Jurnal Ilmiah Administrasi Pemerintahan Daerah (JIAPD)
Vol. 18, No. 1 (2026) pp. 11-20
e-ISSN: 2615-3351
p-ISSN: 1829-5193
url: https://ejournal.ipdn.ac.id/JAPD/index
DOI: 10.33701/jiapd.v18i1.5561

Implementation of Law Number 27 of 2022 concerning Personal Data Protection (PDP) at the Communication and Information Service in Majalengka Regency

Andi Masrich *
Institut Pemerintahan Dalam Negeri
Triyanto
Institut Pemerintahan Dalam Negeri
Edy Supriyono
Institut Pemerintahan Dalam Negeri

*Correspondence: triyanto@ipdn.ac.id

ARTICLE INFO

Article History:
received: 2025-09-16
revised: 2026-06-16
accepted: 2026-06-17

Keywords:
Policy Implementation, Digital Technology , Data Protection , Personal Data

DOI:10.33701/jiapd.v18i1.5561

ABSTRACT

This study discusses the Implementation of Law No. 27 of 2022 concerning Personal Data Protection at the Communication and Informatics Service in Majalengka Regency. The phenomenon that occurs with digitalization is very vulnerable regarding personal data protection because it is vulnerable to leaks, misuse, and cyber attacks . The main objective of this study is to analyze, identify obstacles or challenges and formulate strategies for the Implementation of Law No. 27 of 2022. The research method used is a descriptive research method with a qualitative approach. The results of this study indicate that the implementation of the Personal Data Protection Law at the Majalengka Regency Communications and Information Office is still in the regulatory and infrastructure strengthening stage. Despite the existence of supporting regional policies, implementation still faces challenges in terms of regulatory understanding, human resources (HR), and information technology readiness to securely manage personal data. Government employees' awareness and understanding of personal data protection still needs to be improved. Interviews and observations indicate that many employees still do not fully understand their rights and obligations regarding personal data management, which can increase the risk of data breaches or leaks. However, implementation has shown significant progress in increasing the efficiency and transparency of public services. However, challenges in infrastructure, human resources, and data security still need to be seriously addressed. Further efforts are needed to strengthen service integration and improve public digital literacy to optimally achieve these goals.

INTRODUCTION

The rapid development of information technology has brought significant benefits to various sectors, including government, business, and social life. However, along with digitalization, new challenges arise regarding personal data protection. Unprotected personal data is vulnerable to leaks,

misuse, and cyberattacks, which can threaten individual privacy and national security (Solove, 2021) . The massive and rapid implementation of digitalization has changed the way individuals and organizations manage personal data. The collection, storage, and processing of personal data are now commonplace in various sectors, from banking and healthcare to education and online services. However, the rise in data leaks and misuse of personal information raises concerns about the protection of citizens' privacy rights.

In response, Indonesia passed Law No. 27 of 2022 concerning Personal Data Protection (PDP Law). This law marks a significant milestone in establishing the rights of data subjects and the obligations of data controllers. However, implementation on the ground still faces various challenges, such as minimal institutional preparedness, lack of public awareness, and weak law enforcement.

Therefore, this study aims to analyze the effectiveness of the implementation of the Personal Data Protection Law and provide policy recommendations to strengthen personal data protection in Indonesia. The past two decades have transformed nearly every aspect of human life, from communications and financial transactions to healthcare and government administration. In this digital ecosystem, personal data has become a vital commodity collected, analyzed, and traded by various parties. However, as dependence on digital technology increases, threats to the right to privacy also increase.

Indonesia has experienced a number of alleged large-scale data breaches in recent years. Some prominent cases include the alleged leak of the Ministry of Health's e-HAC data. alleged leak of KPU voter data The exposure of millions of customer data from e-commerce platforms demonstrates Indonesia's weak security infrastructure and personal data protection systems. This underscores the need for comprehensive regulations and robust legal protection mechanisms.

