Journal of Business, Management, and Social Studies
Vol. 5, No. 2, June 2025, pp 77-84
e-ISSN 2798-6209
DOI: https://doi.org/10.53748/jbms.v5i2.123
Available online at www.jbms.site

Threats and Strategies for Personal Data Protection in Digital Services: A Thematic Review and Regulatory Analysis

Djayanti
Master of Law Program, Universitas Tarumanagara, Jakarta, Indonesia

Wilma Silalahi
Lecturer, Master of Law Program, Universitas Tarumanagara, Jakarta, Indonesia

ABSTRACT
Purpose - This article aims to analyze the threats to personal data in digital services and the protection strategies used, by integrating legal, policy, information technology, and digital literacy approaches.
Methodology - This research uses a qualitative approach based on doctrinal, thematic, and comparative analysis. Data was collected from legal texts, policy documents, academic literature, and empirical studies to build a comprehensive analytical framework. The analysis was conducted to identify threat categories and protection strategies, and evaluate the effectiveness of regulatory frameworks such as the General Data Protection Regulation (GDPR) and the PDP Law.
Findings - The research found that threats to personal data stem from both technical (phishing, malware, dark patterns) and non-technical factors (low digital literacy, weak regulation). An effective protection strategy is the integration of technical approaches such as encryption and digital auditing, as well as non-technical approaches such as education, regulation, and institutional transparency.
Novelty - This study distinguishes itself from previous literature by combining legal, technological, and social analysis in a unified synthesis, and provides a review of the effectiveness of the PDP Law as a public protection instrument.
Keywords: *personal data protection, digital security, PDP Law, digital literacy, data regulation*

JEL Classification: K20, K23, L86
Article Info: Received 2 June 2025; Revised 9 June 2025; Accepted 10 June 2025
Article Correspondence: kiki.djayanti@gmail.com
Recommended Citation: Djayanti, & Silalahi, W. (2025). Threats and Strategies for Personal Data Protection in Digital Services; A Thematic Review and Regulatory Analysis. Journal of Business, Management, and Social Studies, 5(2), 77-84.

I. INTRODUCTION

In the era of the digital economy, personal data has become a vital commodity while being vulnerable to exploitation. Data utilization by digital service providers such as financial applications, e-commerce, and social media is often done with manipulative consent or without full understanding from the user. In this context, the urgency of personal data protection is heightened as information such as identity, location, preferences, and transaction history can be used for profiling, fraud, or manipulation of online behavior. In addition to being targeted for commercialization, user data is also vulnerable to being used for political

Journal of Business, Management, and Social Studies
Vol. 5, No. 2, June 2025, pp 77-84
e-ISSN 2798-6209
DOI: https://doi.org/10.53748/jbms.v5i2.123
Available online at www.jbms.site

purposes or the spread of disinformation. Public ignorance of their digital rights exacerbates the situation, as it provides greater room for data abuse by service providers. Most digital platforms are not transparent in explaining the purpose of data collection, which reinforces the information asymmetry between users and service providers. This calls for proactive public policies and effectively functioning legal protections. Understanding the root causes and solutions of data protection is a priority in national digital governance.

The phenomenon of massive data leaks in Indonesia, such as the BPJS Health case and the President's vaccination certificate, is an alarm that the national digital ecosystem does not yet have adequate protection fortresses (Runtuwene et al., 2023). On the other hand, regulations such as Law No. 27 of 2022 on Personal Data Protection (UU PDP) have become an important foothold, but implementation challenges are still great. Huda et al. (2024) emphasized that privacy protection guarantees are part of citizens' rights in a rule of law system, which must be enforced substantively, not just normatively. Weak institutional structures, lack of human resource capacity, and lack of enforcement mechanisms are the main obstacles. Many public and private institutions do not have internal policies that are in line with data protection principles. In addition, coordination between agencies in responding to data breaches is often slow and unstructured. All of this points to the need for a comprehensive strengthening of legal and institutional capacity to ensure the effectiveness of the PDP Law.

