

Original Article

The Integration of Pancasila-Based Justice in the Legal Protection of Specific Personal Data in the Digital Era

Raihan Imam Cahya Akbar¹, **Ramlan²**, **Ida Nadirah³**

^{1,2,3} Faculty of Law, Doctor of Law Program, Muhammadiyah University of North Sumatra, Medan, Indonesia

Correspondence Author: raihanakbar06@gmail.com

Abstract:

The rapid expansion of digital technologies has transformed personal data into a strategic asset, while simultaneously increasing the risk of misuse, particularly concerning specific and sensitive personal data. This article examines the integration of Pancasila-based justice into the legal protection framework for specific personal data in Indonesia. Using a normative juridical method with philosophical and statutory approaches, this study analyzes how the values of Pancasila—especially human dignity, social justice, and democratic governance—are embedded within Law Number 27 of 2022 on Personal Data Protection. The findings reveal that although the Personal Data Protection Law reflects Pancasila values at a normative level, significant challenges remain in its substantive implementation, particularly due to sectoral fragmentation, enforcement limitations, and the asymmetry of power between data controllers and data subjects. This study argues that strengthening the protection of specific personal data requires not only regulatory harmonization but also the reconstruction of enforcement mechanisms grounded in Pancasila-based substantive justice.

Keywords: Pancasila Justice; Personal Data Protection; Specific Personal Data; Substantive Justice; Digital Era.

Introduction

The rapid advancement of digital technology has fundamentally transformed the structure of modern society, particularly in the creation, processing, and utilization of information. Digitalization has permeated almost all spheres of human activity, including governance, economic transactions, healthcare services, education systems, and social interaction. Within this transformation, personal data has evolved into a

strategic resource that supports digital innovation and economic development. At the same time, extensive reliance on data-driven systems has increased individual exposure to privacy violations and unlawful data exploitation. Legal systems are therefore required to respond to the complex interaction between technological progress and the protection of fundamental rights. This condition places personal data protection at the center of contemporary legal discourse. Regulation in this field increasingly reflects a state's commitment to justice and the preservation of human dignity in the digital era.

Specific or sensitive personal data occupies a particularly significant position within personal data protection frameworks. Information relating to health, biometric identifiers, genetic characteristics, religious beliefs, sexual orientation, and financial records carries a heightened risk of harm when misused. The improper processing of such data may generate consequences that extend beyond material loss, including social exclusion, discrimination, and long-term damage to personal dignity. Legal protection for sensitive personal data therefore requires stricter standards than those applied to general personal data. International legal regimes, including the European Union's General Data Protection Regulation, acknowledge this necessity through differentiated protection mechanisms. The rapid expansion of digital platforms and electronic-based services in Indonesia further intensifies the urgency of safeguarding sensitive personal data. These developments require a legal approach oriented toward justice rather than mere formal compliance.

Personal data protection is inherently connected to the protection of fundamental human rights, particularly the right to privacy and personal security. The Indonesian constitutional framework expressly guarantees these rights through Article 28G paragraph (1) of the 1945 Constitution. This provision affirms the right of every individual to protection of personal identity, family, dignity, and property, as well as protection from threats. Personal data, as an extension of individual identity, falls squarely within the scope of constitutional protection. Legal norms governing personal data must therefore be interpreted as part of the broader human rights protection regime. Inadequate legal safeguards may result in constitutional harm, especially where information asymmetries are exploited by state authorities or private entities. Personal data protection thus constitutes a constitutional obligation rather than a purely technical or administrative concern.

Indonesia responded to these constitutional and societal demands through the enactment of Law Number 27 of 2022 on Personal Data Protection. This legislation represents a major development in Indonesian data governance by establishing a comprehensive framework regulating the collection, processing, storage, and dissemination of personal data. The law explicitly distinguishes between general personal data and specific personal data, thereby recognizing the heightened legal risks associated with sensitive information. Core principles such as consent, purpose limitation, data minimization, and accountability are incorporated into the regulatory structure. These principles correspond with widely accepted international data protection standards. Evaluation of the PDP Law cannot be limited to its textual formulation alone. Legal protection must be assessed according to its capacity to realize justice in practice, using a philosophical and constitutional framework grounded in national legal values.

Pancasila, as the philosophical foundation of the Indonesian legal system, articulates a conception of justice that exceeds procedural legality. Justice within the Pancasila framework emphasizes human dignity, equality, and social welfare as substantive legal

objectives. The second principle, *Kemanusiaan yang Adil dan Beradab*, requires respect for human dignity and prohibits the reduction of individuals to instruments of economic or political interests. Application of this principle to personal data protection demands recognition of individuals as rights-bearing legal subjects rather than passive data objects. The fifth principle, *Keadilan Sosial bagi Seluruh Rakyat Indonesia*, obliges the state to ensure equitable legal protection across all segments of society. These principles establish justice as a moral and social mandate of law, rather than a purely formal requirement.