In response to this situation, the government passed Law No. 27 of 2022 concerning Personal Data Protection (PDP Law). This law is expected to serve as the primary legal basis for guaranteeing individuals' rights over their personal data, establishing obligations for data controllers and processors, and establishing an independent supervisory authority. Thus, data management is no longer solely based on operational needs, but must adhere to principles that protect data subjects. Furthermore, the enactment of this law also emphasizes that personal data—such as identity numbers, addresses, health data, and biometric information—has value that must be protected due to its potential impacts on privacy, security, and misuse.

However, the challenges in implementing this law are significant. Many parties, both users and data managers, still do not understand the substance and obligations stipulated. For example, in the practice of collecting public service data, there are still unclear consent forms or consent forms that do not explain the processing purposes in detail. Furthermore, some agencies or business actors have not fully prepared data security mechanisms, such as access control, encryption, logging, and incident response procedures in the event of a data breach. Another challenge is ensuring that data processing is carried out according to purpose limitations and minimizing the collection of irrelevant data. Institutionally, the supervisory authority promised in the law has not yet been fully established, so the process of monitoring, enforcement, and compliance standards can still face limited coordination.

This research is crucial for assessing the extent to which the Personal Data Protection Law has been implemented in practice, the public's and institutions' understanding of personal data protection, and identifying existing barriers to the policy's implementation. This study can explore, for example, the extent to which agencies apply the principle of transparency in providing information to data subjects, how the mechanism for requesting access or deletion of data is implemented, and the extent to which controllers and processors understand their roles and responsibilities. Furthermore, the research is expected to identify factors such as the availability of human resources, budget support, the readiness

of information technology systems, and the level of maturity of data governance within the organization. With this mapping, this study is expected to contribute to policy refinement, increase public awareness, and encourage the establishment of safer and fairer data governance in Indonesia.

In an effort to improve personal data protection, the Indonesian government passed Law No. 27 of 2022 concerning Personal Data Protection (PDP Law). This law provides a legal basis for managing personal data, regulating the rights of data subjects, the obligations of data controllers and processors, and sanctions for violators. Key principles of the PDP Law include legality, transparency, clear objectives, and adequate data security (Law No. 27 of 2022, Article 3). The application of the legality principle, for example, requires that data processing only be carried out on a valid legal basis, such as for the fulfillment of government duties or based on conscious and specific consent. Meanwhile, the transparency principle can be realized through easy-to-understand notifications regarding data use, retention periods, and data subjects' rights.

The Majalengka Regency Communications and Informatics Office plays a strategic role in the implementation of the Personal Data Protection Law at the regional level. As the agency that manages government information and communication systems, is responsible for ensuring that personal data managed by local government agencies is properly safeguarded in accordance with data protection principles. In this context, can act as a data governance facilitator, for example through the development of technical guidelines, fostering the implementation of information security standards, and strengthening procedures for managing access to public service systems. Furthermore, Communication and Information Technology Office also plays a role in the dissemination and supervision of other agencies in the implementation of personal data protection policies, including ensuring that all data management complies with provisions related to consent, purpose limitations, and incident reporting in the event of a security breach.

Furthermore, the Communication and Information Technology Office plays a significant role in strengthening the readiness of supporting infrastructure, such as user authentication arrangements, role-based access control, the use of secure communication channels, and the establishment of data storage and destruction procedures in accordance with regulations. For example, when application-based administrative services require the public to enter personal data, the Communication and Information Technology Office and relevant agencies need to ensure that the purpose of the processing is clearly communicated, the data is processed only for relevant purposes, and technical safeguards are implemented to mitigate the risk of leakage. Therefore, the successful implementation of the Personal Data Protection Law (PDP) in the regions depends not only on regulations but also on consistent implementation and effective inter-agency coordination.

This study aims to examine the implementation of the Personal Data Protection Law at the Communication and Informatics Office of Majalengka Regency, including policies, challenges , and strategies for securing personal data. This study is expected to provide a comprehensive overview of the effectiveness of the PDP Law's implementation and provide recommendations for improving personal data protection governance in the region. Therefore, this research is crucial, particularly in Majalengka Regency.

