyberspace.[51]

In addition to this information, the latest data released by the Indonesian Internet Service Providers Association (APJII) in Fauzi & Shandy (2022: 458) states that in 2021-2022, as many as 210 million Indonesians were connected to the internet, or in other words, 77.02% of the total population used the internet as part of the progress in the Society 5.0 era. However, the increase in the number of internet users is not accompanied by an increase in awareness, knowledge, and public initiative regarding the vulnerability of personal data. This is evidenced by the continued voluntary provision of personal data on various online services such as marketplaces without understanding the potential misuse of personal data.[52] Yamin, et al. (2024: 145) also support this argument by stating that the low public understanding of the risks of personal data breaches is further exacerbated by the complexity of technology that is increasingly evolving, resulting in the neglect of basic security protocols, such as using strong passwords, regularly changing passwords, updating software regularly, and lack of knowledge about two-factor authentication features. Additionally, the tendency to skip reading privacy policies and terms & conditions set by online services is also a major issue in personal data protection in Indonesia from a societal perspective. Related to societal factors in personal data protection, another challenge that must be watched out for is the low legal awareness of the public.[53] Usman (2014: 52) reveals that legal awareness among the Indonesian public is still considered low due to a lack of understanding of legal provisions, lack of appreciation for the legal enforcement process, and low morality.[54] As a result, legal enforcement efforts cannot run optimally with the low understanding of law among the public. Thus, this challenge must be watched out for, because if ignored, it will result in the ineffective implementation of

[51] Witjaksono, D., & Kriswibowo, A. (2023). Fondasi Keamanan Siber Untuk Layanan Pemerintah. *AL-IJTIMA`I: International Journal of Government and Social Science*, *9*(1), 21–38.
[52] Fauzi, E., & Shandy, N. (2022). Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Lex Renaissance*, *3*(7), 445–461.
[53] Yamin, A., Rachmawati, A., Pratama, R., & Wijaya, J. (2024). Perlindungan Data Pribadi Dalam Era Digital: Tantangan dan Solusi. *Meraja Journal*, *2*(2), 135–155.
[54] Usman, A. (2014). Kesadaran Hukum Masyarakat dan Pemerintah Sebagai Faktor Tegaknya Negara Hukum di Indonesia. *Jurnal Wawasan Hukum*, *30*(1), 26–53.

the UU PDP among the public, as the basic protection provisions are likely to be neglected.

Third, the lack of competence of human resources managing personal data also influences why personal data protection in Indonesia is still considered weak. Essentially, human resources are one of the important factors in ensuring the implementation of cybersecurity as the protocols have been established through the UU PDP. As conveyed by the Director of the Indonesia Cyber Security Forum (ICSF), Ardi Sutedja in (Fatwa, 2019), the key to cybersecurity lies not only in the sophistication of technology but also in the competence of human resources in securing the state when faced with cyber-attacks, such as personal data breaches of Indonesian society. Ardi added that Indonesia needs at least 10,000 cybersecurity engineers and analysts to ensure optimal cybersecurity.[55] However, the need for human resources in the field of cybersecurity is not balanced with the needs of the workforce and educational curriculum that exclude cybersecurity components in learning (BSSN, 2020). The lack of absorption of cybersecurity engineers and analysts is partly due to the unrealized establishment of a personal data management institution as mandated by Articles 58-61 of the PDP law, which is hindered by the absence of a meeting point due to the numerous institutions established by various regulations that cannot work optimally. Thus, the issue of personal data protection is still entrusted to the respective institutions responsible for its management, along with the Ministry of Communication and Informatics (Kominfo) and the National Cyber and Crypto Agency (BSSN) (Waspiah, 2023: 5172).[56]

Nevertheless, Qamar (2020) in Witjaksono & Kriswibowo (2023: 32) states that the understanding of state officials related to cybersecurity is still low. Qamar mentions that the low understanding of state officials on cybersecurity issues, including personal data protection, results in the minimal budget allocated for personal data security. Thus, cybersecurity technology and human resources remain stagnant. Additionally, with the yet-to-be-formed special institution that handles personal data protection of Indonesian society and the management of cyber affairs entrusted to incompetent officials, there is a lack of synergy among institutions in handling personal data protection issues. Synergy in handling cybercrime is

[55] Fatwa, A. (2019, August 22). *Tiap Tahun Indonesia Butuh 10 Ribu SDM Keamanan Siber*. Retrieved from validnews.id