Comparison with global regulations such as GDPR shows that the success of data protection is not only determined by legal norms, but also by implementation, monitoring and user literacy (Marikyan et al., 2023; Santos et al., 2025). Practices such as dark patterns and third-party exploitation of data are evidence that data protection demands a multidisciplinary approach, including reform of digital system design and strengthening of institutional controls (Santos et al., 2025). In Europe, the GDPR requires breach notification within 72 hours and imposes substantial penalties on violators, while in Indonesia, the response to breaches remains unsystematic. Digital literacy is an important differentiator, as a data-savvy society is more likely to demand accountability and exercise their rights. The implementation of data protection must be combined with a broad and sustained public education campaign. Cross-country studies show that a comprehensive approach has a greater impact than a sectoral and reactive approach.

This research seeks to present a comprehensive analysis of threats and strategies for personal data protection in the digital era with a thematic approach based on a structured literature review. The literature that were reviewed based on their relevance, publisher reputation, and contribution in explaining the forms of threats and personal data protection strategies. This research not only elaborates on the technical and policy aspects, but also examines the effectiveness of the legal approach and its implementation challenges in Indonesia. Taking into account the Indonesian context, which is building the foundation of national digitalization, this study places data protection as a fundamental element in the development of a fair and sustainable digital system. The analysis is conducted by considering global dynamics and best practices from other jurisdictions to strengthen contextualized recommendations.

Against this background, this article aims to answer some fundamental questions: (1) What are the categories of threats to personal data that are evolving in the digital era? (2) What strategies have been proposed or implemented to address these threats? (3) What is the effectiveness of current legal and policy approaches in ensuring data protection? (4) What are the policy recommendations based on the literature findings to strengthen security and public trust in digital services? In addition, this research aims to provide a conceptual and practical basis that can be used to redesign data protection policies more effectively and responsively to current needs. These questions serve as the main framework for reviewing the literature and formulating applicable recommendations. In the Indonesian context, addressing data protection challenges also means building digital trust and guaranteeing citizens' basic rights in the virtual realm. Thus, this research becomes relevant not only academically but also strategically for public policy reform.

Journal of Business, Management, and Social Studies
Vol. 5, No. 2, June 2025, pp 77-84
e-ISSN 2798-6209
DOI: https://doi.org/10.53748/jbms.v5i2.123
Available online at www.jbms.site

II. LITERATURE REVIEW

The development of digital services has brought about fundamental changes in the landscape of personal data protection, technically, socially and legally. The literature reviewed in this study shows that data protection issues are multidimensional and demand an interdisciplinary approach. The basic concept of personal data as an individual right that must be safeguarded by the state is comprehensively outlined by Rupp and von Grafenstein (2024), who emphasize that data anonymization is not an absolute solution if it is not accompanied by strict control over third parties. Aji (2023) adds that the state's approach to data sovereignty largely determines the extent to which individuals are protected from digital exploitation. In the Indonesian context, Rosadi (2023) provides a juridical mapping of the Personal Data Protection Law (PDP Law) and highlights the gap between its normative content and implementation.

Threats to personal data are not only technical in nature such as hacking, phishing, and malware, but also arise from non-technical aspects such as low digital literacy and the use of dark patterns by application developers. Santos et al. (2025) explain how digital interface design can trick users into giving up data without realizing it. Meanwhile, Marikyan et al. (2023) showed that the level of cognitive efficacy of individuals has a major influence on their own data protection. Runtuwene et al. (2023) and Faizal et al. (2023) emphasized that weak system security controls put user data at high risk, especially in widely used platforms such as social security systems and e-commerce applications. Yuniarti et al. (2023) add that similar risks are also present in the digital logistics sector, which lacks adequate data protection standards.

Personal data protection strategies in the literature are categorized into two main approaches: technical and non-technical. Technical strategies include the use of encryption systems, periodic digital audits, and the development of secure and transparent system architecture (Isus et al., 2024; Handayani, 2023). Meanwhile, non-technical strategies emphasize education, digital literacy, and strengthening the role of supervisory institutions. Erikha and Hoesein (2025) emphasize that public education is a key component that has been overlooked in data protection policies. Zahwani and Nasution (2024) add that the effectiveness of regulations will only be achieved if people understand their rights as data subjects and have the ability to resist violations.