METHOD

This research uses a qualitative descriptive method, aiming to provide an in-depth overview of the implementation of the Personal Data Protection Law in Majalengka Regency. Through this approach, the research not only describes the existence or absence of regulations but also explores how the provisions of Law Number 27 of 2022 concerning Personal Data Protection are actually translated

into policies, procedures, and data management practices within local government. Thus, the research captures the context of implementation, emerging obstacles, and institutional responses to the implementation of personal data protection.

The data sources used in this study include primary and secondary data. Primary data consists of interviews with two officials from the Majalengka Regency Communications and Information Department, including the head of the public information and communication and informatics divisions. These two officials were selected because they are directly involved in the formulation and implementation of personal data protection policies, including the management of information systems related to government and public communication needs. In addition to interviews, the study also conducted direct observations of the information systems used in personal data management, such as examining data access flows, account management, server security, and control practices for the use of sensitive data. In order to strengthen the data, observations can be directed at concrete examples, for example, how data is uploaded, stored, processed, and withdrawn when no longer needed in accordance with the principles of purpose limitation and retention.

Secondary data includes Law Number 27 of 2022 concerning Personal Data Protection and related regulations, such as Government Regulations and regional policies relevant to data protection governance. Furthermore, researchers also included references from internal documents or guidelines supporting implementation, such as standard procedures for information system management, technical data security regulations, and supporting documents for the implementation of digital services that utilize public data. Thus, secondary data provides both a normative framework and institutional context for understanding the appropriateness of practices in the field.

Data collection techniques were conducted through a literature review of relevant regulations and academic documents, in-depth interviews with Communication and Information Technology (Diskominfo) officials and data security experts, and observations of the implementation of the data protection system in Majalengka Regency. The in-depth interviews aimed to specifically explore implementation practices, such as those related to the identification of controller and processor roles, the application of data minimization principles, and mechanisms for reporting incidents or data leaks in the event of disruptions. Meanwhile, observations were directed at observing the implementation of technical and administrative controls, such as the use of encryption, role-based access restrictions, system activity logging, and possible risk assessments for certain systems that store citizen data.

Data were analyzed using thematic analysis, grouping the research findings into several main themes, such as policies, challenges, and recommendations. Under the policy theme, researchers examined how the PDP Law is translated into regulations or SOPs within organizations. Under the challenge theme, the research identified obstacles such as limited resources, gaps in technical and legal understanding, the complexity of managing an integrated information system, and the need for ongoing training for officers accessing data. Furthermore, under the recommendation theme, the analysis results were compiled to offer realistic improvement measures, such as strengthening governance, developing compliance documents, improving information security standards, and strategies to increase awareness and capacity of human resources related to personal data protection.

RESULTS AND DISCUSSION

Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) aims to provide legal guarantees for personal data owners and encourage all parties to manage data securely, responsibly, and in accordance with statutory provisions. Under this law, every process of collecting, storing, utilizing, and destroying personal data cannot be carried out haphazardly but must consider aspects of data owner consent, purpose limitations, and protection from the risk of leakage or misuse. Furthermore, the PDP

Law also serves as a foundation for enforcing compliance, ensuring that data management agencies have clear procedures, measurable audits, and accountable security standards.

In Majalengka Regency, the implementation of the Personal Data Protection Law by the Communication and Informatics Office has demonstrated several positive steps. First, the development of regional regulations aligned with the principles of the PDP Law, for example by clarifying data management procedures within regional government agencies, establishing approval mechanisms, and limiting data access based on service requirements. Second, the implementation of a data security system is a primary focus to ensure that public personal data is not misused. For example, Diskominfo can implement security through role-based access control, encryption for data storage or transmission, and monitoring system activity to detect potential incidents early. Third, outreach to government employees on personal data governance is carried out so that all officers understand the obligations and ethics in handling data, including data minimization practices (retrieving only necessary data), secure document management, and vigilance against threats such as phishing or data leaks through unprotected storage media.

