VOL. 4, NO. 2, 2024 (74-85)
JIEE:
Jurnal Ilmiah Ekotrans & Erudisi
EISSN: 2777-0184
PISSN: 2797-2259

Personal Data Protection in Public Services

Elwidarifa Marwenny[1*], Robi Syafwar[2], Puja Yani[3]
[1,2,3] Faculty of Law, Universitas Dharma Andalas, Indonesia
** elwidarifamarwenny@gmail.com*

ARTICLE INFO

Article history:
Received 1 September 2024
Received in revised form 10 October 2024
Accepted 12 December 2024

ABSTRACT

The rapid advancement in technology and infomation has transformed human life paradigms, shifting conventional activities into digital realms through various technological devices. However, alongside technological progress, personal data has become increasingly vulnerable to misuse and privacy violations. The protection of personal data is considered a fundamental human right that must be guaranteed and respected. Although the Personal Data Protection Law has been enacted, its implementation faces various challenges such as data theft, fraud, data selling, and leaks managed by the government for public services. Therefore, this research examines how the government manages the protection and utilization of personal data in public services and the participation of the community in personal data protection. To address these questions, the author employs a qualitative writing method with a normative juridical approach. Law Number 27 of 2022 concerning Personal Data Protection provides a robust legal framework to safeguard individual data and ensure legal certainty for data controllers. Satu Data Indonesia plays a role in integrating data to enhance public service efficiency and ensure data security. However, the implementation and improvement of data protection systems are still necessary. Active participation from the government, data controllers, data owners, law enforcement agencies, as well as digital literacy education and regulatory strengthening, are expected to enhance security and public trust in managing personal data in the digital era.

Keyword:
Personal Data, Data Protection, Public Services.

INTRODUCTION

The swift progression of technological innovation and information dissemination has exerted a profoundly significant influence on diverse dimensions of human existence, transforming traditional human activities into digital formats through an array of rapidly evolving technological instruments, with most societal interactions now conducted via digital platforms (Al Ghani, 2022; Aseeva, 2024; Rosmani et al., 2020). The ramifications of adopting digital-based operational methodologies are evident in the functionality of data management systems across both governmental and private sectors, wherein many activities are

[1] *elwidarifamarwenny@gmail.com*

executed digitally. Data or information acquired through electronic mediums, particularly concerning the Indonesian population and demographic statistics, such as family cards, population registration numbers, and identity cards, possess exceedingly high intrinsic value (Fathiyana et al., 2022; Hendri, 2023; Hisbulloh, 2021).

As these innovations unfold, personal data has become one of the most vital and sensitive elements due to the rise in digital engagements. The scope of personal information covers numerous categories: names, residential addresses, identification digits, financial records, medical backgrounds, and additional confidential details connected to individuals (Chua et al., 2021; Sudarwanto & Kharisma, 2022). In the context of the swift evolution of the digital age, individual personal data is increasingly susceptible to potential exploitation and privacy breaches. Safeguarding personal data is regarded as a fundamental human right that necessitates assurance and reverence (Suari & Sarjana, 2023). Personal data constitutes specific information about individuals that is systematically stored, managed, and preserved, emphasizing its accuracy and ensuring its confidentiality is upheld (Fuster, 2010; Panebianco, 2022; Rianarizkiwati, 2022).

Data protection denotes that individuals have the autonomy to make determinations regarding sharing or exchanging their personal information. Also, people maintain the option to set the parameters regarding the transfer of their data. Besides, ensuring data security is fundamentally linked to understanding privacy rights (Grech & Agius-Muscat, 2018; Lynskey, 2014). The right to privacy has undergone significant evolution, thereby facilitating the establishment of the right to safeguard personal data (Mulia et al., 2022; Neisse et al., 2014; Stanzione, 2020). Given that every citizen's engagement within the digital domain is invariably associated with personal data, the effective utilization of this information necessitates the presence of robust and accountable governance. This underscores the imperative for comprehensive, stringent, and resolute regulatory frameworks (Ketmaneechairat et al., 2024; Subiakto, 2021).