On the regulatory side, a number of studies have highlighted the importance of strengthening the legal system and credible enforcement. Husamuddin et al. (2024) discuss the role of criminal law in prosecuting digital data breaches and emphasize the need for an independent and competent cyber unit. Huda et al. (2024) further view data protection as an integral part of the guarantee of citizens' constitutional rights. Books like Gani (2023) and Huda et al. (2024) deepen the understanding of the dynamics between technology and privacy rights, emphasizing that data protection is part of the protection of human dignity in the context of a digital society. The books of Pratama et al. (2024) and Rosadi (2023) amplify this discussion by outlining the institutional and technical frameworks needed to ensure the sustainability of data protection in both the public and private sectors.

In general, the literature reviewed underscores the importance of digital regulatory reform, strengthening public literacy, and the simultaneous integration of technical and legal strategies. Threats to personal data cannot be addressed with just one approach, but must be through a multidimensional synthesis that includes legal, technological, policy and digital culture aspects of society. This study emphasizes that the effectiveness of data protection depends on the synergy between legal norms, public awareness, and the readiness of technology used by state institutions and digital service providers.

Journal of Business, Management, and Social Studies
Vol. 5, No. 2, June 2025, pp 77-84
e-ISSN 2798-6209
DOI: https://doi.org/10.53748/jbms.v5i2.123
Available online at www.jbms.site

III. METHODOLOGY

This research uses a qualitative approach based on doctrinal methods, comparative analysis, and thematic synthesis. The main focus is to explore a holistic understanding of the threats and strategies of personal data protection in the context of digital law and technology. Data was collected from secondary sources in the form of indexed journal articles and scientific books published in 2021-2025 that are relevant to the topic of study.

Literature selection was based on five criteria: (1) relevance to the issue of personal data protection; (2) focus on digital services; (3) publication within the last five years; (4) published in accredited journals or reputable academic publishers; and (5) contain analysis of technical, legal, or public policy strategies related to data protection.

The analysis was conducted in three stages. First, the forms of threats described in the literature were identified. Second, the recommended or implemented protection strategies were analyzed. Third, a thematic synthesis was conducted to find patterns, gaps and potential recommendations that could be developed for policy formulation. This process is reinforced by a comparative approach to international and national regulations.

The results of this analysis are organized into thematic categories to emphasize the linkages between threat types, strategic approaches, and policy implementation challenges. This framework is expected to contribute to academic discussions and the formulation of contextualized and applicable data protection policies.

IV. RESULTS AND DISCUSSION

Categories of Threats to Personal Data in the Digital Age

Based on the results of the study, it shows that threats to personal data in Indonesia's digital ecosystem are increasingly complex and multidimensional. Threats to personal data in the digital era can be divided into two major groups, namely technical threats and non-technical threats, both of which are interrelated and strengthen the vulnerability of data protection systems in society. Technical threats are attacks carried out by utilizing system or software gaps, such as phishing, malware, ransomware, SQL injection, denial of service (DoS), and exploitation of network and server protocol weaknesses. This threat increases along with the integration of personal data in the digital ecosystem, ranging from the financial sector, health, education, to government services. A study by Faizal et al. (2023) noted that more than 40% of data leakage cases in Indonesia occurred due to weak encryption and the absence of regular security audits. This is exacerbated by the use of dark patterns in digital applications that are deliberately designed to mislead users, as stated by Santos et al. (2025). They show that manipulative designs can encourage users to agree to harmful terms of use without full understanding.

Furthermore, non-technical threats often go unnoticed by the public but are no less dangerous. This is supported by people's low digital literacy. Marikyan et al. (2023) show that low digital self-efficacy causes people to be gullible and unaware of the importance of data protection. Erikha and Hoesein (2025) also highlighted the lack of education and socialization regarding digital rights, which makes data protection policies ineffective despite being legally established. This finding is supported by Zahwani and Nasution (2024), who state that the lack of public participation in data use monitoring leads to many violations going unreported and not being followed up legally.