Implementation of the PDP Law reveals a number of structural and normative challenges that limit the realization of substantive justice. A persistent imbalance of power exists between data controllers and data subjects. Large corporations and public institutions possess technological, economic, and informational advantages that significantly exceed those of individual data subjects. Consent mechanisms, although legally mandated, frequently operate under conditions of informational inequality that weaken genuine autonomy. Under such conditions, consent may function as a symbolic formality rather than an effective safeguard. Pancasila-based justice requires legal protection that addresses structural inequality and preserves human dignity. Legal norms that fail to correct power imbalances cannot be regarded as substantively just.

Institutional capacity and enforcement mechanisms constitute a further dimension that influences the effectiveness of justice-based personal data protection. Legal norms, regardless of their philosophical coherence, require effective institutional structures to ensure compliance and accountability. Limitations in supervisory authority, coordination gaps among regulatory bodies, and restricted access to remedies weaken the practical realization of personal data rights. Data subjects often encounter procedural and informational barriers when seeking redress for data protection violations. Such conditions diminish the deterrent effect of the law and reduce public confidence in legal protection mechanisms. Pancasila-based justice requires not only normative recognition of rights but also institutional arrangements capable of enforcing those rights equitably. Strengthening oversight institutions and ensuring accessible enforcement procedures therefore becomes integral to the realization of substantive justice in personal data governance.

Fragmentation of data protection regulation across sectors constitutes another significant obstacle. Financial services, healthcare, education, and digital commerce remain subject to sector-specific regulatory regimes that apply differing standards of personal data protection. Such fragmentation generates inconsistency in enforcement and uncertainty for both data controllers and data subjects. Supervisory authorities encounter difficulties in ensuring uniform compliance across diverse regulatory environments. Unequal levels of protection undermine the principle of equality before the law. From the perspective of Pancasila, regulatory disparity contradicts the mandate of social justice for all citizens. Harmonization of sectoral regulations therefore represents a necessary condition for justice-oriented data protection.

Cross-border data flows further complicate the protection of personal data in the digital era. Personal data belonging to Indonesian citizens is frequently processed and stored outside national jurisdiction, particularly by multinational technology corporations. This situation raises complex legal issues concerning jurisdiction, enforcement, and accountability. Provisions governing cross-border data transfers exist within the PDP Law, yet enforcement capacity remains limited. Absence of effective international cooperation exposes sensitive personal data to transnational power

structures beyond domestic oversight. Justice cannot be secured solely through territorial regulation under these conditions. A Pancasila-based approach requires active state involvement in safeguarding human dignity within global digital ecosystems.

Existing legal scholarship on personal data protection in Indonesia has primarily focused on doctrinal interpretation, sectoral compliance, or comparative regulatory analysis. Such studies provide important insights into regulatory development but often insufficiently engage with justice as a substantive evaluative framework. Limited attention has been given to Pancasila as an operational legal standard for assessing data protection effectiveness. Many analyses position Pancasila as a symbolic or ideological reference rather than a normative tool for legal evaluation. This orientation constrains critical examination of whether existing regulations adequately protect human dignity and social equality. A significant research gap therefore exists in integrating Pancasila-based justice into the analysis of specific personal data protection.

This article addresses that gap by positioning Pancasila-based justice as an analytical framework for evaluating the legal protection of specific personal data in the digital era. The central inquiry examines how justice, as conceptualized within Pancasila, may be substantively integrated into data protection law. Emphasis is placed on substantive outcomes rather than procedural compliance alone. A normative juridical method grounded in statutory and philosophical analysis is employed to examine both the strengths and limitations of the PDP Law. This approach facilitates assessment of the law's coherence with constitutional values. The analysis advances a justice-oriented critique that moves beyond descriptive evaluation.

The objectives of this research are threefold. Analysis is directed toward identifying the extent to which the PDP Law embodies Pancasila-based justice within its normative structure. Structural and institutional barriers hindering realization of substantive justice in protecting specific personal data are subsequently examined. Reconstruction of personal data protection law aligned with Pancasila values is proposed as a normative response. Such reconstruction seeks to ensure that legal protection does not merely promote administrative efficiency or economic interests. Law is instead positioned as an instrument for safeguarding human dignity and social equality. These objectives reflect an effort to align digital governance with constitutional morality.

