LEGAL PROTECTION OF FACEBOOK USERS' PERSONAL DATA IN INDONESIA UNDER THE PERSONAL DATA PROTECTION LAW

Evita Rouli Silaban[1]
Universitas Esa Unggul, Jakarta, Indonesia
evitasilaban22@gmail.com

Endik Wahyudi[2]
Universitas Esa Unggul, Jakarta, Indonesia
endik.wahyudi@esaunggul.ac.id

Abstract

The rapid advancement of digital technology has enabled seamless global communication, yet it simultaneously heightens the risk of personal data breaches. A salient example is the Facebook data incidents between 2018 and 2021 which affected millions of Indonesian users and revealed systemic weaknesses in data governance. Earlier regulatory instruments, particularly the Information and Electronic Transactions Law (UU ITE), provided limited remedies and made accountability for data controllers difficult to enforce. This study examines legal protections for personal data and the legal liability of Meta through a normative juridical method integrating statutory, conceptual, and case-based analyses using descriptive secondary data. The analysis focuses on key provisions of the Personal Data Protection Law, including Article 17, which guarantees data subject rights to access, correct, and delete their data; Article 18, which obliges controllers to implement adequate security measures to prevent breaches; Article 58, which establishes supervisory authorities to ensure compliance; and Article 75, which imposes administrative sanctions as a deterrent. These provisions collectively strengthen legal certainty for victims and address deficiencies in prior regulations by compelling global digital platforms to adopt higher compliance standards. In conclusion, the Personal Data Protection Law constructs a comprehensive protection regime by affirming user rights and enforcing sanctions effectively.

Keywords: Personal Data Protection Law, Facebook Data Leak, Legal Protection

INTRODUCTION

The phenomenon of digitalization in the contemporary era has become an integral and familiar element of global society. This transformation has been embedded in everyday realities, facilitating access to a wide range of information through online platforms. Within discussions of digitalization, personal data constitutes an inseparable component. Generally, when individuals access websites or authenticate applications, service providers require personal data as a prerequisite for access. Such data include, among others, names, addresses, places and dates of birth, telephone numbers, email addresses, and other related information. However, the disclosure of such data to third parties potentially increases the risk of cybercrime (R. Syailendra & Fitzgerald, 2023).

Nevertheless, the proliferation of electronic media usage has also brought implications in the form of increased risks of personal data loss, thereby heightening users' vulnerability to external threats. One significant empirical example is reflected in a Kompas.com article entitled "Data Pengguna di Indonesia Bocor, Facebook Terancam Sanksi Administratif dan Pidana", which describes privacy violations affecting Facebook users in Indonesia in 2018 and 2021. These incidents involved the leakage and widespread dissemination of millions of pieces of personal data, triggering extensive investigations into the adequacy of privacy and data security protection mechanisms in the digital era.

As part of legal scholarship, personal data protection in Indonesia is grounded in various laws and regulations. One of the primary legal foundations is Law Number 19 of 2016 concerning Electronic Information and Transactions (EIT Law), which regulates privacy rights related to personal data. This law also establishes legal mechanisms to address privacy violations, including reporting procedures and legal claims that may be filed by individuals affected by data breaches. Pursuant to this framework, Minister of Communication and Informatics Regulation Number 20 of 2016 further elaborates provisions and guidelines for the protection of personal data in electronic media. However, the implementation and enforcement of these regulations, as well as the protection afforded to victims, continue to face significant challenges across various dimensions (Sa et al., 2025).

The data breach incidents involving Meta through Facebook in Indonesia illustrate the vulnerability of accessed personal data. Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) expands the regulatory scope and establishes a more robust legal foundation by clarifying the obligations of electronic system controllers in protecting individuals' personal data. Meta, as the parent company of Facebook, is required to disclose data breaches within 72 hours and may be subject to administrative, criminal, civil, and compensatory sanctions if the harm suffered by users is deemed to result from negligence. Conversely, individuals whose personal data have been compromised may submit complaints to the Ministry of Communication and Informatics and pursue legal remedies against the relevant electronic system operators. Nevertheless, law enforcement faces particular challenges due to the transnational nature of technology companies' operations. In the absence of effective complaint mechanisms and enforcement coordination, the imposition of criminal and administrative sanctions becomes imperative (Khansa Rusyda, 2025).

