Barelang Journal of Legal Studies
Volume 1 Issue 1 (March 2023), pp. 72-89
ISSN (Online): -
Published by Universitas Internasional Batam, Indonesia

An Academic Analysis of Data Privacy Frameworks in Indonesia

Sebastian Tan[1*], Calvin Alexander[2], Tantimin[3]
*Corresponding Author

Received: 21-3-2023
Revised: 15-3-2023
Accepted: 10-4-2023
Published: 20-5-2023

Citation:
Tan, S., Alexander, C., & Tantimin, T. (2023). An Academic Analysis of Data Privacy Frameworks in Indonesia. *Barelang Journal of Legal Studies*, 1(1), 72-89.

ABSTRACT

The rapid advancement of the digitalization era has led to a growing emphasis on safeguarding personal data. The collection, management, and storage of personal data have become more streamlined through the integration of technology, a development that has raised concerns regarding individual privacy. Privacy is a universally recognized human right that necessitates the legal protection of personal data. In accordance with the rule of law, Indonesia has established legal safeguards for human rights, as explicitly enshrined in the 1945 Constitution. Concurrently, Indonesia has embraced the adoption of information and communication technology, including the internet. Consequently, Indonesia is faced with the imperative of instituting legal safeguards for data protection. In light of this, employing normative juridical research methods, this paper endeavors to elucidate the existing legal framework for the protection of personal data in Indonesia.

Keywords: Personal Data, Legal Protection, Legal Politics
DOI: http://dx.doi.org/10.37253/barjoules.v1i1.8585

[1] Faculty of Law, Universitas Internasional Batam, Indonesia, sbstnrose25@gmail.com
[2] Faculty of Law, Universitas Internasional Batam, Indonesia
[3] Faculty of Law, Universitas Internasional Batam, Indonesia

INTRODUCTION

The age of digitization, characterized by the rapid and widespread integration of digital technology, has ushered in a lifestyle marked by instantaneity and sophistication (Megawati, 2021; Disemadi & Budi, 2023). A prominent outcome of this digital era is the advent of Industry 4.0, which has seamlessly amalgamated digital technology and the internet with traditional industries (Tarantang, Awwaliyah, Astuti, & Munawaroh, 2019). The internet, serving as a vast computer network that interconnects information resources across broad parameters, has emerged as a pivotal driving force behind Industry 4.0, facilitating essential functions such as data acquisition, automated networking devices, the Internet of Things (IoT), extensive big data analytics, cloud computing, and cybersecurity (Raimundo & Rosário, 2022). The omnipresence of this instant and sophisticated internet has ushered in both positive and negative repercussions across various facets of human existence, ranging from lifestyle and behavioral patterns to sociocultural norms.

The utilization of the internet has yielded numerous positive impacts, including its role as a primary medium for information retrieval, a platform for discussions and communications, a means for seamless data transfer, a pivotal learning tool, a facilitator of efficiency in professional endeavors, a medium for visual representation through images and photos, and a critical source of news and health-related information (Prawiyogi & Anwar, 2023). Over the past decade, there has been an unprecedented surge in the adoption of technology, particularly in the realm of internet and digital technology, within Indonesia. The Ministry of Communication and Informatics, specifically the Directorate General of Informatics Applications (Dirjen Aptika), has reported a substantial 11 percent increase in internet users in Indonesia in 2021 compared to the previous year, soaring from 175.4 million to 202.6 million users (Agustini, 2021). This places Indonesia as the 6th highest-ranked country worldwide in terms of internet user population. However, it is imperative to acknowledge that alongside its benefits, internet use also carries detrimental repercussions. These include copyright infringement, violations of intellectual property rights, proliferation of explicit content, dissemination of misinformation, circulation of illicit content, online gambling, instances of hacking, and unauthorized distribution of personal data.

The hacking and subsequent leakage of personal data in Indonesia have become rampant, affecting individuals from all walks of life, including high-ranking state officials, between 2021 and 2022. The extensive personal data breach encompasses comprehensive information such as full names, national identity card details (KTP), phone numbers, email addresses, residential addresses, political affiliations, personal photographs, health records, and even familial information. This disconcerting phenomenon of personal data exposure can be traced back to the initial incident where records of approximately 279 million users of the Health Social Security Administrative Body (BPJS) were made available for purchase on the online forum site Raidforums.com at a price of 0.15 bitcoin, equivalent to approximately IDR 87.6 million. Subsequently, the breach expanded to include data from Bank Rakyat Indonesia (BRI) (Nabila, 2022). According to findings by Hudson Rock, an Israel-based cybersecurity firm, there is substantial evidence indicating that several computers owned by employees of BRI and BRI Life were subjected to cyberattacks, resulting in the unauthorized disclosure of personal information from 2 million customers. This distressing trend further extended to comprise databases from the Indonesian National Police (POLRI), with a staggering 17 million users' data compromised, as well as the leakage of 1.3 billion SIM card numbers. Additionally, the scope of the breach transcended into the domain of governmental officials, encompassing ministers, prominent community leaders recognized across Indonesia, and even reaching up to the presidential level. Notable figures such as Mahfud MD, Johnny G Plate, Joko Widodo (commonly known as Jokowi), and data from the General Election Commission (KPU) have all recently fallen victim to this data exposure. This alarming development was catalyzed by the emergence of an anonymous figure known as "Bjorka," who has garnered recognition as a proficient and trustworthy hacker, primarily due to the fact that the personal data targeted and accessed by "Bjorka" pertained to high-ranking state officials (Sutikno, & Stiawan, 2022).