Consequently, the government undertook measures to implement the Personal Data Protection Law (UU PDP). This regulation is acknowledged as establishing the essential legal framework for safeguarding personal data. This regulation was formulated in response to apprehensions regarding the rising occurrences of personal data breaches within Indonesia, which can potentially adversely impact legal entities and individuals (Januarita et al., 2024; Natamiharja & Setiawan, 2024; Rohmansyah et al., 2023).

Conversely, despite the enactment of the Personal Data Protection Law, the operationalization of the PDP Law is anticipated to encounter multiple obstacles. Personal data theft, fraud, illicit data transactions, and data breaches represent criminal activities that persistently proliferate in tandem with advancements in technology and information systems. In 2019, the Jakarta Legal Aid Institute (LBH) documented an excess of five thousand grievances about the improper utilization of personal data. The PLN, or State Electricity Company, experienced a security incident that compromised the data of 17 million clients, revealing private details, including names, addresses, and billing information. Indihome, a provider of internet services, similarly experienced a data leak affecting 26 million user accounts, compromising information including browsing history, names, email addresses, and population registration numbers; additionally, the Peduli Lindungi application faced a breach

of approximately 3.2 billion user data records that were subsequently sold on the dark web. Data breaches were also reported by the KPU in May 2020, involving 2.3 million records, and BPJS Kesehatan, which reported a staggering 297 million records in May 2021; furthermore, breaches were noted on governmental platforms, including prakerja.go.id (17,331 credentials), datadik.kemdikbud.go.id (15,729 credentials), info.gtk.kemdikbud.go.id (10,761 credentials), and djponline.pajak.go.id (10,409 credentials).

This data breach revelation illustrates that the information overseen by governmental entities is susceptible to unauthorized disclosures. The governing body manages a hefty volume of personal details related to its citizens to fulfill the obligations of public offerings. The methodology employed for data collection is frequently executed through various means, including coercion and voluntary participation. The populace supplies certain identity-related information, such as population registration numbers and family card identifiers, under duress from governmental regulations. Conversely, some information is provided voluntarily, particularly in the context of individuals applying for positions as state civil servants. Within this framework, a critical dimension that warrants emphasis and scrutiny is the preservation of the security of the amassed data and the protocols governing its utilization. It is imperative to prevent the information encapsulated within the data from being commodified and exploited in an unethical manner. Furthermore, individuals have a discernible tendency to disseminate personal information readily; thus, initiatives are essential to cultivate a collective awareness among the public regarding the significance of safeguarding personal data (Saputra et al., 2023; Yolanda & Hutabarat, 2023).

RESEARCH METHODS

In the present investigation, the researcher employs a qualitative methodology in conjunction with a normative jurisprudential framework to address the inquiries that have been delineated (Atikah, 2022). This methodological approach encompasses a comprehensive literature review to identify concepts, perspectives, or interpretations pertinent to the issue under examination. Moreover, legal procedures are analyzed based on the articulated material, alongside statutes collated through a literature review, which are evaluated and critiqued.

RESULTS AND DISCUSSION

Protection and utilization of personal data managed by the government in public services

The swift progression of technology and information systems has conferred numerous advantages upon diverse demographic groups across various sectors. Nonetheless, in certain instances, criminal activities frequently outpace the measures implemented by the community, including law enforcement agencies, in the context of formal and material legal frameworks. The expanding demographic of users leveraging technology and information devices has highlighted the necessity for protecting personal data, particularly amid frequent data breaches that have led to fraudulent schemes and other illegal actions. The safeguarding of personal data is fundamentally intertwined with the right to privacy, which encompasses the right of individuals to dictate the use and accessibility of their personal information. This principle empowers individuals to establish the conditions under which their data could be shared or relocated (Abouahmed et al., 2024; Guo et al., 2024; Saria et al., 2024). In Law Number 27 of 2022, specifically