Contribution of this study extends to both national and international legal discourse on personal data protection. At the national level, a normative foundation is offered for strengthening implementation of the PDP Law in accordance with Indonesia's constitutional identity. At the international level, the study demonstrates how indigenous legal philosophies may enrich global debates on data governance and digital rights. Contemporary data protection regimes are frequently shaped by technocratic or market-oriented considerations. Integration of justice-based values provides a corrective to such tendencies. Pancasila is therefore positioned as a practical legal framework capable of addressing contemporary digital challenges, reaffirming personal data protection as an essential component of justice in the digital era.

Methods

This study employs a normative juridical method, which is particularly appropriate for examining legal norms, principles, and values governing the protection of personal data within the Indonesian legal system. Normative juridical research conceptualizes law as a system of norms that prescribes standards of conduct while embodying underlying philosophical and constitutional values. This methodological approach enables the

analysis of personal data protection not merely as a technical regulatory mechanism, but as an expression of justice within a constitutional and philosophical framework. The normative juridical method is especially relevant to this research, as it seeks to assess the coherence between statutory regulation and Pancasila-based justice. Through this approach, the study critically evaluates the extent to which existing legal norms ensure substantive and equitable protection of specific personal data. The method allows for a systematic examination of law as both a normative structure and a justice-oriented institution.

A statutory approach is applied by examining Law Number 27 of 2022 on Personal Data Protection (PDP Law) as the primary legal instrument governing personal data protection in Indonesia. This approach involves a systematic analysis of statutory provisions relating to the classification, processing, and safeguarding of personal data, with particular emphasis on specific and sensitive categories of data. Relevant constitutional provisions, notably Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, are analyzed to establish the constitutional foundation of privacy and personal data protection. Implementing regulations and sectoral legal instruments are also examined to identify normative coherence as well as potential regulatory fragmentation. Through statutory analysis, the study assesses whether existing legal norms adequately reflect justice-oriented protection for data subjects. This approach further serves to identify regulatory gaps and structural limitations in enforcement.

A philosophical approach is employed to analyze justice through the values embodied in Pancasila as the foundational philosophy of the Indonesian legal system. This approach situates legal norms within a broader ethical and constitutional context, emphasizing that law functions as an instrument for realizing human dignity, equality, and social justice. Particular attention is given to the second principle of Pancasila, *Kemanusiaan yang Adil dan Beradab*, which affirms respect for human dignity and individual autonomy, and the fifth principle, *Keadilan Sosial bagi Seluruh Rakyat Indonesia*, which mandates equitable legal protection for all members of society. Examination of these principles provides a normative benchmark for evaluating personal data protection law. The philosophical approach enables the study to move beyond formal legality and assess the moral legitimacy of regulatory arrangements. Within this framework, Pancasila is positioned as an operational standard for legal evaluation rather than a symbolic or ideological reference.

A conceptual approach is also applied to clarify and analyze key legal concepts relevant to the study, including personal data, specific personal data, consent, privacy, substantive justice, and human rights protection. Conceptual analysis is necessary to ensure terminological precision and theoretical consistency, particularly in a legal field characterized by the intersection of law and digital technology. Substantive justice is examined as distinct from procedural or formal justice, with emphasis placed on legal outcomes that genuinely protect human dignity rather than mere regulatory compliance. This approach facilitates understanding of personal data protection as an integral component of the broader human rights framework. Clarification of these concepts establishes clear evaluative criteria for assessing the adequacy of legal protection. The conceptual approach thereby enhances the analytical depth and coherence of the research.

The legal materials utilized in this study consist of primary and secondary legal sources. Primary legal materials include the 1945 Constitution of the Republic of

Indonesia and Law Number 27 of 2022 on Personal Data Protection, which serve as the principal normative references for constitutional rights and statutory obligations. Secondary legal materials comprise scholarly books, peer-reviewed journal articles, and authoritative legal commentaries addressing Pancasila, theories of justice, personal data protection, human rights, and digital governance. These sources provide doctrinal interpretation, theoretical insight, and contextual analysis relevant to justice-oriented data protection. Selection of secondary materials is based on relevance, academic credibility, and contribution to the development of legal discourse. Collectively, these materials form a comprehensive foundation for normative legal analysis.