This study identifies a research gap concerning the effectiveness of protection under the PDP Law. Although numerous studies and public reports have addressed Facebook data breaches and their impacts, there remains a lack of specific evaluations of the PDP Law's

implementation in the context of ongoing data breaches in Indonesia. Previous research has often relied on outdated regulatory frameworks and has not sufficiently examined enforcement challenges. Additionally, another gap exists regarding the role of multi-stakeholder collaboration in personal data law enforcement. Prior studies have primarily focused on regulatory aspects and the consequences of data breaches, while paying limited attention to the synergy between government authorities, technology providers such as Meta/Facebook, and society in implementing data protection in accordance with the PDP Law, particularly in large-scale cross-border data breach cases.

The novelty of this research lies in the integration of normative legal analysis of the PDP Law as the most recent legal framework with a normative legal approach to map practical implementation challenges. Furthermore, the study focuses on recent Facebook data breach cases by examining regulatory challenges and opportunities within modern legal frameworks, as well as the dynamics between perpetrators and victims, thereby offering a fresh perspective compared to general or global studies. Overall, this research fills a significant gap by evaluating legal protection under the PDP Law in Indonesia and the role of multi-actor collaboration in Facebook data breach cases, which have not been extensively explored in previous journals, while providing an original contribution to the evolving intersection of law and technology in Indonesia.

The research questions addressed in this journal are as follows: (1) What forms of legal protection are afforded to Facebook users' personal data under Law Number 27 of 2022 concerning Personal Data Protection? and (2) What is the legal responsibility of electronic system operators (Meta/Facebook) for data breaches involving Facebook users in Indonesia?

REVIEW OF LITERATURE

Studies on personal data protection have increasingly gained scholarly attention in response to the rapid expansion of digital platforms and social media usage. Previous research has generally emphasized the vulnerability of personal data in digital ecosystems, highlighting how the collection, processing, and dissemination of user data by online platforms expose individuals to privacy violations and cyber risks (Syailendra & Fitzgerald, 2023). These studies underline that personal data has become a valuable digital asset, requiring comprehensive legal safeguards to prevent misuse and unauthorized disclosure.

Several scholars have specifically examined data breaches involving global social media platforms, including Facebook, as a manifestation of systemic weaknesses in digital governance. Research focusing on Facebook data leak incidents has predominantly analyzed the scale of breaches, the technological vulnerabilities exploited, and the implications for users' privacy rights. However, many of these studies concentrate on technical or policy dimensions rather than conducting in-depth legal analysis of corporate responsibility and regulatory enforcement, particularly within national legal systems such as Indonesia.

In the Indonesian context, existing literature on personal data protection has largely relied on the Electronic Information and Transactions Law (Law Number 19 of 2016) and its implementing regulations. These studies assess privacy protection mechanisms primarily through the lens of consent, electronic system security, and administrative obligations of electronic system operators. While such research provides important foundational insights,

it remains limited due to its reliance on pre-Personal Data Protection Law regulatory frameworks, which lack comprehensive enforcement mechanisms and clear sanctioning regimes.

Following the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), several recent studies have begun to discuss its normative significance as Indonesia's first comprehensive personal data protection regime. These studies emphasize the expanded rights of data subjects, the enhanced obligations imposed on data controllers and processors, and the introduction of administrative, civil, and criminal sanctions. Nevertheless, most of this scholarship remains theoretical and has not sufficiently examined the practical effectiveness of the PDP Law in addressing large-scale, cross-border data breaches involving transnational technology corporations such as Meta/Facebook.

Accordingly, a clear research gap persists regarding the evaluation of legal protection and enforcement effectiveness under the PDP Law in real-world data breach cases. Prior studies tend to focus either on regulatory design or on general discussions of data privacy without integrating case-based normative analysis. This study seeks to fill this gap by critically examining Facebook data breach incidents in Indonesia through the framework of the PDP Law, while also analyzing the legal responsibility of electronic system operators and the challenges of enforcing personal data protection in a transnational digital environment.