Article 1, numeral 1, personal data is described as details about an individual that can be recognized independently or alongside additional information, whether through digital or traditional channels. Also, Article 4 of the PDP Law breaks down personal data into two major types: Specific Personal Data, covering health-related information; biometric details; genetic data; criminal records; data associated with minors; personal identification data; and/or further details as specified by relevant laws and regulations, and General Personal Data, which contains full names; gender; nationality; religion; marital status; and/or personal data combined to identify a specific individual. The government is responsible for preserving the confidentiality of citizens' data and preventing its potential misuse. Data is classified as personal if it directly correlates to an individual, thereby enabling the identification of its possessor. Moreover, personal data involves all kinds of details about individuals that are kept via electronic means or traditional methods, whether they are clearly named or can be recognized, either separately or along with other data, in direct or indirect forms (Kretschmer et al., 2018).

If one observes meticulously, nearly every annum yields many concerning incidents of data breaches. For instance, in August 2021, there was a substantial compromise of user data associated with the Ministry of Health's e-HAC3, encompassing approximately 1.3 million records, with a total volume nearing 2 GB. In September 2021, there emerged a breach involving the population registration numbers (NIK) of candidates for the presidential and vice-presidential positions during the 2019 electoral process, which were subsequently disseminated across the digital landscape; furthermore, there were claims of considerable data breaches originating from prominent applications within Indonesia (Kautsar, 2022). There were also allegations concerning the unauthorized exposure of approximately 44.237 million personal records managed by the MyPertamina application, which operates under the aegis of PT Pertamina. The myriad issues surrounding personal data breaches in public domains should serve as a crucial instructive moment for each public agency or institution tasked with the delivery of public services, as this scenario engenders profound inquiries regarding the preparedness of public agencies or institutions, at both the central and regional government echelons, in safeguarding personal data.

A significant tenet in the domain of personal data handling, as articulated in the Personal Data Protection (PDP) Law, revolves around the principle of integrity and confidentiality, which is realized through the duty to uphold security during data processing, shield the confidentiality of information, and communicate notifications when a data breach takes place. Each data controller or processor is mandated to implement requisite technical and organizational measures to guarantee a robust level of security in the administration of personal data under their stewardship. These approaches involve obscuring data, swapping actual identities for fictional ones, securing data through encryption, ensuring the protection of data processing frameworks and services, upholding the confidentiality, integrity, accessibility, and durability of data; reinstating data access and availability in cases of loss; and conducting tests, assessments, and evaluations to determine the success of security initiatives in data processing. This indicates that such actions constitute integral components of security measures and risk management strategies in safeguarding personal data. By sticking to these rules, personal details can be safely guarded against numerous

threats, including unauthorized entry, data compromises, and online invasions.

The PDP Law asserts that at least four stakeholders are engaged in initiatives to safeguard personal data. To begin with, Personal Data Processors are characterized as entities encompassing individuals, governmental organizations, and global institutions involved in handling personal data, either independently or in partnership, representing the Personal Data Controller. Secondly, Personal Data Controllers are identified as entities that assume a significant role in establishing the objectives and governance of personal data processing, whether independently or in conjunction with others. Thirdly, Personal Data Subjects are recognized as individuals whose personal data is pertinent to them. As a fourth point, the Indonesian Government, guided by its central authority headed by the President, operates per the regulations detailed in the 1945 Constitution of Indonesia. The governmental entity is responsible for ensuring personal data protection measures are enacted in compliance with prevailing legislation. Through the engagement of these four stakeholders, personal data will be systematically collected by each relevant party. Consequently, each stakeholder must comprehend and acknowledge their distinct roles and obligations, given the critical significance of personal data protection that necessitates collective recognition and implementation.