However, the effectiveness of implementation still faces challenges, such as the lack of adequate technological infrastructure and a lack of employee understanding of the newly implemented regulations. According to Westby in Thipaporn Klawklong (2025) Personal Data Protection and Privacy , the effectiveness of implementing personal data protection in the government sector is highly dependent on regulatory readiness, technological infrastructure, and awareness of users and data managers.

Policy Compliance with the PDP Law

In assessing the compliance of regional policies with the PDP Law, several aspects of concern are Compliance with the Basic Principles of the PDP Law, such as the legitimacy of data processing, transparency, and data security. The legitimacy of data processing, for example, must have a clear legal basis (e.g., for a specific public service), a specific processing purpose, and retention limits so that data is not stored longer than necessary. Transparency also needs to be realized through notification to the public regarding the type of data processed, the expected benefits, and complaint channels in case of objections. Furthermore, data security is a crucial element, for example through the implementation of access control, encryption, and system security to prevent data leaks or misuse.

Furthermore, compliance with Data Subject Rights is a key indicator, encompassing the right to access, the right to rectification, and the right to data deletion. In practice, the right to access can be demonstrated through a request for documents or information relating to a citizen's personal data, while the right to rectification can be exercised when data is incorrect (e.g., NIK, address, or contact information). The right to deletion requires a procedural process, for example, after the processing purpose has been completed or when the data subject withdraws consent in accordance with the provisions. To ensure the effectiveness of these rights, regional policies should provide easily accessible procedures, clear response deadlines, and proportionate identity verification to prevent misuse of requests.

Furthermore, the implementation of Technical and Organizational Protections must also be considered, including the digital security standards used by the Communication and Information Technology Office. For example, the implementation of account management policies (least privilege), strong authentication (e.g., multi-factor authentication), activity logging, and monitoring for unauthorized access are essential. Organizationally, roles and responsibilities, employee training on information security, and incident response procedures are needed in the event of hacking attempts or

data breaches. This way, all technical and governance measures are aligned with the provisions of the Data Protection and Data Protection Law and ensure the ongoing implementation of data protection.

Regional policies in Majalengka are relatively in accordance with the principles of the PDP Law, but there are several gaps as follows:

Table 1 – GAP Analysis of the Implementation of the PDP Law in Majalengka

Aspects of the PDP Law	National Standard	Conditions in Majalengka	GAP
DPO designation	Mandatory in every agency	New at Diskominfo	Not yet in other OPDs
Data Subject Rights	Access, correction, deletion of data	There is no formal mechanism yet	Need SOP
Data Security	Encryption, MFA, regular audits	Basic firewall and backup	Limited security technology
Incident Report	Max. 72 hours	There is no procedure yet	Very crucial
Public Socialization	Massive digital literacy	Limited socialization	Needs to be expanded

This GAP analysis shows that although Majalengka normatively supports the PDP Law, in practice there are still major gaps, especially at the technical and procedural levels. Currently, the Majalengka Regency Communications and Information Service has adjusted its internal policies to national regulations, although there are still aspects that need to be improved, such as the data security audit system and increasing the role of the Data Protection Officer (DPO). According to Solove (20 21) in Privacy Law Fundamentals , many local governments are still in the early stages of implementing data protection regulations so that there is often a gap between national policies and their implementation in the regions.

A. Impact of Implementation on Personal Data Security

The implementation of the Personal Data Protection Law has had several impacts on personal data security in Majalengka Regency. In general, these impacts can be seen from two perspectives: positive and negative. First, there has been an increase in awareness of the importance of personal data security, both among government employees and the public. For example, employees in various agencies have become more careful in storing documents containing National Identity Numbers (NIK), contact numbers, and population information, and have become more selective in sharing data access through official accounts. Second, cybersecurity infrastructure has also been strengthened, such as by implementing firewalls, updating security systems (patching), setting role-based access rights, and using data encryption to prevent data interception or theft during transmission and storage. Furthermore, third, internal oversight and audits of personal data management have begun to be implemented in a more structured manner, for example through regular reviews of data management procedures, checking compliance with security standards, and evaluating incidents in the event of disruptions.