RESEARCH METHOD

The research method adopted in this study is normative legal research. This approach essentially focuses on the systematic analysis of the existing legal framework, encompassing jurisprudential principles, regulations, normative provisions, legislative instruments, legal consensus, and relevant legal doctrines (Maharani & Prakoso, 2024). Within this framework, doctrinal inquiry refers to a comprehensive examination of the body of law that has been formulated and elaborated based on the teachings and principles firmly upheld by its conceptual architects and/or developers.

This study applies a normative legal approach by employing the statute approach, comparative approach, and conceptual approach (Intan et al., 2023). The case approach centers on an in-depth examination of Facebook data breach incidents in Indonesia in 2018—where more than two million data records were leaked through the JustToknow server—and in 2021—when 87 million data records were reportedly sold on the dark web via RaidForums—illustrating systemic vulnerabilities and the practical effectiveness of the Personal Data Protection Law (Khansa Rusyda, 2025).

The research is designed using a systematic approach to produce a comprehensive and holistic understanding, in which data are processed through a descriptive-analytical method. This study seeks to systematically examine the positive law regulatory framework governing personal data protection within the jurisdiction of Indonesia, with particular emphasis on specific provisions of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). The methodology includes a comparative review of relevant legislative instruments and various legal doctrines that serve as conceptual foundations, aimed at formulating an optimal and functional paradigm for ensuring juridical protection for individuals as personal data subjects.

Primary and secondary legal materials were employed in this study. Primary legal materials consist of statutes and regulations related to personal data protection, particularly Law Number 27 of 2022 concerning Personal Data Protection, while secondary legal materials include legal doctrines, scholarly articles, journal publications, and relevant case reports. The collected legal materials were analyzed using qualitative descriptive-analytical techniques to draw normative conclusions.

Research Hypothesis

This study is based on the hypothesis that the enactment of Law Number 27 of 2022 concerning Personal Data Protection has not yet been optimally implemented in addressing large-scale personal data breaches involving transnational electronic system operators such as Meta/Facebook. Furthermore, this research hypothesizes that weaknesses in enforcement mechanisms, institutional coordination, and cross-border regulatory cooperation limit the effectiveness of legal protection afforded to Facebook users' personal data in Indonesia.

Research Model

This study adopts a normative legal research model that conceptualizes personal data protection as an interaction between legal norms, institutional actors, and enforcement mechanisms.

Law → Obligations of Meta/Facebook → Enforcement Mechanisms → Legal Protection of Users

The model places the Personal Data Protection Law (Law Number 27 of 2022) as the primary normative framework governing the obligations of electronic system operators, particularly Meta/Facebook, and the rights of data subjects. Within this framework, the effectiveness of legal protection is analyzed through statutory provisions, institutional enforcement capacity, and cross-border regulatory challenges. This conceptual model enables an evaluation of how legal norms are translated into practical protection for personal data subjects in cases of large-scale data breaches.

RESULTS AND DISCUSSION

Forms of Legal Protection for Facebook Users' Personal Data under Law Number 27 of 2022 concerning Personal Data Protection

Prior to the enactment of Law Number 27 of 2022 concerning Personal Data Protection (the PDP Law), the regulatory framework governing personal data protection in Indonesia could be characterized as fragmented, limited, and lacking holistic integration. Earlier legal instruments, such as the Electronic Information and Transactions Law (EIT Law) and several regulations concerning the operation of electronic systems, provided only general juridical foundations. These regulations did not adequately elaborate the rights of data subjects, the obligations imposed on data controllers, nor the mechanisms for effective legal implementation. As a result, the management and protection of personal data largely depended on internal corporate or institutional policies, without binding national standards. This regulatory gap significantly contributed to the risk of data breaches, as exemplified by the Facebook incident in 2021, in which millions of users' data were leaked and potentially misused without adequate legal protection for victims in Indonesia (Simanjuntak, 2024).

The enactment of the PDP Law represents a response to the urgent need for a comprehensive personal data protection framework in Indonesia. This law establishes

fundamental principles governing personal data processing, as set forth in Article 7, including the principles of fairness, transparency, purpose limitation, and restrictions on data processing based on relevance and proportionality. These principles are essential as a foundation to ensure that all data processing activities respect the rights of data subjects, mitigate the potential for misuse, and strengthen public trust in entities responsible for data management (Sutarli & Kurniawan, 2023). In addition, Article 4 of the PDP Law explicitly classifies personal data into general personal data and specific (sensitive) personal data, with the latter requiring a higher and more stringent level of protection. This classification is particularly relevant given that data compromised in security breaches on online platforms—such as those involving Facebook—often include not only general information but also highly sensitive data, the exploitation of which may cause significant adverse consequences for affected individuals.