Furthermore, the collaborative regulatory framework concerning safeguarding personal data underscores the significance of preventive strategies. It incorporates a diverse array of non-governmental stakeholders in executing these initiatives (Lorè, 2020; Zhengyu, 2021). Trade associations possess the capability to formulate collective regulations aimed at governing the management of personal data within specific sectors, including pertinent technical standards, and to actualize these regulations via a Joint enforcement mechanism, wherein the government retains the accountability for the supervisory role to ensure that the initiatives undertaken by these associations are executed equitably and align with the principles of competitive market dynamics. The strategy of empowering Data Protection Officers (DPOs) has been validated in various nations as an effective means to establish professional community benchmarks for exemplary practices in personal data protection. The function of Data Protection Officers (DPOs) is defined in articles 53 and 54 of the Personal Data Protection (PDP) Law. Article 53 of the PDP Law delineates that personal data controllers and processors must designate an official or officer tasked with executing personal data protection (PDP) responsibilities. This responsibility pertains to the handling of personal data for public service. Moreover, personal data controllers whose primary operations involve the extensive and continuous collection, utilization, and management of personal data must ensure consistent and systematic oversight.

Leading up to establishing the Personal Data Protection (PDP) Law, Indonesia's Personal Data Protection was overseen by a complex web of policies. At least 32 regulatory frameworks were disseminated across various sectors, including finance, health, demographics, telecommunications, banking, commerce, and additional domains, while public service entities adhered to distinct standards and references about personal data protection. It is imperative to note that the government requires access to individuals' data to execute governmental functions effectively, a necessity that diverges from the private sector's utilization of data primarily for economic advantages; the government's use of data is

aimed at enhancing public administration and fostering transparent and accountable policy-making. Nonetheless, the obstacles encountered include the heterogeneity of data across governmental departments and institutions, which may impede effective decision-making processes and exacerbate administrative burdens.

One Data Indonesia assumes a pivotal function in Personal Data Protection by fostering the establishment of an integrated, contemporary, and readily shareable data repository to address the complexities inherent in data governance. Presidential Regulation Number 39 of 2019 pertains to One Data Indonesia. It delineates the protocols for administering governmental data, ensuring high-quality data is readily accessible and sharable between national and regional agencies. In contrast, Law Number 27 of 2022 regarding Personal Data Protection seeks to safeguard individual personal data while offering legal certainty to data controllers concerning using personal data for public policy and public service objectives. One Data Indonesia's significance as a data exchange platform is paramount in this framework. It necessitates adherence to the stipulations of the PDP Law, which underscores the critical nature of robust personal data protection within public service contexts. This includes processing personal data by the SDI policy aimed at integrating data from diverse sources to enhance the efficiency and efficacy of information interchange among governmental entities while concurrently ensuring the security and integrity of public services.

The PDP Law and its associated regulations facilitate effective governance and enhance public confidence in data management. The appropriate execution of the PDP Law can guarantee the integrity and accessibility of data within public services, aligning with global standards. The passage of Law Number 27 in 2022 addressing Personal Data Protection reaffirms the Indonesian government's promise to safeguard its citizens' private information. This legislation is designed as a proactive measure against potential offenses and lapses in data management that may lead to breaches and as an initiative to cultivate public confidence in governmental entities and corporations. The significance of data governance and processing enshrined in this law underscores the necessity for data management to be limited, legal, and transparent, thereby ensuring data security while concurrently upholding the rights of data subjects, such as the rights to delete or amend their personal information. It follows that Law Number 27 of 2022 related to Personal Data Protection holds a significant aim, covering not only the defense of personal information but also the formation of a bedrock of public assurance in the agencies managing data.

The safeguarding of personal data within the digital age encounters numerous significant obstacles. Firstly, the proliferation of internet users coupled with the utilization of personal data, particularly within the public sector, has culminated in an increased volume of data that necessitates diligent management and protection. Secondly, technological advancements facilitate extensive and automated data collection, exacerbating the potential for data misuse and breaches. Thirdly, the rising incidence of data breaches, along with novel complexities in oversight, necessitates the implementation of more stringent and efficacious security protocols. Fourthly, the coexistence of overlapping regulations governing personal data protection can engender confusion in their application. Fifthly, disparities in standards and practices for personal data protection among various institutions, including in managing third parties, may impede the coherence and efficacy of data protection strategies. Lastly, the

inadequate and inconsistent public awareness concerning the significance of personal data protection presents a substantial challenge in ensuring compliance and enhancing the execution of data protection policies.