Indonesia possesses a legal framework that affords protection for personal data, exemplified by the 1945 Constitution of the Republic of Indonesia Article 28G, paragraph (1). This constitutional provision delineates the rights of individuals to safeguard themselves, their family, honor, dignity, and property under their purview. Moreover, Law Number 11 of 2008, specifically the Information and Electronic Transactions Act, Article 30, paragraph (1), prescribes criminal sanctions for illicit access to other individuals' computers and/or electronic systems. Additionally, the Regulation of the Minister of Communication and Informatics Number 20 of 2016 deals with

the Protection of Personal Data in Electronic Systems, albeit certain provisions within these regulations remain somewhat general and only address specific facets. The ramifications of this regulatory landscape have been evident in the proliferation of hacking incidents, leading to the compromise of personal data. It is suggested that the extant legal framework may not be sufficiently adept at safeguarding the personal data of Indonesian citizens (Hisbulloh, 2021). This assertion is substantiated by the surge in cases of personal data breaches over the past year. Consequently, the mounting instances of personal data leakage underscore the exigency for a dedicated legal framework that ensures unequivocal protection for personal data (Bukit & Ayunda, 2022; Weley & Disemadi, 2022).

This requisite has been addressed through the enactment of the Personal Data Protection Bill (RUU PDP), which was recently ratified on September 20, 2022, transforming into Law Number 27 of 2022 concerning Personal Data Protection. The comprehensive ratification of the PDP Law is imperative to afford Indonesian citizens the requisite legal safeguards for their personal data, thus aligning their protection with the provisions of the extant legal framework (Natamiharja, Sabatira, Banjarani, Davey, & Setiawan, 2022). Furthermore, the PDP Law is indispensable for the prosecution and resolution of extensive personal data breaches that have transpired, in addition to proactively forestalling future instances of personal data leakage (Fikri & Rusdiana, 2023).

Research on the safeguarding of personal data is not a novel endeavor, as it builds upon previous scholarly investigations. For instance, Rosalinda Elsina Latumahina delved into the legal dimensions of personal data protection in the realm of cyberspace (Latumahina, 2014). Additionally, Lia Sautunnida explored the pressing need for legislation pertaining to personal data protection in Indonesia, conducting a comparative analysis with the UK and Malaysia (Sautunnida, 2018). Eka Martiana Wulansari concentrated her research on the foundational normative aspects in the context of personal data protection, specifically in relation to an individual's right to privacy in Indonesia (Wulansari, 2020). Lastly, Hari Sutra Disemadi's research addressed the necessity of specialized regulations and the application of artificial intelligence in materializing personal data protection in Indonesia (Disemadi, 2021). Drawing on the collective findings and ideas of these earlier studies, this current research shares a common conceptual framework by exploring personal data protection. However, it distinctively centers

on the legal-political dynamics surrounding the regulation of personal data protection in Indonesia, with a particular emphasis on the Personal Data Protection (PDP) Law and its role in safeguarding the personal data of every Indonesian citizen.

Derived from the aforementioned background context, the research problem is formulated as follows: the study focuses on the regulation of personal data protection in Indonesia and the legal-political aspects governing the establishment of personal data protection frameworks within the Indonesian legal landscape. Consequently, this research endeavors to offer insights into the regulation of personal data protection in Indonesia, along with an examination of the legal-political dynamics influencing the formulation of personal data protection frameworks. This inquiry is grounded in philosophical, juridical, and sociological principles, aiming to enrich the realm of legal literature concerning the regulatory framework for data protection under the Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) in Indonesia.

METHOD

This research adopts the normative juridical research methodology, employing secondary data as the primary source of information. Secondary data, in this context, pertains to information derived from library materials, encompassing books, literature, notes, and reports (Disemadi, 2022). The collected data is subsequently subjected to qualitative and juridical analysis, presented in a structured and scholarly manner to facilitate analytical, descriptive problem elucidation related to this research. Library research, a methodology for data collection, involves an extensive examination of literature, encompassing sources pertinent to the research subject. The library research conducted herein aimed to accumulate secondary data, wherein secondary data obtained includes legal materials in the forms of primary, secondary, and tertiary legal sources. Primary legal materials are binding legal documents endowed with authoritative significance, encompassing statutes, legal commentaries, and judicial decisions, playing a pivotal role in law formulation and adjudication. Secondary legal materials encompass explanatory resources that shed light on primary legal materials, including academic papers, theses, journals, and scientific articles. Tertiary legal materials, on the other hand, constitute auxiliary resources outside the legal domain, utilized by legal researchers to complement and bolster their research data. These tertiary

materials serve as supplementary sources, augmenting the information and data contained in primary and secondary legal sources.