In response to large-scale data breach phenomena, as reflected in previous incidents involving major corporate entities, the PDP Law plays a crucial role as a jurisprudential foundation that definitively and systematically delineates the obligations of data controllers. Article 18 of the PDP Law expressly mandates data controllers to implement personal data security measures in accordance with appropriate security standards, taking into account the level of risk and the characteristics of the data being processed (Wahyudi et al., 2025). Furthermore, data controllers are required to promptly notify competent supervisory authorities and affected data subjects of any personal data breach within a prescribed timeframe. These provisions constitute fundamental elements in realizing the principles of transparency and accountability in personal data governance, enabling affected individuals to access information promptly and to undertake anticipatory and effective protective measures. Such measures may include replacing authentication credentials, monitoring account activity, or assessing relevant legal remedies when necessary.

Before the implementation of the PDP Law, Indonesia's regulatory framework governing personal data security was limited and lacked sufficient detail. Consequently, there were no binding obligations requiring data controllers to notify affected data subjects of data breach incidents (Aqilah et al., 2024). This condition resulted in compromised individuals frequently receiving inadequate information and facing significant obstacles in seeking legal accountability against parties that negligently managed or misused their personal data (Mahendra, 2024). With the introduction of mandatory breach notification provisions, the handling of data breaches has become more structured, coordinated, and effective in minimizing the negative impacts experienced by data subjects, including the potential exploitation of personal data by unauthorized entities.

Furthermore, the regulatory framework concerning data subject rights as stipulated in Article 17 of the PDP Law strengthens the direct legal standing of individuals as owners of their personal information. These provisions grant data subjects the right to access information regarding data collected and processed by data controllers; the right to rectify or update inaccurate or incomplete data; the right to erasure of data processed unlawfully; and the right to object to data processing that deviates from the fundamental principles of personal data protection. The existence of these rights places data subjects in a more substantial position to manage and safeguard their personal information against unauthorized use (Novel & Subiyanto, 2025).

These rights are particularly significant in the context of Facebook data breach cases that have drawn global attention, as they provide a clear juridical basis for victims to seek accountability and pursue legal remedies for the unlawful use or dissemination of their personal data. This represents a substantial advancement compared to prior conditions, in which victims often encountered difficulties in obtaining justice due to the absence of adequate regulatory safeguards. Accordingly, the personal data protection framework serves not merely as a protective legal instrument but also as a preventive mechanism and an educational vehicle aimed at data controllers and the public at large, with the objective of enhancing awareness and ensuring compliance with personal data privacy principles (Agustin, 2025).

In addition, the implementation of the PDP Law requires data controllers to conduct periodic assessments and updates of their data security policies and system architectures. This obligation is intended to ensure adaptability to technological developments and to mitigate increasingly complex cybersecurity threats. This indicates that the PDP Law is not merely a static regulatory framework, but rather promotes the establishment of an accountable and sustainable data governance culture to safeguard the fundamental rights of citizens in the contemporary digital sphere.

The enforcement dimension of the PDP Law represents a substantial advancement compared to previous regulatory instruments. Notably, Articles 74 and 75 explicitly stipulate criminal and administrative sanctions for violations related to personal data processing. Article 74, for example, provides for criminal penalties, including imprisonment and/or substantial fines, for acts such as misuse of personal data, unauthorized disclosure without the consent of the data subject, and other violations that endanger personal data security. These sanctions apply not only to individuals but also to corporations that negligently manage personal data, thereby exerting tangible legal pressure to ensure organizational compliance (Lidya et al., 2020).