In many cases, users do not fully understand the privacy terms and conditions of the services they use, thus unknowingly giving platforms permission to process and distribute their personal data. This phenomenon is exacerbated by low digital literacy and the lack of regulations governing data usage

Journal of Business, Management, and Social Studies
Vol. 5, No. 2, June 2025, pp 77-84
e-ISSN 2798-6209
DOI: https://doi.org/10.53748/jbms.v5i2.123
Available online at www.jbms.site

transparency. In Indonesia, the absence of a strong data protection culture makes people more vulnerable to exploitation, both by corporations and bad actors who utilize data for opinion manipulation, digital fraud, and personal tracking that violates privacy rights (Handayani & Supriadi, 2022).

These threats show that personal data protection is not just a technical challenge that can be solved by strengthening digital security systems, but also a structural problem that demands updates in social norms, business behavior, and legal frameworks. The gap between the speed of technological development and regulatory readiness creates a gap that is exploited by various parties with an interest in data.

Strategies for Countering Threats to Personal Data

The strategies developed to mitigate threats to personal data can basically be categorized into two main approaches: technical approaches and non-technical approaches, which ideally go hand in hand. Technical strategies include the application of information security technologies such as end-to-end encryption, multi-factor authentication, the use of artificial intelligence-based firewalls, and software development based on privacy-by-design principles. The use of these technologies aims to reduce the possibility of unauthorized access to personal data, minimize the risk of leakage, and increase users' control over their own data. For example, encryption not only protects the content of data, but also maintains data integrity and authentication during the transmission process between devices or servers.

This is where non-technical approaches become relevant. Some of the non-technical strategies that emerged from the literature analysis include improving people's digital literacy, reviewing data collection practices by digital platforms, empowering users to understand their privacy rights, and establishing digital ethics committees at the organizational and government levels. This strategy emphasizes the importance of empowering individuals to not only be passive objects in the digital ecosystem, but also actors who have full control and awareness over their data.

Some articles propose the integration of hybrid approaches that combine technical solutions with social and policy interventions, such as the development of user-friendly privacy dashboards, labeling the security level of digital platforms, and implementing data protection certifications that can increase the accountability of digital services. In other words, strategies that are participatory and transparent have a greater chance of creating sustainable digital trust.

Effectiveness of Legal and Policy Approaches in Indonesia

The passing of Law No. 27 of 2022 on Personal Data Protection (PDP Law) is an important milestone in Indonesia's legal system that regulates the management and protection of personal data in a more structured manner. It provides a legal definition of personal data, establishes the rights of data subjects, and requires data controllers to report incidents of data breaches (Kurniawan et al., 2023). However, a number of articles highlight that while this regulation is a progressive step, its effectiveness is still limited by implementation challenges. Weak law enforcement, the lack of an independent data protection authority, and the lack of human resources in digital forensics and cybersecurity are the main obstacles in the operationalization of this law.

The PDP Law in Indonesia has indeed provided a legal foundation, but its implementation is still far from ideal. Rosadi (2023) revealed that many agencies do not yet have a data protection task force, and public complaint mechanisms are still weak. Husamuddin et al. (2024) emphasized that there needs to be a specific law enforcement unit to handle data breaches, equipped with integrated digital audit tools and efficient breach reporting protocols. In the context of the rule of law, Nurul Huda et al. (2024) stated that personal data protection is not just a technical issue, but also involves the fulfillment of constitutional rights and public trust in the state.

Journal of Business, Management, and Social Studies
Vol. 5, No. 2, June 2025, pp 77-84
e-ISSN 2798-6209
DOI: https://doi.org/10.53748/jbms.v5i2.123
Available online at www.jbms.site

In addition, the legal structure in Indonesia is still reactive, taking action after a violation has occurred, rather than preventing it through a strong monitoring and education system. Compared to the European Union's General Data Protection Regulation (GDPR), the PDP Law has not fully adopted the principle of privacy as a right, which places privacy as a fundamental right that cannot be compromised. In many cases, data processing is still carried out without transparent and explicit consent mechanisms, especially in the context of public services or the informal sector. The absence of strong enough sanctions also means that there is no deterrent effect for violators.