DISCUSSION AND ANALYSIS

Regulatory Framework of Personal Data Protection in Indonesia

Paragraph (3) of the 1945 Constitution of the Republic of Indonesia (hereinafter referred to as the "1945 Constitution") unequivocally proclaims that "Indonesia is a country based on law." This constitutional provision underscores the foundational premise that the Indonesian state is grounded in the principles of a legal state (*Rechtstaat*) rather than being solely reliant on coercive power (*Machtsstaat*). Consequently, the practical realization of these principles necessitates the collective adherence of the populace, the nation, and the state to the conditions and tenets of a legal state. A more granular interpretation of Article 1, Paragraph (3) elucidates that the implementation of these principles must be concomitant with the prevailing laws and regulations, emphasizing the crucial role of the law in ensuring that the social, national, and state affairs are conducted in strict accordance with the established legal framework.

In light of Paragraph (3) of the 1945 Constitution, the fundamental objective of the law is to safeguard the harmonious conduct of the societal, national, and state functions within the bounds of legality. The law, therefore, assumes the pivotal responsibility of establishing the normative framework underpinning all aspects of public life. It ensures that the actions and interactions of the community, the nation as a whole, and the government adhere to the stipulated legal standards, thereby upholding the principle of the rule of law. In essence, the law, as enshrined in the 1945 Constitution, emerges as the quintessential instrument that not only legitimizes the Indonesian state but also regulates and guides the multifaceted dimensions of its existence.

Personal data, as stipulated by the General Data Protection Regulation (GDPR), is delineated as "any information relating to an identified or identifiable individual (data subject)." This encompasses any information that directly identifies an individual or has the potential to ascertain their identity (Ziqra, Sunarmi, Siregar & Leviza, 2021). The GDPR, in explicit terms, enumerates the constituents of personal data to encompass the individual's name, identity

number, location data, online identifier, or any distinctive attributes pertaining to the physical, physiological, genetic, mental, economic, cultural, or social aspects of an individual (Villa & Tan, 2022). Furthermore, the GDPR extends the classification of personally identifiable data to encompass data that may be unidentified in isolation but, when paired with supplementary information, becomes capable of identifying an individual (Yuniarti, 2019).

The safeguarding of personal data is governed by specific regulations within the field of telecommunications and informatics (Hutauruk, Sudirman, Disemadi & Tan, 2023). Initially, the protection of the right to privacy was enshrined in Law Number 36 of 1999 concerning Telecommunications. This law delineated that the confidentiality of personal information and communications constitutes a legal framework for safeguarding personal data and privacy, expressly prohibiting unauthorized wiretapping. Subsequently, broader regulations concerning personal data protection were enacted under Law Number 19 of 2016 concerning Information and Electronic Transactions (ITE Law) (Rosadi, 2017; Yuniarti, 2019). Article 26 of the ITE Law stipulates that "unless otherwise prescribed by law, the utilization of any electronic media information pertaining to an individual's personal data necessitates the explicit consent of the concerned individual." This interpretation underlines that individuals possess full control over their personal data, necessitating prior consent from the data subject for any data utilization. In the event of data misuse, parties aggrieved by such actions have the option to initiate legal proceedings as outlined in Article 26(2) of the ITE Law. They may petition the electronic system operator to erase irrelevant personal data, thereby asserting their rights as data owners. However, it is noteworthy that the ITE Law does not provide an exhaustive definition of "personal data." In contrast, Article 26 merely enumerates that personal rights and personal data protection encompass three fundamental dimensions: the right to privacy, freedom from undue intrusions, the right to communicate without surveillance, and the right to exercise control over access to personal data and information.

Apart from the Information and Electronic Transactions (ITE) Law, which primarily governs personal data protection, several other legal provisions exist that encompass general regulations pertaining to the safeguarding of personal data. Law Number 39 of 1999, titled "Human Rights," addresses the establishment of personal data protection frameworks. Article 21 within this law emphasizes that all individuals possess inherent rights to safeguard their personal

well-being, which includes spiritual and physical aspects. Consequently, individuals should not be subjected to being the subject of research without their explicit consent. The term "subject of research" pertains to any activity that involves individuals being the primary focus, where inquiries are made regarding their personal lives, and personal data is collected, as well as the capturing of their images and voices.