Analysis of legal materials is conducted through qualitative and prescriptive legal reasoning. Legal norms are interpreted and systematized to identify their underlying principles, objectives, and internal coherence. These norms are subsequently evaluated against the values of Pancasila-based justice and human rights protection. Identification of normative inconsistencies or regulatory gaps forms the basis for prescriptive legal arguments aimed at strengthening the protection of specific personal data. The prescriptive dimension of this research reflects the core function of normative juridical inquiry, which seeks not only to describe existing law but also to propose improvements consistent with constitutional values. Through this analytical process, the study contributes to the development of a justice-oriented framework for personal data protection in Indonesia.

Results

Normative Recognition of Pancasila-Based Justice in the Personal Data Protection Law

The results of this study demonstrate that Law Number 27 of 2022 on Personal Data Protection (PDP Law) normatively integrates Pancasila-based justice through its recognition of personal data protection as a fundamental right intrinsically linked to human dignity and personal autonomy. This normative orientation is evident in the legal construction of personal data as an extension of individual identity rather than as a mere economic commodity. By framing personal data protection within a rights-based paradigm, the PDP Law departs from a purely administrative or managerial model of regulation. Such positioning aligns with the second principle of Pancasila, *Kemanusiaan yang Adil dan Beradab*, which requires the law to uphold the intrinsic worth of every individual. Protection of personal data is therefore situated within a moral and constitutional framework. This approach reflects an understanding that technological governance must remain subordinate to human dignity.

A central manifestation of this justice-oriented framework is the explicit differentiation between general personal data and specific personal data. The PDP Law acknowledges that certain categories of data—such as health, biometric, genetic, religious, and financial data—carry a heightened risk of harm if misused. This differentiation indicates a normative awareness that equal treatment of unequal risks would undermine justice. From a Pancasila perspective, such differentiation is consistent with substantive justice, which demands proportional legal protection based on vulnerability and potential harm. The law thereby rejects a uniform regulatory approach in favor of differentiated safeguards. This normative choice reflects sensitivity to social realities and individual vulnerability. Differentiated protection thus functions as a justice mechanism rather than a technical classification.

The PDP Law also incorporates fundamental principles of data protection, including

lawfulness, fairness, transparency, purpose limitation, data minimization, and accountability. These principles serve as normative constraints on the power of data controllers and aim to prevent arbitrary or exploitative data processing practices. Within the framework of Pancasila-based justice, these principles operate as instruments for balancing competing interests between individuals and institutional actors. This balance resonates with the fifth principle of Pancasila, *Keadilan Sosial bagi Seluruh Rakyat Indonesia*, which requires equitable protection and fair distribution of legal burdens and benefits. Justice, in this sense, is embedded within the structure of legal obligations imposed on data controllers. However, such embedding remains largely normative in nature.

In addition, the normative structure of the PDP Law reflects an implicit constitutionalization of personal data protection within Indonesia's legal system. By situating personal data within the realm of fundamental rights, the law reinforces the constitutional hierarchy that places human dignity above economic or administrative efficiency. This constitutional orientation strengthens the legitimacy of personal data protection as a core obligation of the state. Within the Pancasila framework, law functions not merely as an instrument of governance but as a moral expression of collective values. The PDP Law therefore operates as a vehicle for translating constitutional morality into the digital context. This normative positioning enhances the authority of data protection law as a justice-oriented regime.

The findings also suggest that the PDP Law reflects a cautious legislative effort to reconcile global data protection standards with Indonesia's constitutional identity. Adoption of principles comparable to those found in international regimes demonstrates openness to transnational legal norms. Anchoring these principles within Pancasila-based justice preserves national philosophical coherence. This hybrid normative construction positions Indonesia's data protection regime as neither purely transplanted nor entirely insular. Pancasila serves as a mediating framework that contextualizes global norms within domestic constitutional values. Such contextualization is essential for maintaining legitimacy in a plural legal environment.

Despite this normative alignment, the study finds that the PDP Law largely articulates justice at the level of principles rather than operational enforcement. Many justice-oriented provisions remain framed in general terms that lack concrete implementation standards. This formulation allows interpretative discretion that may favor powerful data controllers. Normative justice without enforceable institutional mechanisms risks remaining aspirational. In the Pancasila framework, justice requires institutional realization, not merely moral declaration. A legal framework lacking effective enforcement capacity cannot fully embody substantive justice.

Overall, the PDP Law demonstrates a strong normative commitment to Pancasila-based justice by embedding dignity, fairness, and proportionality into its legal structure. Personal data protection is conceptualized as a matter of rights rather than regulatory convenience. Nevertheless, translation of these justice values into enforceable standards remains incomplete. Justice appears more prominently as a guiding value than as an operational benchmark. This condition underscores the need for deeper institutionalization of Pancasila-based justice within the personal data protection regime.