This situation underscores the critical necessity of meticulously enhancing data security measures, which will, in turn, augment operational efficiency and foster public confidence. Measures that must be undertaken to bolster public confidence in data security within the framework of digital transformation in the public sector encompass the enhancement of regulatory frameworks and policies; consequently, the government is compelled to promptly ratify and finalize a series of derivative regulations stemming from the Personal Data Protection (PDP) Law. The regulations mentioned earlier consist of ten governmental rules that act as measures for the protection of personal data within Indonesia, outlined in Articles 10 (paragraph 2), 12 (paragraph 2), 13 (paragraph 3), 16 (paragraph 3), 34 (paragraph 3), 48 (paragraph 5), 54 (paragraph 3), 56 (paragraph 5), 57 (paragraph 5), and 61. Moreover, it is vital to acknowledge that a dedicated independent entity has not been created as per the directives of Article 58 of the PDP Law to manage the enforcement of personal data protection; therefore, enhancing network security should take precedence through the evolution of technologies like firewalls, intrusion detection and prevention systems, and real-time network monitoring features. The government must also consistently disseminate security reports to demonstrate its commitment to transparency. Additionally, it is essential to comprehensively elevate digital literacy education for the public regarding the significance of personal data protection while concurrently reinforcing the resources available to the government.

Public participation in personal data protection

The evolution of information technology, particularly within the domains of computing and the internet, has exerted a profoundly beneficial influence on human existence (Saputra et al., 2024). It enhances societal welfare and cultural development and serves as a conduit for illicit activities. A prominent risk associated with this technological advancement is the emergence of criminal behavior, particularly concerning safeguarding personal data that necessitates stringent protection. Concurrent with the proliferation of information technology, there exists a requisite for heightened public consciousness regarding the criticality of personal data protection. A study by the Directorate General of Applications and Informatics (Aptika) in July 2021, encompassing 11,305 participants, indicated that while the public acknowledges the significance of safeguarding personal data, their proactive measures in securing their information remain suboptimal.

> *"As many as 87.8% of participants acknowledged their comprehension of the privacy policy during the application installation process; however, they demonstrated a lesser degree of selectivity in regulating access to devices and applications that may facilitate data expropriation. Although the general public's awareness regarding personal data is relatively commendable, with nearly all respondents recognizing the significance of personal data, the mean score about the comprehension of specific facets of personal data indicates that there remains substantial potential for enhancement (6.70 out of 10 for general understanding, and 5.26 out of 10 for particular comprehension). The inappropriate utilization of personal data remains prevalent*

across Indonesia, notwithstanding the heightened awareness concerning the necessity of safeguarding such information. The extent of public worry concerning personal data privacy is still alarmingly poor, as illustrated by the data that reveals a substantial share of Facebook users (55.5%) and Instagram users (25.5%) fail to customize the privacy features of their social media accounts. While public perception of personal data confidentiality is regarded as relatively satisfactory, with a mean score of 6.05 out of 10 for Indonesia's data protection framework, there is a pressing necessity for advancements in both the system and the execution of personal data protection legislation."

This survey demonstrates a substantial level of awareness regarding the significance of personal data protection; however, obstacles persist in motivating the public to undertake definitive measures to safeguard their personal information, alongside the necessity for enhancing the current protection framework in Indonesia. To bolster personal data protection, engagement from diverse stakeholders, encompassing the private and public sectors, is imperative. The level of public involvement in ensuring the security of their data can be augmented by emphasizing the principles of caution, selectivity, and prudence in their interactions with digital technology. By employing this methodology, each individual can actively defend their personal information against digital threats. The proactive involvement of various societal segments, manifested through preventive and punitive measures, will markedly enhance Indonesia's digital ecosystem's security.

The state bears a fundamental duty to safeguard the personal data of its citizens; however, this responsibility cannot be executed in isolation. Consequently, the involvement of all stakeholders is crucial in achieving adequate personal data protection. The administration functions as a controlling organization with two essential missions: first, to construct a legal basis that defends personal data as a crucial right to privacy, and second, to regulate and uphold the necessary guidelines. The successful execution of these two functions is imperative for effectively implementing personal data protection measures. Data Controllers and Processors also hold significant accountability in upholding data security. They must adeptly navigate various challenges and implement risk mitigation strategies to avert data breaches. By BSSN Regulation No. 8 of 2020, they are mandated to conduct security certification corresponding to the risk level present.