[56] Waspiah, Sekar, N., Lies, A., Islami, T., Wida, S., & Widyaning, S, Op. Cit. 5172

possible because this matter is handled by at least three institutions, namely the National Cyber and Crypto Agency (BSSN), the Indonesian National Police through the Cybercrime Division, and the Ministry of Communication and Informatics (Kominfo) through Civil Servant Investigators (PPNS). Witjaksono & Kriswibowo (2023: 35) mention that the police and Kominfo do not have a clear division of tasks in handling cybercrime, such as personal data protection issues. According to him, this issue actually pits the interests of the two institutions against each other, resulting in a lack of synergy and coordination between the police and Kominfo.[57] This is evidenced by the issue mentioned earlier regarding the breach of the National Data Center, where national news reported the poor performance of Kominfo and BSSN in handling data breaches in the national data center due to sectoral ego (CNN, 2024).[58]

Not only the issue of sectoral ego, but Aznil Tan, an Executive Director of Migrant Watch, in a Kompas report (2024), expressed his opinion that the stubbornness and unwillingness to admit mistakes still color the characteristics of officials in Indonesia. In the case of the National Data Center breach, Kominfo and BSSN were throwing responsibilities and blaming each other. Not only that, they swayed public opinion to excuse this mistake. However, this persuasion did not work because the impact of the National Data Center breach was already experienced by the Indonesian public.[59] This phenomenon triggered various public reactions, such as the emergence of petitions demanding the resignation of the Minister of Communication and Informatics, Budi Arie, on change.org. The Executive Director of the Southeast Asia Freedom of Expression Network (Safenet), Nenden Sekar Arum, in a Kompas report, stated that the public's demand for the resignation of Minister of Communication and Informatics, Budi Arie, through petitions, is not political. However, the demand arose due to performance issues in handling the national data system. Despite the many public demands, there has been no apology or remorse from the Ministry of Communication and Informatics and BSSN for the incident. Thus, there is no

[57] Witjaksono, D., & Kriswibowo, A. Op. Cit., 35
[58] CNNIndonesia. (2024, June 27). *cnnindonesia.com*. Retrieved from Buruk Keamanan Siber di Indonesia Akibat Egosektoral:
[59] Tan, A. (2024, June 28). *usat Data Nasional Jebol: Menkominfo Mundur atau Dimaklumi?* Retrieved from Kompas.com:

moral responsibility from the officials managing the personal data of the Indonesian society, in the era of Society 5.0.[60]

Conclusion

In the era of Society 5.0, marked by the integration of advanced technologies like AI and IoT, personal data protection in Indonesia is critical to prevent data misuse and cyber threats. The implementation of Law No. 27 of 2022 on Personal Data Protection reflects Indonesia's commitment to safeguarding citizens' rights amidst increasing digitalization. However, challenges such as low public awareness, political patronage, and the need for competent officials hinder effective enforcement. Comparing international frameworks like GDPR and laws in Singapore and Malaysia highlights the necessity for Indonesia to strengthen its legal and regulatory measures to ensure robust data protection, thereby fostering human security and addressing the ethical implications of technological advancements.

This research generally identifies various challenges faced by the Indonesian government in protecting citizens' personal data in the era of Society 5.0, despite the enactment of the Personal Data Protection Act (UU PDP) No. 27 of 2022. These challenges include regulatory weaknesses not balanced with implementing regulations and a specialized agency, low public awareness and understanding of the importance of personal data protection, lack of competence in human resources managing personal data, as well as sectoral ego and minimal moral responsibility of the related officials. The implementation of the UU PDP is still far from effective as the existing regulations have not been able to provide recovery guarantees for victims of privacy breaches, while public awareness and understanding, as well as human resource competence in cybersecurity, remain low. Additionally, sectoral ego among related agencies often hampers the handling of personal data protection issues, as seen in the National Data Center breach incident, where related officials passed the responsibility to each other without any clear corrective action.

[60] Nugraheny, D., & Meiliana, D. (2024, June 29). *Safenet: Petisi Tuntut Menkominfo Mundur Murni karena Kinerja, Bukan Politik*.

Acknowledgment

The authors would like to express their gratitude to the Research and Community Services Institute of UNNES (LP2M) for funding this research through the Student Organization Research Funding Scheme. Our sincere thanks to the Faculty of Law, Universitas Negeri Semarang, for being the home institution of the authors. We also extend our appreciation to the Communication and Informatics Agency (Dinas Komunikasi dan Informatika) of Central Java for the opportunity to engage in discussions and gather empirical data.