Meanwhile, Article 75 governs administrative fines that may be imposed on data controllers for violations of the PDP Law, including failure to report data breach incidents, failure to implement adequate security standards, or failure to respond to data subject requests in accordance with statutory requirements. The magnitude of these fines is designed to produce a deterrent effect, encouraging companies and data controllers—including large and global digital platforms—to take national data protection standards more seriously. This marks a significant departure from the pre-PDP Law era, in which available sanctions were minimal and predominantly administrative in nature, lacking effective criminal enforcement and resulting in many violations going unaddressed (Mahameru et al., 2023).

Moreover, the establishment of a regulatory supervisory authority, as mandated by the PDP Law, serves as a fundamental pillar in the supervision and implementation of personal data protection regulations (Dayang et al., 2025). This supervisory body is endowed with broad and strategic authority, including receiving public complaints, conducting investigations and compliance audits of data controllers, issuing corrective recommendations, and imposing administrative sanctions. Such authority positions the supervisory body as an independent and professional oversight mechanism, ensuring that personal data governance does not rely solely on traditional law enforcement institutions, which often face extensive and complex workloads (Matheus & Gunadi, 2024).

The role of the supervisory authority is vital in ensuring that data controllers fulfill their obligations transparently and accountably, while also guaranteeing the optimal protection of data subject rights. Through a structured oversight system, improvements in personal data governance quality across all sectors—governmental, private, and international digital platforms operating in Indonesia—are expected. The existence of this authority also strengthens a culture of compliance with personal data protection norms, given the tangible risk of sanctions and consistent supervision. Collectively, these provisions reflect a new paradigm in the enforcement of personal data protection law in Indonesia: transitioning from a previously weak and ambiguous framework to one that is firm, systematic, and oriented toward the protection of individual rights.

Nevertheless, the practical effectiveness of the PDP Law continues to face several challenges. The readiness of human resources, both among regulators and business actors, remains a decisive factor in the successful implementation of the law. In addition, public awareness of personal data protection rights must be continuously enhanced to enable individuals to actively exercise their rights. Corporate technological infrastructure and internal procedures must also be aligned with the data governance standards prescribed by the PDP Law. Therefore, the government and relevant stakeholders must intensify socialization efforts, training programs, and technical support to ensure effective implementation of the law.

Overall, the PDP Law represents a significant advancement in personal data protection in Indonesia. Although enacted after major data breaches such as the Facebook incident in 2021, its existence provides a strong legal foundation and clear mechanisms for preventing and addressing future data breach incidents. Through detailed regulation of data subject rights, data controller obligations, supervisory authority mechanisms, and stringent sanctions, the PDP Law creates opportunities for more effective personal data protection, enhances public trust in digital technologies, and encourages companies to prioritize data security in their operations within Indonesia.

Legal Liability of Electronic System Operators (Meta/Facebook) for Facebook User Data Breaches in Indonesia

Law Number 27 of 2022 on Personal Data Protection (the PDP Law) establishes a comprehensive regulatory framework for the protection of personal data of individuals in Indonesia. This legislation explicitly articulates the rights of data subjects and the obligations of data controllers in managing personal information. One of the most crucial components of this law is Article 3, which introduces the principle of extraterritoriality. This principle implies that data controllers, regardless of their physical location outside Indonesian territory, are required to comply with the PDP Law insofar as they process the personal data of data subjects located within Indonesia. This principle serves as a fundamental juridical basis to ensure that global digital platform providers operating across jurisdictions cannot evade compliance with Indonesia's personal data protection regulations. Nevertheless, this principle also presents substantive challenges in terms of implementation and law enforcement, particularly due to limitations in jurisdictional authority and supervisory mechanisms over foreign entities (Sidi et al., 2025).

Furthermore, provisions concerning the rights of data subjects are comprehensively regulated under Articles 28 to 35 of the PDP Law. Article 28 specifically guarantees the right

of data subjects to obtain transparent and accountable information regarding the acquisition and processing of their personal data. This provision is essential to ensure that individuals retain full control over their personal data utilized by corporations, including global digital platforms. Article 29 further guarantees the right of access, enabling data subjects to review the personal data collected and processed by data controllers. Articles 30 and 31 regulate the rights to rectification and erasure of personal data, which are particularly relevant in safeguarding individuals from potential data misuse or mismanagement by corporations (Suroso et al., 2024). These rights affirm that data subjects are not merely passive objects but possess legal authority to control their personal data (Quinn, 2021).