However, negative impacts have also emerged and require attention. One example is the suboptimal understanding and implementation of the Personal Data Protection Law by human resources (HR). This is evident in the fact that some employees still lack a thorough understanding of basic concepts such as data processing consent, data minimization principles, or mechanisms for handling data access and deletion requests by data subjects. Furthermore, the risk of data leaks is increasingly prominent due to cyberattacks, given that security systems are still being strengthened. For example, phishing attacks targeting employees or hacking attempts on application-based services can potentially open up leaks, especially if verification and incident reporting procedures are not yet effective.

Furthermore, the lack of public involvement in understanding their rights and obligations regarding personal data protection also contributes to obstacles, as people often do not know how to file complaints, request clarification, or report misuse of their personal data.

According to a 2022 report by the Ponemon Institute, more than 40% of local government agencies across the country face the risk of data breaches due to a lack of human resource understanding of data protection policies. In other words, the primary problem lies not only in the technology but also in the preparedness of the people managing the system. Therefore, education and training are key elements in effective implementation, for both employees and the public. Education can be delivered through face-to-face outreach, campaigns through official social media, and practical training that includes data breach scenario simulations, an introduction to types of cyber threats, and the implementation of incident handling procedures. This is further reinforced by an interview with the Head of the Majalengka Regency Communications and Information Office, who stated that public education and training in managing personal data are essential. Through these measures, it is hoped that the implementation of the Personal Data Protection Law will not stop at administrative compliance but will truly improve the resilience of personal data security on a sustainable basis.

As part of a comparative analysis, this study examines the implementation of the Personal Data Protection Law in Majalengka Regency and compares it with several other regions considered more advanced in personal data management, namely Bandung City and Sleman Regency. Using this approach, the study seeks to determine the extent to which each region has translated national norms into governance practices, institutional strengthening, and technical readiness to protect citizen data.

In Majalengka Regency, derivative regulations are already in place at the regional level, for example through the development of guidelines or regional head regulations regarding data management and procedures for handling service requests containing personal data. Furthermore, measures to strengthen data security systems have begun to be introduced, such as the implementation of role-based access control, employee account management, and restrictions on authorization to access certain databases. However, the capacity of the data security infrastructure remains relatively limited, both in terms of supporting devices (e.g., the availability of security monitoring systems and advanced encryption) and in terms of preparedness for incident response procedures. Furthermore, employee understanding of data protection provisions needs to be continuously improved through ongoing training, given that in daily practice there is still a diversity of understanding regarding the legal basis for data processing, consent mechanisms, and procedures for handling data subject rights.

Furthermore, the City of Bandung has a more comprehensive regulatory framework and has adopted cloud-based security technology as a data protection measure. This implementation is evident, for example, in the use of managed storage services that enable the implementation of centralized security policies, activity monitoring, and regular system updates. However, the main challenge remains the high volume of data managed, as cities with diverse public services tend to generate large amounts of data from various work units. Therefore, a more structured and complex risk management approach is required, including mapping data breach risks, establishing protection priority levels, and periodically evaluating vendor compliance and inter-agency system integration.

Meanwhile, in Sleman Regency, a Data Protection Officer plays an active role in overseeing compliance with the Personal Data Protection Law. This role is reflected in reviewing policy documents, coordinating with regional government agencies regarding data processing, and facilitating the development and adjustment of service procedures concerning the public's personal data. However, efforts to educate the public about data protection rights still face challenges, such as limited information channels that reach all segments of the population and varying levels of digital literacy. As

a result, public understanding is not yet fully entrenched, leaving some residents unaware of their rights to access, correct, or request deletion of data in accordance with applicable regulations.

According to Greenleaf's (2019) research in Asian Data Privacy Laws , the effectiveness of implementing personal data protection regulations is largely determined by the readiness of the infrastructure and the capabilities of human resources in understanding and implementing the established provisions.