Special thanks to Mrs. Waspiah, S.H., M.H., as the supervisor of UKM Lex Scientia, for her guidance. We are also deeply grateful to Mr. Laga Sugiarto, S.H., M.H., for the assistance and enlightenment provided to the authors in the development and refinement of this research.

References

Books

Boer, M., & Wilde, J. (2008). *The Viability of Human Security*. Amsterdam University Press.

Eide, A., & Swinehart, Theresa. (1992). *The Universal Declaration of Human Rights: A Commentary*. Scandinavian University Press.

Ferrera, G. (2004). *CyberLaw Text and Case*. South-Western Cengage Learning.

Friedman, L. M. (1975). *The Legal System a Social Science Perspective*. Russel Sage Foundation.

Guntur, Waham, Wishnu, Huda, & Nurdiayantoro. (2020). *Perkembangan Teknologi Informasi di Indonesia Menghadapi Industri 5.0.* CV Jagad Media Publishing.

Latif, A., & Ali, H. (2010). *Politik Hukum*. Sinar Grafika.

Marion, N. E., & Twede, J. (2020). *Cybercrime: An Encyclopedia of Digital Crime*. ABC-CLIO.

Marzuki, P. M. (2019). *Penelitian Hukum Edisi Revisi*. Kencana.

Muhammad, A. (2004). *Hukum dan Penelitian Hukum*. Citra Aditya Bakti.

Rosadi, S. (2022). *Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional (Edisi Revisi)*. Refika Aditama.

Rosadi, S. (2023). *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022)*. Sinar Grafika Offset.

Sagala, M., Muttaqin, Chamidah, D., Simarmata, J., Karim, A., Samosir, K., Ardiana, D., Antares, J., & Jamaludin. (2021). *Hukum dan Cybercrime*. Penerbit Kita Menulis.

Sidharta, A. (1999). *Refleksi tentang Struktur Ilmu Hukum*. Mandar Maju.

Journal Article

Amrozi, Y., Nadiya, K., Rahmah, L., Shofiyah, N., & Thowimma, O. (2021). Tantangan Security dan Kehandalan Sistem dalam Aplikasi Bergerak. *Jurnal Pendidikan Teknologi Informasi (Jukanti)*, *4*(2), 1–10.

Anggoro, S. (2019). Politik Hukum: Mencari Sejumlah Penjelasan. *Jurnal Cakrawala Hukum*, *10*(1), 77–86.

Chaipipat, S. (2019). *ASEAN Governance on Data Privacy: Challenges to Regional ASEAN Governance on Data Privacy: Challenges to Regional Protection of Data Privacy and Personal Data in Cyberspace*. Chulalongkorn University.

Bahtiar, R. (2020). Potensi, Peran Pemerintah, dan Tantangan dalam Pengembangan E-Commerce di Indonesia [Potency, Government Role, and Challenges of E-Commerce Development in Indonesia]. *Jurnal Ekonomi & Kebijakan Publik*, *11*(1), 13–25.

Delpiero, M., Reynaldi, F., Ningdiah, I., & Muthmainnah, N. (2021). Analisis Yuridis Kebijakan Privasi dan Pertanggungjawaban Online Marketplace dalam Pelindungan Data Pribadi Pengg. *Padjadjaran Law Review*, *9*(1), 1–22.

Faruqi, U. (2019). Future Service in Industry 5.0. *Jurnal SIstem Cerdas*, *2*(1), 67–79.

Fauzi, E., & Shandy, N. (2022). Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Lex Renaissance*, *3*(7), 445–461.

Hanasi, R. (2024). Peran Teknologi Informasi dalam Modernisasi Administrasi Publik. *Jisosepol: Jurnal Ilmu Sosial Ekonomi Dan Politik*, *1*(1), 64–70.

Hartono, B. (2023). Ransomware: Memahami Ancaman Keamanan Digital. *Bincang Sains Dan Teknologi*, *2*(2), 55–62.

Iswandari, B. (2022). Jaminan Keamanan Data Pribadi Warga Negara dalam Penyelenggaraan Urusan Pemerintahan Berbasis Elektronik (E-Government). *Dharmasisya: Jurnal Program Magister Hukum Fakultas Hukum Universitas Indonesia*, *2*(1), 75–86.