Furthermore, the law also extends its provisions to safeguarding personal data, which implies ensuring the protection of personal information and preventing unauthorized disclosure. It is crucial to delineate the conditions under which personal data may be collected and used to avoid infringing on an individual's right to privacy and consent. This aspect is particularly relevant in an era marked by increased digital data collection and transmission, as it underscores the importance of aligning legal regulations with the evolving technological landscape. In summary, the Law Number 39 of 1999 plays a pivotal role in underlining the significance of obtaining informed consent and protecting personal data in the context of research and other data-driven activities.

The protection of personal data is also addressed in Law Number 24 of 2013 concerning Population Administration. This legislation imposes an obligation on the state to ensure the confidentiality of individual data and proprietary documents. Personal data, which encompasses information that is stored, maintained, and safeguarded with accuracy and kept confidential, is a central concern. Consequently, administrative officers and entities tasked with collecting personal data from citizens are duty-bound to uphold the confidentiality of this data. Moreover, it is noteworthy that Presidential Regulation Number 67 of 2011 provides more detailed provisions related to the implementation of the national identification card (KTP) based on unique identification numbers. Nonetheless, it is crucial to emphasize that this regulation does not encompass the protection of individuals' personal information, particularly concerning requests for the post-recording of fingerprint and eye retina information.

Additionally, the regulatory landscape governing personal data protection extends to the financial sector. Law Number 10 of 1998 concerning Banking delves into the regulation of personal data, primarily concerning issues related to bank secrecy. The legislation stipulates that all information pertaining to customers, including their financial and personal details, must be upheld in strict confidence by the bank, aligning with the fundamental principle of

confidentiality. In a contemporary context, the Financial Services Authority (OJK) has further fortified these data protection provisions by promulgating Regulation No 13/POJK.02/2018 concerning Digital Financial Innovation in the Financial Services Sector. Article 30 of this regulation explicitly assigns the responsibility of maintaining the confidentiality, integrity, and availability of personal data, transaction data, and data derived from such information to fintech business operators. This obligation persists until the ultimate destruction of the data, accentuating the significance of data privacy and protection in modern financial services.

A groundbreaking development in the realm of personal data protection has emerged with the enactment of PDP Law, ratified on September 21, 2022. This landmark legislation has ushered in a new era for the management and safeguarding of individuals' personal data, particularly within the digital domain. The PDP Law defines personal data as information pertaining to identifiable individuals or information that, when combined with other data, can facilitate the identification of individuals, whether directly or indirectly, through electronic or non-electronic systems. The PDP Law serves as a pivotal legal framework aimed at mitigating and addressing the prevalent challenges of personal data breaches and violations, which continue to be a pervasive concern in the realm of personal data protection.

This new legislation represents a critical step towards reinforcing the protection of personal data in Indonesia, and it is poised to play a vital role in enhancing the security and privacy of individuals' information in an increasingly digitalized society. As personal data breaches continue to pose significant threats, the PDP Law is expected to contribute significantly to the prevention and redress of these violations (Nursiyono & Huda, 2023). The effective implementation of this law will demand close collaboration among relevant stakeholders and a comprehensive understanding of its provisions to ensure its potential is fully realized.

The Formation of Personal Data Protection Arrangements in Indonesia: A Legal-Political Perspective

The escalating incidents of hacking and unauthorized leaks of personal data in Indonesia have necessitated a more stringent legal framework for resolution. The existing legal provisions

related to personal data protection appear to be inadequate in safeguarding the privacy of Indonesian citizens (Priscyllia, 2019). These preceding regulations on personal data protection predominantly operated in a partial and sectoral manner, without a comprehensive and intensive approach. To date, there has been no specialized and comprehensive legislation dedicated to the safeguarding of personal data. This is corroborated by recent real-world evidence, manifesting a surge in hacking and the unauthorized release of personal data within Indonesia over the past two years, which has been attributed to negligent actors (Jannah, 2022). The prevalence of these incidents has generated substantial concern and garnered widespread attention among the Indonesian populace, particularly highlighting governmental shortcomings in ensuring the protection of its citizens' rights. The heightened risk of hacking and large-scale data breaches stems from the absence of a well-defined legal framework that specifies mechanisms for law enforcement when violations occur. Therefore, the need for clear and specific rules and regulations, encapsulated within dedicated legislation, has become imperative.