In parallel, the obligations of data controllers are stipulated in Articles 37 to 47 of the PDP Law. Article 37 obliges data controllers to process personal data lawfully and fairly, while Article 38 requires explicit consent from data subjects. Such consent must be freely given, specific, and based on adequate information, thereby compelling global digital platform companies to adopt transparent and ethical practices toward Indonesian users. Article 40 imposes an obligation on data controllers to ensure the security of personal data and prevent misuse. Additionally, Article 44 mandates that data controllers promptly notify both the data subjects and the competent authority in the event of a personal data breach that may cause harm to data subjects. This requirement demands swift and responsible responses from global digital companies, which in practice often proves difficult when such companies operate outside Indonesian jurisdiction.

Articles 49 and 50 of the PDP Law further emphasize the necessity of international cooperation in the enforcement of personal data protection law. Article 49 provides that Indonesia's personal data protection authority may cooperate with data protection authorities in other countries, including through coordination mechanisms, information exchange, and mutual legal assistance in enforcement actions (Besemer, 2020).

From a practical perspective, despite the clarity of rights and obligations set forth in the PDP Law, its implementation vis-à-vis global digital platforms continues to face significant obstacles (Wahyudi & Adilah, 2024). Major corporations such as Google, Facebook, and Amazon operate complex, transnational data infrastructures and are subject to multiple regulatory regimes, including the General Data Protection Regulation (GDPR) in the European Union, which in some respects adopts standards different from those of the Indonesian PDP Law. Consequently, corporations tend to prioritize regulatory frameworks that are more familiar or economically advantageous, thereby diminishing the effectiveness of personal data protection for Indonesian data subjects (Tjatur et al., 2024). Furthermore, the limited capacity of Indonesian authorities to conduct direct audits or investigations of foreign corporations constrains effective law enforcement.

Accordingly, the successful implementation of the PDP Law with respect to global digital platform providers depends on three principal factors. First, the strengthening of the institutional capacity and authority of Indonesia's personal data protection regulator to conduct supervision and enforcement, including the development of effective international cooperation mechanisms. Second, regulatory harmonization at the international level is necessary to prevent legal fragmentation or conflicts of law that may undermine personal data protection. Third, increased awareness and commitment on the part of global

corporations to comply substantively with the PDP Law, rather than merely adhering to the regulations of their home jurisdictions, is essential.

Nevertheless, it must be emphasized that the PDP Law, in a holistic manner, has established the prerogative rights of individual data subjects and the legal obligations of data controllers, as reflected, inter alia, in Articles 3, 28–35, 37–47, and 49–50. However, cross-jurisdictional complexity remains a fundamental challenge to the effective implementation of personal data protection obligations for global digital service providers. Therefore, a cohesive and integrative strategy—encompassing the consolidation of domestic regulatory frameworks, proactive legal advocacy in the international arena, and collective commitment from multinational corporate actors—is crucial to ensuring optimal personal data protection in Indonesia within an increasingly interconnected and multilayered digital ecosystem.

CONCLUSION

Law Number 27 of 2022 on Personal Data Protection (the PDP Law) has established a comprehensive legal protection framework for the personal data of Facebook users in Indonesia. The provisions contained in Articles 28 to 35 explicitly guarantee the rights of data subjects, including the rights to information, access, rectification, erasure, and objection to the processing of personal data. In addition, Articles 37 to 47 impose obligations on data controllers to process personal data lawfully, transparently, and securely. The incorporation of the extraterritoriality principle under Article 3 extends the scope of legal protection to include global digital platforms that process the personal data of Indonesian citizens. Normatively, therefore, the PDP Law provides greater legal certainty and more robust protective instruments compared to the previous regulatory regime.

With regard to the legal liability of Meta/Facebook as an electronic system operator, the PDP Law clearly establishes obligations concerning data security, mandatory reporting of personal data breaches, and the potential imposition of administrative and criminal sanctions. Although these legal responsibilities are normatively regulated in a firm and explicit manner, their practical implementation continues to encounter significant challenges, particularly due to Meta's transnational operational structure and the limitations of cross-jurisdictional law enforcement mechanisms. Divergences in data protection standards among jurisdictions and the limited capacity of national authorities to conduct direct supervision over foreign entities remain the principal obstacles. Consequently, the effectiveness of Meta's legal accountability is highly dependent on the strengthening of supervisory institutions, enhanced international cooperation, and the company's commitment to complying with the provisions of the PDP Law.