Putra, T. I. (2023). Juridical Analysis of The Application of Local Currency Settlement Between Indonesia and China in Business Transactions. *Journal of Private and Commercial Law*, *7*(2), 13–34.

Putra, Tegar Islami. (2024) "Data Protection Impact Assessment Indicators In Protecting Consumer E-Commerce Platforms." *The Indonesian Journal of International Clinical Legal Education* 6 (1), 1–22.

Putra, Tegar Islami, and Nurul Fibrianti. (2024). "Criminalization of Consumers for Criticism Given to Companies Through Cyberspace in Theoritical Studies." *Annual Review of Legal Studies,* 1 (2), 179–204.

Putra, T. I., Fibrianti, N., Fakhis, A. Z. P., & Fakhrullah, M. R. (2024). Critically Reveal The Dimensions of Damage From Unauthorized Use of Personal Data. *The Digest: Journal of Jurisprudence and Legisprudence*, *5*(2), 231-262. https://doi.org/10.15294/digest.v5i2.19941

Putra, T. I., Fakhis, A. Z. P., Tussaleha, A., Firdhausya, M. U., & Aflah, M. H. N. (2025). Risks of Consumer Personal Data Protection at the Personal Data Processing Stage of E-Commerce Websites. *Journal of Private and Commercial Law*, *8*(2), 110-127. https://doi.org/https://journal.unnes.ac.id/journals/jpcl/article/view/20081/3828

Putra, T. I., Fibrianti, N., & Fakhis, A. Z. P. (2025). Implementation of CNIL's Basic Logging Measures in Indonesia : A Juridical Study on Personal Data Protection. *The Indonesian Journal of International Clinical Legal Education*, *7*(2), 203–234.

Putra, Tegar Islami, Akbar Jihadul Islam, and Abdullah Mufti Abdul Rahman. (2024). "Integrating Islamic Laws into Indonesian Data Protection Laws: An Analysis of Regulatory Landscape and Ethical Considerations." *Contemporary Issues on Interfaith Law & Society,* 4 (1), 85–118.

Rizqiyanto, N., Rohman, A., & Raya, F. (2024). Politik Hukum Pembentukan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Media Hukum Indonesia (MHI)*, *2*(2), 1–14.

Saleh, A. (2021). Perlindungan Data Pribadi Dalam Perspektif Kebijakan Hukum Pidana. *Hukmy: Jurnal Hukum*, *1*(1), 91–108.

Saputra, T., & Rasji. (2023). Perlindungan Data Pribadi Sebagai Pemenuhan Atas Hak Privasi di Era Digital. *Nusantara: Jurnal Ilmu Pengetahuan Sosial*, *10*(1), 349–357.

Sari, A. (2023). Aspek Hukum Perlindungan Data Pribadi Sebagai Hak Privasi Pengguna Media Sosial. *Jurnal Rectum: Tinjauan Yuridis Penanganan Tindak Pidana*, *5*(1), 970–980.

Sintiya, T., & Yulianto, R. (2024). Analisis Kebijakan Indonesia Terkait dengan Perlindungan Dta Diri Warga Indonesia. *Case Law: Journal of Law*, *5*(1), 1–16.

Sutrisna, C. (2021). Aspek Hukum Perlindungan Data Pribadi dan Kondisi Darurat Kebocoran Atas Data Pribadi di Indonesia. *Wacana Paramarta Jurnal Ilmu Hukum*, *20*(5), 1–10.

Usman, A. (2014). Kesadaran Hukum Masyarakat dan Pemerintah Sebagai Faktor Tegaknya Negara Hukum di Indonesia. *Jurnal Wawasan Hukum*, *30*(1), 26–53.

Waspiah, Sekar, N., Lies, A., Islami, T., Wida, S., & Widyaning, S. (2023). Model Perlindungan Hukum Data Pribadi di Era Digital Guna Menjamin Hak Warga Negara Atas Perlindungan Data Pribadi. *Syntax Literate: Jurnal Ilmiah Indonesia*, *8*(9), 5165–5179.

Witjaksono, D., & Kriswibowo, A. (2023). Fondasi Keamanan Siber Untuk Layanan Pemerintah. *AL-IJTIMA`I: International Journal of Government and Social Science*, *9*(1), 21–38.

Yamin, A., Rachmawati, A., Pratama, R., & Wijaya, J. (2024). Perlindungan Data Pribadi Dalam Era Digital: Tantangan dan Solusi. *Meraja Journal*, *2*(2), 135–155.