The Indonesian government has not remained passive in its approach to addressing the issue at hand. One significant and effective step taken thus far has been the endorsement and implementation of Law Number 27 of 2022, which pertains to the Protection of Personal Data. This legislative approval marks a pivotal milestone in safeguarding the personal data of Indonesian citizens. The presence of a robust legal foundation, represented by the PDP Law, is expected to serve as a substantial legal framework for government authorities, empowering them to undertake more assertive measures against individuals involved in crimes related to the protection of personal data. The PDP Law encompasses 76 articles, categorically organized into sections that encompass general provisions, substantive content, and closing provisions. Broadly, the substantive content of the PDP Law addresses key areas such as fundamental principles, categories of personal data, the rights of individuals whose data is processed, data handling procedures, responsibilities of data controllers and processors, data transfers, administrative penalties, institutional roles, international cooperation, community involvement, dispute resolution, procedural legal aspects, prohibitions on unauthorized data usage, and criminal provisions. In the Indonesian context, the implementation of the PDP Law represents a significant stride towards bolstering the security of personal data. It establishes a comprehensive legal framework that not only outlines the rights and obligations of relevant parties but also introduces a stringent mechanism to penalize those who violate the sanctity of personal data (Mardiana &

Meilan, 2023). The various components within the PDP Law, from its fundamental principles to its criminal provisions, collectively contribute to the creation of a robust legal structure that is poised to enhance the protection of personal data and empower government authorities to take more vigorous actions against those who jeopardize the privacy and security of individuals' personal information.

The introduction of regulations concerning the protection of personal data is anticipated to yield a multitude of consequential effects on both the societal and governmental domains. Firstly, these regulations are expected to engender the safeguarding and assurance of the fundamental rights of citizens concerning their personal data, a right intrinsically intertwined with the concept of privacy. Secondly, a pivotal outcome is the heightened consciousness within the public regarding legal and ethical considerations, exemplified by the reverence for the sanctity of an individual's right to privacy. This is one of the overarching expectations stemming from the implementation of personal data protection regulations.

The third salient outcome of these regulatory measures is the harmonious collaboration between government entities, community organizations, and business entities, all operating within the sphere of personal data processing. Within this framework, it is imperative that those involved in processing the personal data of Indonesian citizens assume the responsibility of ensuring the security and confidentiality of such data (Bangsawan, Santoso, Junaidi, Diarti & Mahendra, 2023). Fourthly, an ancillary benefit is the mitigation of potential exploitation by foreign entities concerning the personal data of Indonesian citizens. This vulnerability arises in light of Indonesia's relatively modest technological standing, as underscored by its 75th position in the Global Innovation Index, as reported by the World Intellectual Property Organization (WIPO). Given the dearth of a robust legal framework, the personal data of Indonesian individuals becomes susceptible to external exploitation. Lastly, a fifth consequence is the anticipated proliferation of the technology, information, and communication sector, precipitated by the introduction of these regulations. To fulfill these envisioned objectives and create the requisite conditions, it becomes imperative to devise a legislative framework capable of accommodating these aspirations.

Within the realm of legislating laws and regulations, there exist three foundational pillars that underpin the process of crafting these legal provisions (Zarkasi, 2010). These foundations

encompass the philosophical basis, the juridical basis, and the sociological basis. The philosophical foundation pertains to the rationale and considerations behind the creation of a law, which delineate the philosophical underpinnings of a nation, its moral principles, and its legal ideals. These, in the context of Indonesia, are in accordance with Pancasila and the Constitution (Weley & Disemadi, 2022). Philosophically, the endeavor to establish regulations concerning personal data, safeguarding the privacy rights of every citizen, represents the realization and implementation of the recognition and protection of fundamental human rights. The second tenet of Pancasila, "Just and civilized humanity," serves as the philosophical cornerstone for the regulation of personal data protection. It is premised on the intention that protection will engender justice and foster a society that values and respects the personal data of its individuals (Nurmalasari, 2021).

The considerations articulated within the Personal Data Protection (PDP) Law form the bedrock upon which the law's formulation and ratification are grounded. Some of these considerations include recognizing the protection of personal data as a fundamental human right, ensuring guarantees for citizens' rights to personal data protection as a direct mandate from the Constitution of the Republic of Indonesia, and enhancing the effectiveness of personal data protection implementation (Suharyanti & Sutrisni, 2021). This is achieved by codifying a comprehensive law specifically dedicated to personal data protection. This comprehensive regulation aims to furnish citizens with robust safeguards for their rights, particularly in the realm of personal data protection, and to provide legal certainty to all citizens.

Continuing the discussion on the sociological basis, it is essential to comprehensively understand that the sociological basis involves a thoughtful consideration and rationale that underpins the creation of regulations designed to serve the interests and needs of society. This basis is developed by analyzing empirical data pertaining to societal and governmental challenges. In the context of personal data protection, the sociological basis is derived from the recognition of a pressing need and societal interest in safeguarding individual rights related to the collection, processing, management, and dissemination of personal information (Hisbulloh, 2021). In the Indonesian context, there exists a significant technological, informational, and electronic gap, which has led to a lack of respect for the privacy rights of fellow citizens. This is demonstrated by numerous instances of personal data being illicitly employed in daily life. For instance, according

to a survey conducted by Kompas Research and Development in January 2022, which involved 1,014 respondents across 34 provinces, a substantial portion of individuals exhibited low awareness regarding the security of their digital personal data. Specifically, 67.9% of the respondents had never changed their passwords regularly, 59% had not taken the time to verify the security of applications on their electronic devices, and 36% had only briefly glanced at the terms and conditions related to personal data security within various systems (Saptoyo & Galih, 2022). These statistics underscore a significant deficit in the understanding of and commitment to safeguarding personal data among the Indonesian population. In the realm of practical experiences, one frequently encounters situations where mobile phone users receive Short Message Service (SMS) or calls from unknown numbers offering a wide array of services and products, sometimes from more than ten different sources. These offers range from credit loans, financial services, and product promotions to insurance, and even fraudulent news concerning accidents involving family members.