In addition, Data Owners assume a pivotal role in safeguarding their privacy. While interfacing with numerous digital instruments and services, it becomes vital for users to grasp the moral considerations and laws that oversee their usage and recognize the limitations related to the spread of personal information to lower the chances of misuse. Despite the efforts executed by regulatory bodies and other stakeholders, the necessity for individual cognizance in preserving privacy remains a significant facet of data protection. Ultimately, law enforcement officers, including police, judges, prosecutors, and the National Cyber and Crypto Agency (BSSN), bear the obligation to ensure the effective enforcement of laws about personal data protection. Robust collaboration among law enforcement personnel serves as the fundamental mechanism in the rigorous enforcement of regulations and the adept management of data breaches. Through the concerted efforts of all stakeholders, personal data

protection can be executed more optimally and comprehensively.

In striving to fulfill the Personal Data Protection (PDP) Law, it is essential to understand that Personal Data Controllers ought to nurture a workplace culture that emphasizes the importance of privacy, develop the expertise of staff within organizations focused on personal data protection, create solid technological infrastructures for ensuring data security; and take the initiative in tackling potential dangers linked to violations of personal data protection. In addition, it is vital for Personal Data Subjects to grasp their rights entirely to avoid the reckless distribution of personal information and, crucially, to thoroughly read and assess the provisions and privacy statements linked to the Personal Data Protection Law, which acts as a key structure protecting the public's right to safeguard their data. By enacting this legislation, the government bears the obligation to uphold the security of citizens' data. A multitude of provisions within the PDP Law delineates directives for both the government and the populace regarding safeguarding personal data. For instance, Article 7 of the PDP Law affirms the prerogative of every individual to seek the safeguarding of their data. In contrast, Article 12 mandates the government to institute an adequate data protection mechanism and avert misuse.

The Personal Data Protection Law (PDP Law) additionally governs the public's engagement in safeguarding personal data. Article 63 of the PDP Law delineates that the public may engage either directly or indirectly to bolster initiatives to protect personal data. Paragraph (1) of Article 63 articulates that the public is entitled to participate directly or indirectly to facilitate the execution of personal data protection measures. Conversely, Paragraph (2) prescribes that such public engagement may be conducted via educational endeavors, training programs, advocacy initiatives, socialization efforts, and/or oversight activities by prevailing legal standards. The enactment of the PDP Law aspires to enhance public cognizance regarding the significance of personal data protection. The obligation to safeguard personal data rests with governmental entities and corporations. At the same time, the active involvement of all stakeholders is imperative for ensuring the integrity of personal data within the contemporary digital landscape.

CONCLUSION

Safeguarding personal data in Indonesia has become increasingly paramount due to the rising population of internet users and the proliferation of data breach incidents. The enactment of Law Number 27 of 2022 about Personal Data Protection establishes a comprehensive legal framework designed to safeguard individual data while concurrently providing legal certainty for data controllers. The initiative known as One Data Indonesia serves a pivotal function in consolidating data from diverse sources, enhancing the efficiency of public services while concurrently ensuring data security. The challenges associated with data protection encompass the escalation of internet users, advancements in technology, incidents of data breaches, ambiguities in regulatory frameworks, and a general lack of public awareness. Tactics to resolve these complications entail fortifying regulatory systems, establishing an independent monitoring agency, augmenting network security frameworks, and advocating for digital literacy movements. It is anticipated that enacting the PDP Law and its associated policies will bolster public confidence in the governance of personal data.

Advancements in information technology exacerbate the vulnerability to criminal activities within personal data management. A Director General of Aptika

study in July 2021 indicated that while public awareness is notably elevated, the protective measures remain suboptimal. Law Number 27 of 2022 establishes a robust legal framework; however, there is a pressing need to implement and enhance the data protection system. It is anticipated that proactive engagement from governmental entities, data controllers, data proprietors, and law enforcement officials, in conjunction with initiatives aimed at promoting digital literacy and fortifying regulations, will improve security and augment public confidence in personal data management amidst the digital age.