To strengthen the legal protection of Facebook users' personal data under the PDP Law, it is necessary to optimize the implementation of the comprehensively regulated norms. The government should expedite the establishment and operationalization of an independent personal data protection supervisory authority to ensure effective and consistent oversight of data controllers. Furthermore, increased legal socialization and public education regarding data subject rights are essential to enable individuals to actively exercise the available protection mechanisms. The development of implementing regulations and the standardization of technical data security measures are also required to ensure that the

obligations imposed on data controllers are not merely normative in nature but can be concretely and measurably applied in practice.

In order to ensure Meta/Facebook's legal accountability for data breaches affecting users in Indonesia, the enforcement mechanisms applicable to cross-jurisdictional electronic system operators must be strengthened. The Indonesian government should intensify international cooperation, both through bilateral and multilateral agreements, to support the effective enforcement of the extraterritoriality principle enshrined in the PDP Law. In addition, relevant authorities should be vested with stronger powers to conduct compliance audits and investigations of global technology companies. On the other hand, Meta/Facebook is expected to enhance its commitment to compliance with national data protection standards by comprehensively integrating security and privacy principles into its operational systems, thereby ensuring that the protection of Indonesian users' personal data is implemented effectively and sustainably.

REFERENCES

Agustin, D. (2025). *TANGGUNG JAWAB META INCORPORATION ATAS KEBOCORAN DATA PRIBADI TERSIMPAN DI FACEBOOK MENURUT UNDANG-UNDANG NOMOR 27 TAHUN 2022 TENTANG PERLINDUNGAN DATA*. *31*(1), 11286–11299.

Aqilah, R., Waryenti, D., Susanti, P., Tanggung, :, Negara, J., & Pelindungan, M. (2024). Tanggung Jawab Negara Mengenai Pelindungan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Jurnal Ilmiah Kutei*, *23*(2), 158–172. https://doi.org/10.33369/jik.v23i2.34476

Besemer, Leo. (2020). *Privacy And Data Protection*. Van Haren Publishing.

Dayang, S. G., Olivia Putri, S. L., & Kyara Putri, A. K. (2025). Urgensi Pembentukan Lembaga Pengawas dalam Pembaharuan Hukum Perlindungan Data Pribadi Menurut Undang-Undang PDP. *Locus Journal of Academic Literature Review*, *4*(2), 106–113. https://doi.org/10.56128/ljoalr.v4i2.433

Intan, S., Puwa, P., Puluhulawa, F. U., & Rahim, E. I. (2023). GAGASAN IDEAL PENGATURAN PERLINDUNGAN DATA PRIBADI SEBAGAI BENTUK HAK PRIVASI DI INDONESIA. *PALAR (Pakuan Law Review)*, *9*(2), 25–37. https://doi.org/10.33751/palar.v9i2

Khansa Rusyda, N. (2025). Perlindungan Hukum erhadap Subjek Data Kebocoran Data oleh Badan Publik Menurut UU Nomor 27 Tahun 2022. *Desentralisasi : Jurnal Hukum, Kebijakan Publik, dan Pemerintahan*, *2*(3), 247–262. https://doi.org/10.62383/desentralisasi.v2i3.940

Lidya, S., Widayati, S. H., Novianti, M. H., Trias, M. H., Kurnianingrum, P., Luthvi, M. H., Nola, F., Kn, M., & Nadapdap, B. (2020). *POLITIK HUKUM PELINDUNGAN DATA PRIBADI* (B. Nadapdap, Ed.). Yayasan Pustaka Obor Indonesia. http://www.obor.or.id

Mahameru, D. E., Nurhalizah, A., Wildan, A., Haikal Badjeber, M., & Rahmadia, M. H. (2023). IMPLEMENTASI UU PERLINDUNGAN DATA PRIBADI TERHADAP KEAMANAN INFORMASI IDENTITAS DI INDONESIA. *Jurnal Esensi Hukum*, *5*(2), 115–131. https://journal.upnvj.ac.id/index.php/esensihukum/index