The fact that most people are not yet aware of their rights to personal data, coupled with the low transparency of data use by digital platforms, shows that the effectiveness of current legal approaches is still very limited in ensuring data protection. Cross-sector consolidation between the government, private sector, and civil society is needed to oversee a fairer and more participatory implementation of the PDP Law.

Policy Recommendations to Strengthen Digital Protection and Trust

Based on the literature findings, several strategic policy recommendations can be formulated to strengthen the personal data protection system in Indonesia and at the same time build public trust in digital services. First, the state needs to immediately establish an independent personal data protection authority, as mandated in the PDP Law. This institution must have judicial authority, access to digital forensic technology, and the ability to conduct regular data audits. The existence of such an institution will also strengthen the external monitoring system of digital service providers that tend to be non-transparent.

Second, the government must encourage the transformation from reactive data protection policies to preventive and risk-based approaches. For example, by requiring an impact assessment of information technology policies and projects, especially those involving citizen data.

Third, public digital literacy needs to be systemically improved through integration in primary and secondary education curricula, digital community training, and national campaign programs that highlight digital rights and personal data security practices. This public education will strengthen the public's bargaining position in resisting data abuse and increase citizen participation in data protection advocacy.

Fourth, there is a need to harmonize regional and international laws and policies that can strengthen cross-border cooperation in addressing transnational data breaches. Frameworks such as Cross Border Data Flow, GDPR interoperability principles, and the adoption of ISO/IEC 27701 standards can be a reference in building personal data protection that is adaptive and relevant to the era of globalization.

Fifth, it is important for data protection policies to prioritize digital ethics and social justice principles, so that they are not only oriented towards technological efficiency, but also consider vulnerable groups that are more easily excluded or affected by privacy violations, such as children, the elderly, and people with limited digital access.

Overall, these findings reinforce the argument that the challenges of data protection in Indonesia lie not only in legal tools, but also in institutional capacity, public literacy, and technological readiness. To ensure the effectiveness of personal data protection, a systemic and collaborative approach is imperative, with the active involvement of all stakeholders.

V. CONCLUSION

The research concludes that threats to personal data in digital services come from a variety of sources, both technical and non-technical. Cyberattacks, misuse of interface design, weak digital literacy, and lack of institutional transparency are the main issues identified. A successful protection strategy requires the

Journal of Business, Management, and Social Studies
Vol. 5, No. 2, June 2025, pp 77-84
e-ISSN 2798-6209
DOI: https://doi.org/10.53748/jbms.v5i2.123
Available online at www.jbms.site

integration of technical approaches such as encryption and automated reporting systems, with non-technical approaches such as regulation, education, and public oversight.

While the PDP Law has been a legal milestone, its implementation challenges show that data protection reforms must include improving institutional systems, strengthening the technical capacity of officials, and raising public awareness. Going forward, personal data protection should no longer be considered as a secondary issue, but rather as the main foundation of inclusive, transparent, and fair digital service governance.

The policy implications of this study include: (1) An independent and responsive data monitoring unit should be established at the national level; (2) The government should provide curriculum-based digital education in schools and the general public; (3) Regulations should require periodic digital audits for digital service providers; and (4) Digital literacy should be used as an indicator in the evaluation of data-based public policies.

With this framework, Indonesia is expected to be able to build a highly resilient personal data protection system, while strengthening public trust in the national digital ecosystem.

REFERENCES

Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi). Jurnal Politica Dinamika Masalah Politik dalam Negeri dan Hubungan Internasional, 13(2), 222-238.

Erikha, A., & Hoesein, Z. A. (2025). Strategi Pencegahan Kebocoran Data Pribadi melalui Peran Kominfo dan Gerakan Siberkreasi dalam Edukasi Digital. Jurnal Retentum, 7(1), 48–64.