REFERENCES

Abouahmed, A., Kandeel, M. E., & Zakaria, A. (2024). PERSONAL DATA PROTECTION IN THE UNITED ARAB EMIRATES AND THE EUROPEAN UNION REGULATIONS. *Journal of Governance and Regulation*, *13*(1), 195–202. https://doi.org/10.22495/jgrv13i1art17

Al Ghani, M. F. (2022). Urgensi Pengaturan Perlindungan Data Pribadi Pada Penyelenggaraan Layanan Pinjaman Online. *The Digest: Journal of Jurisprudence and Legisprudence*, *3*(1), 38–58.

Aseeva, I. A. (2024). The Crooked Mirror of Digitalization. *Voprosy Filosofii*, *2024*(2), 25–33. https://doi.org/10.21146/0042-8744-2024-2-25-33

Atikah, I. (2022). *Metode Penelitian Hukum*.

Chua, H. N., Ooi, J. S., & Herbland, A. (2021). The effects of different personal data categories on information privacy concern and disclosure. *Computers and Security*, *110*. https://doi.org/10.1016/j.cose.2021.102453

Fathiyana, R. Z., Yutia, S. N., & Hidayat, D. J. (2022). Prototype of Integrated National Identity Storage Security System in Indonesia using Blockchain Technology. *International Journal on Informatics Visualization*, *6*(1), 109–116. https://doi.org/10.30630/joiv.6.1.877

Fuster, G. G. (2010). Inaccuracy as a privacy-enhancing tool. *Ethics and Information Technology*, *12*(1), 87–95. https://doi.org/10.1007/s10676-009-9212-z

Grech, V., & Agius-Muscat, H. (2018). WASP (Write a Scientific Paper): Data protection, a guide for health researchers. *Early Human Development*, *124*, 44–45. https://doi.org/10.1016/j.earlhumdev.2018.04.021

Guo, Z., Hao, J., & Kennedy, L. (2024). Protection path of personal data and privacy in China: Moving from monism to dualism in civil law and then in criminal law. *Computer Law and Security Review*, *52*. https://doi.org/10.1016/j.clsr.2023.105928

Hendri, H. (2023). A Novel Algorithm for Monitoring Field Data Collection Officers of Indonesia's Central Statistics Agency (BPS) Using Web-Based Digital Technology. *International Journal on Advanced Science, Engineering and Information Technology*, *13*(3), 1154–1162. https://doi.org/10.18517/ijaseit.13.3.18302

Hisbulloh, M. H. (2021). Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi. *Jurnal Hukum*, *37*(2), 119–133.

Januarita, R., Alamsyah, I. F., & Perdana, A. (2024). Guardians of data: TruMe Life's continuous quest for data protection. *Journal of Information Technology Teaching Cases*. https://doi.org/10.1177/20438869241242141

Kautsar, T. R. (2022). *Kajian Literatur Terstruktur Terhadap Kebocoran Data Pribadi dan Regulasi Perlindungan Data Pribadi*. UIN Ar-Raniry.

Ketmaneechairat, H., Maliyaem, M., & Puttawattanakul, P. (2024). Towards a Management System Framework for the Integration of Personal Data Protection and Data Governance: A Case Study of Thai Laws and Practices. *International Journal of Technology*, *15*(1), 219–229. https://doi.org/10.14716/ijtech.v15i

1.5885

Kretschmer, T., Wiewiorra, L., Krämer, J., Oehler, A., Horn, M., Haucap, J., Klein, S., & Hüllmann, J. (2018). Data capitalism-an economic approach. *Wirtschaftsdienst*, *98*(7), 459–480. https://doi.org/10.1007/s10273-018-2318-3

Lorè, F. (2020). Risk-based analysis in the handling of sensitive data in the health sector. *Giornale Italiano Di Nefrologia : Organo Ufficiale Della Societa Italiana Di Nefrologia*, *37*(3).