The fundamental question arises as to how the personal data, particularly one's mobile phone number, is disseminated and acquired by irresponsible parties. This dilemma underscores the absence of legal certainty and the general lack of awareness among the public regarding personal data protection (Thoriq, & Wahyoeono, 2022). Consequently, these circumstances create a substantial opportunity for unscrupulous individuals or entities to breach and misuse personal data. In response to this critical issue, the regulation on Personal Data Protection enshrined in the PDP Law plays a pivotal role in providing protection, guarantees, and legal clarity concerning the privacy rights of Indonesian citizens (Sautunnida, 2018). This legal framework is aligned with the principles outlined in the Pancasila and the Constitution, thereby ensuring that the rights and privacy of Indonesian citizens are upheld and preserved.

The juridical basis, in an academic context, serves as the foundation and rationale for the formulation of legal regulations. It is established to address legal gaps and ongoing legal issues, with the primary goal of ensuring legal certainty and consistency (Sautunnida, 2018). Typically, the juridical basis pertains to both the substantive content and the fundamental principles required for crafting statutory regulations. In the case at hand, Article 28G, paragraph (1) of the 1945 Constitution of the Republic of Indonesia serves as the juridical basis for the creation of the Personal Data Protection (PDP) Law. This provision reads, "everyone has the right to protection

of oneself, family, honor, dignity, and property under their control, and is entitled to a sense of security and protection from the threat of fear to do or not do something that is a human right." This article obligates the establishment of laws and regulations aimed at safeguarding personal data, as a means of realizing the constitutional mandate. This is due to the recognition of the right to privacy as an essential human right crucial for upholding human dignity, and it forms the basis upon which many other human rights are grounded. Additionally, Law Number 39 of 1999 concerning Human Rights is a concrete embodiment of the constitutional mandate, guaranteeing personal rights. Article 3, paragraph (2) of this law affirms that "Everyone has the right to recognition, guarantees, protection, and fair legal treatment and to receive legal certainty and equal treatment before the law," while paragraph (3) states that "Everyone has the right to protection of human rights and basic human freedoms without discrimination."

Furthermore, there exist additional legal provisions governing personal data apart from the 1945 Constitution and Law Number 39 of 1999 concerning Human Rights. These include Law Number 24 of 2013 concerning Amendments to Law Number 23 of 2006 concerning Population Administration, Law Number 36 of 2009 concerning Health, Law Number 11 of 2008 concerning Information and Electronic Transactions, Law Number 14 of 2008 concerning Public Information Disclosure, Law Number 10 of 1998 concerning Banking, and Law Number 8 of 1999 concerning Consumer Protection. These laws collectively constitute the legal framework for the protection of personal data in Indonesia, reflecting the nation's commitment to upholding the rights and dignity of its citizens in the digital age.

CONCLUSION

Regulations pertaining to personal data protection in Indonesia have historically been addressed in various preceding laws, with specific and comprehensive provisions related to personal data protection conspicuously absent in some of these legislations. Consequently, these regulations have remained partial and sectoral in nature, focusing on individual areas. These laws encompass statutes such as Law Number 19 of 2016 on Information and Electronic Transactions, Law Number 39 of 1999 on Human Rights, Law Number 24 of 2013 on Population Administration, and Law Number 10 of 1998 on Banking. Recognizing the need for more specific and robust

safeguards for personal data, in-depth studies have now led to the landmark enactment of Law Number 27 of 2022 on Personal Data Protection on September 21, 2022. This law represents a new era in the management of public personal data, offering legal certainty for personal data security in the digital age. The formation of this personal data protection framework, embodied in Law Number 27 of 2022, rests upon three fundamental pillars: philosophical foundations, juridical foundations, and sociological foundations. Philosophically, it is rooted in the inherent right to privacy, safeguarding the fundamental human rights of every citizen. Sociologically, it addresses the collective need and interest in protecting individual rights regarding personal data collection, processing, management, and dissemination. Juridically, it draws from a range of regulations governing personal data protection, including the 1945 Constitution Article 28G, Law Number 39 of 1999 on Human Rights, Law Number 23 of 2006 on Population Administration, Law Number 36 of 2009 on Health, Law Number 11 of 2008 on Information and Electronic Transactions, Law Number 14 of 2008 on Public Information Disclosure, Law Number 10 of 1998 on Banking, and Law Number 8 of 1999 on Consumer Protection.