Maharani, R., & Prakoso, A. L. (2024). Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital. *Jurnal USM Law Review*, *7*(1), 333–347. https://doi.org/10.58812/jhhws.v2i05.354

Mahendra, G. S. (2024). Perlindungan Hukum Terhadap Korban Yang Data Pribadi Passportnya Tersebar Akibat Kelalaian Pemerintah. *Terang : Jurnal Kajian Ilmu Sosial, Politik dan Hukum*, *1*(3), 104–111. https://doi.org/10.62383/terang.v1i3.382

Matheus, J., & Gunadi, A. (2024). Pembentukan Lembaga Pengawas Perlindungan Data Pribadi Di Era Ekonomi Digital : Kajian Perbandingan Dengan KPPU. *JUSTISI*, *10*(1), 20–35. https://doi.org/10.33506/jurnaljustisi.v10i1.2757

Novel, S., & Subiyanto, A. E. (2025). Perlindungan Hukum terhadap Data Pribadi Konsumen dalam Tindak Pidana Phishing pada Jasa Layanan E-Commerce Tokopedia. *Jurnal Pendidikan Tambusai*, *9*(2), 27617–27626.

Quinn, Brendan. (2021). *Data protection implementation guide : a legal, risk and technology framework for the GDPR*. Kluwer Law International B.V.

R. Syailendra, M., & Fitzgerald, S. E. (2023). SOSIALISASI PERLINDUNGAN DATA PRIBADI BAGI MASYARAKAT KABUPATEN INDRAMAYU. *Jurnal Serina Abdimas*, *1*(1), 157–165. https://doi.org/10.24912/jsa.v1i1.23845

Sa, R., Ahmad, dillah, Ayu Puspaningtyas, D., Nur Karim Al Ismariy, M., & korespondensi, A. (2025). PERLINDUNGAN HUKUM TERHADAP PRIVASI DATA PRIBADI DI ERA DIGITAL. In *THE JURIS: Vol. IX* (Issue 1). http://ejournal.stih-awanglong.ac.id/index.php/juris

Sidi, I., Wiraguna, A., Ars, M., & Barthos, M. (2025). *HUKUM PRIVASI DAN PELINDUNGAN DATA PRIBADI DI INDONESIA* (N. Rismawati, Ed.). WIDINA MEDIA UTAMA. www.freepik.com

Simanjuntak, P. H. (2024). Perlindungan Hukum Terhadap Data Pribadi pada Era Digital di Indonesia: Studi Undang-Undang Perlindungan Data Pribadi dan General Data Protection Regulation (GDPR). *Jurnal Esensi Hukum*, *6*(2), 105–124. https://journal.upnvj.ac.id/index.php/esensihukum/index

Suroso, T., Gede, D., & Yustiawan, P. (2024). HAK SUBJEK DATA PRIBADI SEBAGAI BAGIAN DARI HAK ATAS PRIVASI DAN PENGATURANNYA DI INDONESIA. *Jurnal Kertha Negara*, *12*(7), 798–812. https://databoks.katadata.co.id/datapublish/2022/09/13/indeks-keamanan-

Sutarli, A. F., & Kurniawan, S. (2023). Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi Phising di Indonesia. *Journal Of Social Science Research*, *3*(2), 4208–4221. https://j-innovative.org/index.php/Innovative

Tjatur, H., Irene C, D., Wardhana, B., & Riyanto, G. D. (2024). *Pelindungan Data Pribadi dalam Jurnalisme dan Media* (C. D. Prastuti, Ed.). Asosiasi Media Siber Indonesia. www.amsi.or.id

Wahyudi, E., & Adilah, D. (2024). Doxing in Cyberspace Based on Law No. 27 of 2022 on Personal Data Protection. *Jurnal Idea Hukum*, *10*(2), 149–161. https://doi.org/10.20884/1.jih.2024.10.2.550

Wahyudi, E., Rifqi, D., & Huda, M. (2025). Pelindungan Hukum Atas Data Pribadi Anak dalam Sistem Elektronik: Perspektif UU No. 27 Tahun 2022 Tentang Pelindungan Data Pribadi dan Global. *Policy and Law Journal (Polaw)*, *2*(1), 1–14.