Faizal, M. A., Faizatul, Z., Asiyah, B. N., & Subagyo, R. (2023). Analisis Risiko Teknologi Informasi pada Bank Syariah: Identifikasi Ancaman dan Tantangan Terkini. Jurnal Asy-Syarikah: Jurnal Lembaga Keuangan, Ekonomi dan Bisnis Islam, 5(2), 87–100.

Gani, T. A. (2023). Kedaulatan Data Digital untuk Integritas Bangsa. Banda Aceh: Syiah Kuala University Press.

Handayani, A. (2023). Perlindungan Hukum atas Tindakan Pencurian Data Pribadi pada Layanan Fintech Lending Terhadap Ancaman Cyber Security di Indonesia. Jurist-Diction, 6(4), 605–630.

Huda, N. U., Astaruddin, T., Nasution, M. I., Al Haddad, A., & Gumelar, D. R. (2024). Data pribadi, hak warga, dan negara hukum: Menjaga privasi di tengah ancaman digital. Bandung: CV Widina Media Utama.

Husamuddin, H. M. Z., Efendi, S., Hamdi, S., Rahma, I., Erick, B., Heryanti, N., & Friwarti, S. D. (2024). Hukum Acara Pidana & Pidana Cyber. Medan: PT Media Penerbit Indonesia.

Isus, R., Kolesnikova, K., Khlevna, J., Oleksandr, T., & Liubov, K. (2024). Development of a model of personal data protection in the context of digitalization of the educational sphere using information technology tools. Procedia Computer Science, 231, 347–352.

Kurniawan, Maulana, A., & Iskandar, Y. (2023). The Effect of Technology Adaptation and Government Financial Support on Sustainable Performance of MSMEs during the COVID-19 Pandemic. Cogent Business & Management, 10(1). https://doi.org/10.1080/23311975.2023.2177400

Marikyan, D., Papagiannidis, S., Rana, O. F., & Ranjan, R. (2023). General Data Protection Regulation: A Study on Attitude and Emotional Empowerment. Behaviour & Information Technology, 43(14), 3561–3577.

Pratama, A. M., Syaiful, & Rahman, M. F. (2024). Keamanan Data dan Informasi. Bandung: Kaizen Media Publishing.

Journal of Business, Management, and Social Studies
Vol. 5, No. 2, June 2025, pp 77-84
e-ISSN 2798-6209
DOI: https://doi.org/10.53748/jbms.v5i2.123
Available online at www.jbms.site

Rosadi, S. D. (2023). Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022). Jakarta Timur: Sinar Grafika.

Runtuwene, S. J., Lambonan, O. M., Kasenda, S. R., Torar, E. J., Tumewan, V. V., & Tumewan, T. A. (2023). Penyalahgunaan Data Pribadi dalam Era Cybercrime. Jurnal Ilmu Komputer dan Sistem Informasi, 9(4), 123–125.

Rupp, V., & von Grafenstein, M. (2024). Clarifying "Personal Data" and the Role of Anonymisation in Data Protection Law: Including and Excluding Data from the Scope of the GDPR (More Clearly) Through Refining the Concept of Data Protection. Computer Law & Security Review, 52, 105932.

Santos, C., Morozovaite, V., & De Conca, S. (2025). No Harm No Foul: How Harms Caused by Dark Patterns Are Conceptualised and Tackled Under EU Data Protection, Consumer and Competition Laws. Information & Communications Technology Law, 1–47.

Yuniarti, D. R., Alfarizy, H. F., Siallagan, Z., & Rizkyanfi, M. W. (2023). Analisis Potensi dan Strategi Pencegahan Cyber Crim dalam Sistem Logistik di Era Digital. Jurnal Bisnis, Logistik dan Supply Chain (Blogchain), 3(1), 23–32.

Zahwani, S. T., & Nasution, M. I. P. (2024). Analisis Kesadaran Masyarakat Terhadap Perlindungan Data Pribadi di Era Digital. Journal of Sharia Economics Scholar (JoSES), 2(2), 105–109.