B. Recommendations for Policy Improvement and Strengthening

Based on the analysis above, there are several recommendations to improve the implementation of the PDP Law in Majalengka Regency:

a) Strengthening Data Security Infrastructure through improving cybersecurity systems by implementing stronger data encryption , adopting international security standards such as ISO 27001 in government data management.
b) Increasing human resource capacity through regular training for government employees on personal data management , increasing the number of cybersecurity experts at the Communication and Information Service , and increasing public awareness.
c) Conducting public campaigns about the right to personal data protection.
d) Develop a complaint channel for the public regarding personal data breaches.
e) Strengthening Regulation and Supervision
f) Establish a special task force to monitor OPD compliance with the PDP Law.
g) Conducting routine audits of personal data management systems in local governments.

According to Cavoukian (2011), in the concept of Privacy by Design, a good data protection system must be built from the beginning into every policy and technology system used, rather than being implemented reactively when problems arise. This means that data protection principles need to be integrated from the planning stage, public service application development, operational procedure management, and data access and storage arrangements. In the context of implementation, policies that include data minimization, transparency to data subjects, and multi-layered security will help ensure that citizen data is processed responsibly.

The implementation of the Privacy and Data Protection Law (PDP) at the Majalengka Regency Communications and Information Technology Office has been carried out through various policies and initiatives, such as establishing internal regulations related to data management, adjusting procedures for system-based services, and strengthening information technology governance. However, despite these steps, challenges remain regarding the effectiveness of their overall implementation. In the field, obstacles often encountered include the consistent application of security standards across all units, suboptimal monitoring of data access, and limitations in ensuring that each new system truly implements Privacy by Design principles from the outset. Furthermore, compared to other regions, Majalengka is still in the early stages of strengthening regulations and infrastructure, so some technical and administrative aspects are not yet fully developed.

Therefore, improvements are needed in several key aspects. First, in terms of data security, mechanisms such as data encryption during transmission and storage, the implementation of role-based access control, and updates to risk management and disaster recovery policies are needed. For example, improved security can be seen in the implementation of regular system audits to detect suspicious activity and security testing of service applications used by the public. Second, human resource capacity also needs to be improved through regular training for employees on understanding the PDP Law, data management ethics, and security practices such as handling data

incidents and secure password management. With better prepared human resources, procedural errors that could potentially lead to data leaks can be minimized.

Furthermore, public involvement in understanding their rights regarding personal data protection is also crucial. For example, local governments can provide easily accessible information channels regarding data subject rights, procedures for submitting requests for data access or correction, and how to file complaints in the event of suspected violations. With targeted education, citizens will better understand how their data is used and what steps can be taken when their rights are not met. With strengthened policies, infrastructure, and better and more integrated education, Majalengka Regency can improve the effectiveness of the implementation of the Personal Data Protection Law. Ultimately, a consistent approach, from system design to operational management, will help ensure the security of its citizens' personal data and increase public trust in government services that utilize citizen data.

CONCLUSION

Despite the existence of supporting regional policies, their implementation still faces obstacles in terms of regulatory understanding, human resources (HR), and information technology readiness to manage personal data securely. The study results show that the implementation of the PDP Law in Majalengka Regency is still in the regulatory and infrastructure strengthening stage. However, progress has been made with the enactment of established rules and regulations. However, major obstacles remain: the lack of formal SOPs for data subject rights, the absence of DPOs at the OPD level, and very limited encryption technology . The Communication and Informatics Agency plays a crucial role as the manager and supervisor of personal data protection. It is tasked with ensuring that the personal data management systems implemented by government agencies and partners adhere to the principles set out in the Personal Data Protection Law, including transparency, accountability, and data security.