Yitawati, K., Purwati, Y., Sarjiyati, & Sukarjono, B. (2022). Implikasi dan Sosialisasi Undang-Undang tentang Perlindungan Data Pribadi dalam Menjaga Kerahasiaan Data Pribadi Seseorang. *DAYA - MAS: Media Komunikasi Hasil Pengabdian Dan Pemberdayaan Masyarakat*, *7*(2), 90–95.

Yuniarti, S. (2019). Perlindungan Hukum Data Pribadi Di Indonesia. *Binus Journal Publishing*, *1*(1), 147–154.

Zaelany, F., & Putranti, I. (2023). Pelanggaran Privasi dan Ancaman Terhadap Keamanan Manusia dalam Kasus Cambridge Analytica. *Journal of International Relations Diponegoro*, *9*(1), 125–137.

Working Paper

BPS. (2022). *Statistik Telekomunikasi Indonesia 2021* (8305002; Telecomunication Statistics in Indonesia 2021).

Christianingrum, R., & Aida, A. (2021). *Analisis RUU Tentang APBN: Tantangan Penguatan Keamanan Siber dalam Menjaga Stabilitas Keamanan Nasional*.

Internet Source

Bangkokpost Publication Team. (2020, November 21). Lazada Denies Being behind Data Leak. Bangkokpost.Com. https://www.bangkokpost.com/thailand/general/2023111/lazada-denies-being-behind-data-leak

CNBC. (2024, June 24). *Asing Sorot Pemerintah RI Ogah Bayar Rp 131 M ke Hacker PDN*. Hentet fra cnbcindonesia.com: https://www.cnbcindonesia.com/tech/20240626141931-37-549501/asing-sorot-pemerintah-ri-ogah-bayar-rp-131-m-ke-hacker-pdn

Djafar, W. (2022, September 1). *Hukum Perlindungan Data Pribadi di Indonesia.* Hentet fra learninghukumonline.com: https://learning.hukumonline.com/wp-content/uploads/2022/09/Hukum-Perlindungan-Data-Pribadi-di-Indonesia-Wahyudi-Djafar.pdf

Ekonomi, W. (2024, June 27). *Tidak Kritis, Pakar Nilai Masyarakat Ikut Bersalah Soal Diretasnya Pusat Data Nasional (PDN)*. Hentet fra wartaekonomi.com: https://wartaekonomi.co.id/read537910/tidak-kritis-pakar-nilai-masyarakat-ikut-bersalah-soal-diretasnya-pusat-data-nasional-pdnhttps://wartaekonomi.co.id/read537910/tidak-kritis-pakar-nilai-masyarakat-ikut-bersalah-soal-diretasnya-pusat-data-nasional-pdn

Fatwa, A. (2019, August 22). *Tiap Tahun Indonesia Butuh 10 Ribu SDM Keamanan Siber*. Hentet fra validnews.id: https://validnews.id/nasional/Tiap-Tahun-Indonesia-Butuh-10-Ribu-SDM-Keamanan-Siber-ivS

Indonesia, C. (2024, June 27). *cnnindonesia.com*. Hentet fra Buruk Keamanan Siber di Indonesia Akibat Egosektoral: https://www.cnnindonesia.com/nasional/20240627100303-20-1114729/buruk-keamanan-siber-di-indonesia-akibat-egosektoral

Nugraheny, D., & Meiliana, D. (2024, June 29). *Safenet: Petisi Tuntut Menkominfo Mundur Murni karena Kinerja, Bukan Politik*. Hentet fra kompas.com: https://nasional.kompas.com/read/2024/06/29/13545771/safenet-petisi-tuntut-menkominfo-mundur-murni-karena-kinerja-bukan-politik

Tan, A. (2024, June 28). *usat Data Nasional Jebol: Menkominfo Mundur atau Dimaklumi?* Hentet fra Kompas.com: https://nasional.kompas.com/read/2024/06/28/08212831/pusat-data-nasional-jebol-menkominfo-mundur-atau-dimaklumi?page=all

Yahya, A. (2023, July 17). *Pengangkatan Budi Arie Jadi Menmkominfo Dinilai sebagai Politik Balas Budi Jokowi*. Hentet fra Kompas.com: https://nasional.kompas.com/read/2023/07/17/17544261/pengangkatan-budi-arie-jadi-menmkominfo-dinilai-sebagai-politik-balas-budi