Lynskey, O. (2014). Deconstructing data protection: The "added-value" of a right to data protection in the eu legal order. *International and Comparative Law Quarterly*, *63*(3), 569–597. https://doi.org/10.1017/S0020589314000244

Mulia, R. A., Saputra, N., Syamsir, S., & Embi, M. A. (2022). Literature Evaluation on Optimizing Supervisory Functions in Improving the Performance of Regional Government Bureaucracy. *Adabi: Journal of Public Administration and Business*, *9*(2), 12–24.

Natamiharja, R., & Setiawan, I. (2024). Guarding Privacy in the Digital Age: A Comparative Analysis of Data Protection Strategies in Indonesia and France. *Jambe Law Journal*, *7*(1), 233–251. https://doi.org/10.22437/home.v7i1.349

Neisse, R., Steri, G., & Baldini, G. (2014). Enforcement of security policy rules for the internet of things. *International Conference on Wireless and Mobile Computing, Networking and Communications*, 165–172. https://doi.org/10.1109/WiMOB.2014.6962166

Panebianco, M. D. (2022). Confidentiality: legal declinations and operational effects. *Federalismi.It*, *2022*(16), 114–150.

Rianarizkiwati, N. (2022). Ius Constituendum Hak Atas Pelindungan Data Pribadi: Suatu Perspektif Hak Asasi Manusia. *Jurnal Hukum Sasana*, *8*(2), 324–341.

Rohmansyah, D. A., Saputra, K. M., & Sholih, B. (2023). Urgensi Perlindungan Hak Asasi Anak Atas Data Pribadi di Era Digitilasasi Berdasarkan Prinsip Negara Hukum. *AL-MANHAJ: Jurnal Hukum Dan Pranata Sosial Islam*, *5*(2), 1099–1110.

Rosmani, A. F., Mutalib, A. A., & Sarif, S. M. (2020). The evolution of information dissemination, communication media and technology in Malaysia. *Journal of Physics: Conference Series*, *1529*(2). https://doi.org/10.1088/1742-6596/1529/2/022044

Saputra, N., Putera, R. E., Zetra, A., Azwar, Valentina, T. R., & Mulia, R. A. (2024). Capacity building for organizational performance: a systematic review, conceptual framework, and future research directions. *Cogent Business & Management*, *11*(1), 2434966.

Saputra, N., Syamsir, S., Embi, M. A., & Mulia, R. A. (2023). Community Participation in Tourism Development at the Macaronis Tourism Attraction, Silabu Beach, Mentawai Islands. *Adabi: Journal of Public Administration and Business*, *10*(1), 12–23.

Saria, S. P., Wahyuni, S., & Marwenny, E. (2024). Penegakan Hukum Tindak Pidana Prosttusi Online Terhadap Pekerja Seks Komersial (PSK) Di Wilayah Hukum Polresta Padang. *Jurnal Kajian Hukum Dan Kebijakan Publik| E-ISSN: 3031-8882*, *1*(2), 238–242.

Stanzione, P. (2020). Data Protection and vulnerability. *European Journal of Privacy Law and Technologies*, *2020*(2), 9–14.

Suari, K. R. A., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132–142.

Subiakto, H. (2021). Perlindungan Data Pribadi dan Tantangannya. *Bappeda. Kaltimprov. Go. Id*.

Sudarwanto, A. S., & Kharisma, D. B. B. (2022). Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia. *Journal of Financial Crime*, *29*(4), 1443–1457. https://doi.org/10.1108/JFC-09-2021-0193

Yolanda, E., & Hutabarat, R. R. (2023). URGENSI LEMBAGA PELINDUNGAN DATA PRIBADI DI INDONESIA

BERDASARKAN ASAS HUKUM RESPONSIF. *Journal of Syntax Literate*, *8*(6).

Zhengyu, S. (2021). A Comparative Analysis of the Regulatory Approaches to Personal Data between the EU and the US. *Contemporary Social Sciences*, *6*(4), 87–105. https://doi.org/10.19873/j.cnki.2096-0212.2021.04.007