ACKNOWLEDGMENTS

We would like to express our sincere gratitude to all parties who have assisted in this research. Especially to the Faculty of Law at Universitas Internasional Batam, for their unwavering support in encouraging students to actively contribute to the realm of knowledge.

REFERENCES

Agustini, P. (2021). Warganet Meningkat, Indonesia Perlu Tingkatkan Nilai Budaya di Internet, https://aptika.kominfo.go.id/2021/09/warganet-meningkat-indonesia-perlu-tingkatkan-nilai-budaya-di-internet/

Bangsawan, M. I., Santoso, B., Junaidi, M., Diarti, D. K., & Mahendra, S. (2023). Personal Data Protection Policy during Covid-19 Pandemic Era. *Law and Justice*, *8*(1), 21-31, https://doi.org/10.23917/laj.v8i1.1558

Bukit, A. N., & Ayunda, R. (2022). Urgensi Pengesahan RUU Perlindungan Data Pribadi Terhadap Perlindungan Kebocoran Data Penerimaan SMS Dana Cepat. *Reformasi Hukum*, *26*(1), 1-20, https://doi.org/10.46257/jrh.v26i1.376

Disemadi, H. S. (2021). Urgensi regulasi khusus dan pemanfaatan artificial intelligence dalam mewujudkan perlindungan data pribadi di Indonesia. *Jurnal Wawasan Yuridika*, *5*(2), 177-199, http://dx.doi.org/10.25072/jwy.v5i2.460

Disemadi, H. S. (2022). Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies. *Journal of Judicial Review*, *24*(2), 289-304, http://dx.doi.org/10.37253/jjr.v24i2.7280

Disemadi, H. S., & Budi, H. S. (2023). Enhancing Trade Secret Protection amidst E-commerce Advancements: Navigating the Cybersecurity Conundrum. *Jurnal Wawasan Yuridika*, *7*(1), 21-45, http://dx.doi.org/10.25072/jwy.v7i1.608

Fikri, M., & Rusdiana, S. (2023). Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Posistif Indonesia. *Ganesha Law Review*, *5*(1), 39-57, https://ejournal2.undiksha.ac.id/index.php/GLR/article/view/2237

Hisbulloh, M. H. (2021). Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi. *Jurnal Hukum*, *37*(2), 119-133, http://dx.doi.org/10.26532/jh.v37i2.16272

Hutauruk, R. H., Sudirman, L., Disemadi, H. S., & Tan, D. (2023). CONVERGENCE OF CONSUMER PROTECTION, INVESTMENT LAW, AND CYBERSECURITY: An in-Depth Analysis of Three-Way Legal Intersections in Investment Apps. *Jurisdictie: Jurnal Hukum dan Syariah*, *14*(1), 127-153, https://doi.org/10.18860/j.v14i1.21180

Jannah, L. M. (2022). *UU Perlindungan Data Pribadi dan Tantangan Implementasinya*, https://fia.ui.ac.id/uu-perlindungan-data-pribadi-dan-tantangan-implementasinya/

Latumahina, R. E. (2014). *Aspek Hukum Perlindungan Data Pribadi di Dunia Maya.* Surabaya: Pelita Harapan University.

Mardiana, N., & Meilan, A. (2023). Urgensi Perlindungan Data Pribadi Dalam Prespektif Hak Asasi Manusia. *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia*, *5*(1), 16-23, https://doi.org/10.52005/rechten.v5i1.108

Megawati, S. (2021). Pengembangan sistem teknologi internet of things yang perlu dikembangkan negara indonesia. *JIEET (Journal of Information Engineering and Educational Technology)*, *5*(1), 19-26, https://doi.org/10.26740/jieet.v5n1.p19-26

Nabila, F. (2022). 11 Daftar Kasus Kebocoran Data di Indonesia, Sebulan Tiga Kali Kejadian!, https://www.suara.com/news/2022/09/02/115017/11-daftar-kasus-kebocoran-data-di-indonesia-sebulan-tiga-kali-kejadian

Natamiharja, R., Sabatira, F., Banjarani, D. R., Davey, O. M., & Setiawan, I. (2022, June). Balancing Two Conflicting Perspectives on Wiretapping Act: Rights to Privacy and Law Enforcement. In *Al-Risalah: Forum Kajian Hukum Dan Sosial Kemasyarakatan* 22(1), 18-30, https://doi.org/10.30631/alrisalah.v22i1.1226

Nurmalasari, N. (2021). Urgensi Pengesahan Rancangan Undang-Undang Perlindungan Data Pribadi Demi Mewujudkan Kepastian Hukum. *Syntax Idea*, *3*(8), 1947-1966, https://doi.org/10.46799/syntax-idea.v3i8.1414