There is a need for awareness and understanding among government employees regarding personal data protection because many employees still do not fully understand their rights and obligations in managing personal data, which can increase the risk of data breaches or leaks. Efforts to mitigate the risk of personal data breaches have been implemented, but further strengthening is needed. Several steps taken by the Communications and Information Technology Office (Diskominfo), such as the use of digital security systems and the appointment of Data Protection Officers (DPOs), are already underway. However, challenges remain in implementing the latest technology-based data security standards and preparing emergency response procedures in the event of a data breach. Comparisons with other regions show that Majalengka Regency still needs to improve the effectiveness of its personal data protection policies. Several regions that are more advanced in implementing the Personal Data Protection Law, such as Bandung City and Sleman Regency, already have more mature policies, stronger data security infrastructure, and more detailed regional regulations. Therefore, Majalengka Regency needs to take strategic steps to accelerate policy adaptation and improve synergy between institutions in personal data protection.

REFERENCE

Alibeigi, A., & Munir, AB (2023). Public Health Data and International Privacy Rules and Practices: A Case Study of Singapore. Lecture Notes in Computer Science (Including Subseries

Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 14149 LNCS(November), 51–66.
Arief, V. (2023). E-Government in Southeast Asia: A Comparison of E-Government Development in Singapore, Malaysia, and Indonesia. Social Issues Quarterly, 1(2), 345–362.
Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online Privacy Concerns and Privacy Management: A Meta-Analytical Review. Journal of Communication, 67(1), 26-53.
Cavoukian, A. (2011). Privacy by Design: The 7 Foundational Principles. Information and Privacy Commissioner of Ontario
Gasser, U., & Palfrey, J. (2019). Fostering Innovation and Protecting Privacy: Challenges of the Internet of Things. Harvard Journal of Law & Technology, 29(1), 1-35.
Greenleaf , G (2019) . Asian Data Privacy Laws : Trade & Human Rights Perspectives, Croydon: Oxford University Press.
Katadata Insight Center. (2022). *Digital Data Protection Survey Report in Indonesia* .
KOMINFO. (2022). Indonesia Digital Literacy Program. Jakarta: Ministry of Communication and Informatics.
KOMINFO. (2023). Annual Report 2022-2023. Jakarta: Ministry of Communication and Informatics.
Livingstone, S., & Helsper, E. J. (2019). Balancing Opportunities and Risks in Teenagers' Use of the Internet: The Role of Online Skills and Internet Self-efficacy. New Media & Society, 12(2), 309-329.
Nasrullah, R. (2022). Digital Communication in Indonesia: Theory and Practice. Jakarta: Elex Media Komputindo.
Nugroho, Y., Putri, DA, & Laksmi, S. (2018). Digital Literacy: Creating an Inclusive Public Space. Yogyakarta: INSISTPress.
Rahman, F. (2021). Legal Framework for Personal Data Protection in the Implementation of Electronic-Based Government Systems in Indonesia. Indonesian Journal of Legislation, 18(1), 81.
Santoso, D. (2022). Cybersecurity and Personal Data Protection in Indonesia. Journal of Information Security, 5(2), 134-148.
Solove, DJ (2021). Understanding Privacy. Harvard University Press.
Schreier, M. (2012). Qualitative Content Analysis in Practice (1st ed.). SAGE Publications Ltd.
Smith, M., Szongott, C., Henne, B., & Von Voigt, G. (2012). Big data privacy issues in public social media. IEEE International Conference on Digital Ecosystems and Technologies.
Thipaporn Klawklong (2025) Modern public administration and legal adaptation in the digital age and a case study of Thailand , Journal of Public and Private Issues, 2 (4) 2025 .
West, S. M. (2019). Data Capitalism and Algorithmic Racism. Surveillance & Society, 17(1/2), 158165.
Mustajab, R. (2023). BSSN: There were 311 cases of data leaks in Indonesia in 2022. Dataindonesia.Id.
https://inet.detik.com/security/d-5704729/kominfo-bssn-usut-kebocoran-data-pribadi-1-3-juta-pengguna-ehac .
https://www.cnnindonesia.com/nasional/20240228133731-12-1068273/bssn-ungkap-kronologi-kebocoran-data-pemilih-kpu-di-sidang-dkpp .