Nursiyono, J. A., & Huda, Q. (2023). Analisis Sentimen Twitter Terhadap Perlindungan Data Pribadi Dengan Pendekatan Machine Learning. *Jurnal Pertahanan & Bela Negara*, *13*(1), 1-16, https://doi.org/10.33172/jpbh.v13i1.1877

Prawiyogi, A. G., & Anwar, A. S. (2023). Perkembangan Internet of Things (IoT) pada Sektor Energi: Sistematik Literatur Review. *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, *1*(2), 187-197, https://doi.org/10.33050/mentari.v1i2.254

Priscyllia, F. (2019). Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum. *Jatiswara*, *34*(3), 239-249, https://www.jatiswara.unram.ac.id/index.php/js/article/view/218

Raimundo, R. J., & Rosário, A. T. (2022). Cybersecurity in the internet of things in industrial management. *Applied Sciences*, *12*(3), 1598, https://www.mdpi.com/2076-3417/12/3/1598

Rosadi, S. D. (2017). Prinsip-Prinsip Perlindungan Data Pribadi Nasabah Kartu Kredit Menurut Ketentuan Nasional Dan Implementasinya. *Sosiohumaniora*, *19*(3), 206-212, https://jurnal.unpad.ac.id/sosiohumaniora/article/view/11380

Saptoyo, R. D. A., & Galih, B. (2022). KABAR DATA: Kesadaran Keamanan Data Pribadi Masyarakat dalam Angka, https://www.kompas.com/cekfakta/read/2022/02/10/090900082/kabar-data-

Sautunnida, L. (2018). Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia. *Kanun Jurnal Ilmu Hukum*, *20*(2), 369-384, https://jurnal.unsyiah.ac.id/kanun/article/view/11159/0

Suharyanti, N. P. N., & Sutrisni, N. K. (2021). Urgensi Perlindungan Data Pribadi Dalam Menjamin Hak Privasi Masyarakat. In *Prosiding Seminar Nasional Fakultas Hukum Universitas Mahasaraswati Denpasar 2020* (Vol. 1, No. 1, pp. 119-134), https://e-journal.unmas.ac.id/index.php/psnfh/article/view/2395

Sutikno, T., & Stiawan, D. (2022). Cyberattacks and data breaches in Indonesia by Bjorka: hacker or data collector?. *Bulletin of Electrical Engineering and Informatics*, *11*(6), 2989-2994, https://doi.org/10.11591/eei.v11i6.4854

Tarantang, J., Awwaliyah, A., Astuti, M., & Munawaroh, M. (2019). Perkembangan sistem pembayaran digital pada era revolusi industri 4.0 di indonesia. *Jurnal al-qardh*, *4*(1), 60-75, https://doi.org/10.23971/jaq.v4i1.1442

Thoriq, Y. A., & Wahyoeono, D. (2022). Perlindungan Hukum Terhadap Pengguna Aplikasi WhatsApp dalam Kewajiban Penyerahan Data Pribadi. *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, *2*(1), 184-205, https://doi.org/10.53363/bureau.v2i1.25

Villa, O., & Tan, D. (2022). Efektivitas Perlindungan Data Diri Konsumen Dalam Bidang Perbankan. *Jurnal Justitia: Jurnal Ilmu Hukum dan Humaniora*, *9*(5), 2441-2452, http://dx.doi.org/10.31604/justitia.v9i5.2441-2452

Weley, N. C., & Disemadi, H. S. (2022). Implikasi Hukum Pemasangan CCTV di Tempat Umum secara Tersembunyi terhadap Perlindungan Data Pribadi. *Amnesti Jurnal Hukum*, *4*(2), 79-93, https://doi.org/10.37729/amnesti.v4i2.2151

Wulansari, E. M. (2020). Konsep Perlindungan Data Pribadi sebagai Aspek Fundamental Norm dalam Perlindungan terhadap Hak atas Privasi Seseorang di Indonesia. *Jurnal Surya Kencana Dua: Dinamika Masalah Hukum dan Keadilan*, *7*, 265-289.

Yuniarti, S. (2019). Perlindungan hukum data pribadi di Indonesia. *Business Economic, Communication, and Social Sciences Journal (BECOSS)*, *1*(1), 147-154, https://doi.org/10.21512/becossjournal.v1i1.6030

Zarkasi, A. (2010). Pembentukan Peraturan Daerah Berdasarkan Peraturan Perundang-Undangan. *INOVATIF| Jurnal Ilmu Hukum*, *2*(4), https://mail.online-journal.unja.ac.id/jimih/article/view/371

Ziqra, Y., Sunarmi, S., Siregar, M., & Leviza, J. (2021). Analisis Hukum General Data Protection Regulation (GDPR) Terhadap Data Pribadi Konsumen Dalam Melakukan Transaksi Online. *Iuris Studia: Jurnal Kajian Hukum*, *2*(2), 330-336, https://doi.org/10.55357/is.v2i2.146