Substantive Justice, Power Asymmetry, and the Protection of Specific Personal Data

Analysis of the PDP Law reveals that substantive justice in the protection of specific personal data is significantly constrained by structural power asymmetries inherent in contemporary digital governance. Data controllers, particularly large technology corporations, financial institutions, and public authorities, possess extensive technological, informational, and economic resources. Data subjects frequently lack sufficient knowledge and bargaining power to influence data processing practices. This imbalance creates conditions in which legal safeguards operate only formally. Substantive justice requires not merely recognition of rights but also the capacity to exercise them effectively. Power asymmetry therefore constitutes a central obstacle to justice-oriented data protection.

Consent functions as a primary mechanism legitimizing data processing under the PDP Law. While formally required, consent often operates within contexts of informational inequality and standard-form contractual arrangements. Such conditions restrict genuine choice and undermine autonomy. Consent under these circumstances functions as procedural compliance rather than a meaningful expression of will. From a Pancasila-based justice perspective, this condition compromises human dignity. Justice requires legal mechanisms that acknowledge unequal bargaining positions. Reliance on formal consent without corrective safeguards weakens substantive protection.

Substantive justice in personal data protection also depends on the ability of legal norms to address systemic inequalities embedded in digital infrastructures. Technological systems are designed and controlled by actors with concentrated economic and technical power. These systems shape data processing practices in ways largely invisible to users. Legal protection focused solely on individual consent fails to address these systemic dimensions. Pancasila-based justice requires recognition of structural conditions influencing autonomy. Without addressing systemic inequality, legal protection remains formal rather than transformative.

The findings further indicate that enforcement mechanisms do not sufficiently reflect the differentiated risks associated with specific personal data. Sanctions and enforcement practices often fail to correspond to the severity of harm arising from misuse of sensitive data. Violations involving sensitive personal data are frequently treated similarly to general data breaches. This approach contradicts the principle of proportionality, which is central to substantive justice. Pancasila-based justice requires calibrated legal responses based on harm severity and social impact. Absence of differentiated enforcement undermines effective protection.

The analysis also highlights the importance of accountability mechanisms in correcting power imbalances. Accountability extends beyond formal compliance to include oversight, transparency, and sanctions proportionate to harm. Weak accountability allows data controllers to retain disproportionate control over personal data. This condition undermines the corrective function of law. Pancasila-based justice requires accountability as a tool for rebalancing social relations. Strengthened accountability reinforces public trust and affirms individuals as rights holders.

Preventive measures constitute another essential component of substantive justice. Principles such as privacy by design and privacy by default embed protection within technological systems. The PDP Law places limited emphasis on such preventive obligations. Lack of preventive integration results in a reactive regulatory model that addresses harm only after violations occur. Reactive protection is inherently insufficient

for safeguarding sensitive personal data. Justice-oriented regulation must therefore prioritize prevention alongside remediation.

Collectively, the findings indicate that substantive justice in protecting specific personal data has not yet been fully realized. Power asymmetries, reliance on formal consent, limited preventive obligations, and weak accountability mechanisms undermine effective protection. Pancasila-based justice requires law to actively correct inequality rather than merely acknowledge rights. Achievement of substantive justice necessitates stronger institutional safeguards and accountability frameworks.

Social Justice, Regulatory Fragmentation, and the Need for Justice-Oriented Reconstruction

Regulatory fragmentation emerges as a critical impediment to achieving social justice in personal data protection. Although the PDP Law operates as a general framework, sector-specific regulations continue to govern data processing in healthcare, finance, education, and electronic commerce. These regimes apply divergent standards of protection and enforcement. Individuals consequently experience unequal levels of legal protection depending on the sector in which their data is processed. Such disparity undermines equality before the law. From a Pancasila perspective, this condition contradicts the mandate of *Keadilan Sosial bagi Seluruh Rakyat Indonesia*.

Fragmentation also complicates institutional enforcement and weakens regulatory coherence. Supervisory authorities face difficulties coordinating oversight across regimes with differing standards and mandates. Enforcement gaps created by regulatory complexity may be exploited by powerful data controllers. Ordinary citizens face increased difficulty in understanding and enforcing their rights. Justice-oriented regulation requires coherence, accessibility, and predictability. Fragmentation undermines these foundational attributes of justice.

Social justice in personal data protection also requires equal access to remedies and complaint mechanisms. Fragmented regulation often produces uneven procedural pathways for dispute resolution across sectors. Individuals subjected to data misuse may encounter different standards and procedures depending on regulatory context. Such disparity undermines equal access to justice. Pancasila-based justice emphasizes equality not only in substantive norms but also in access to legal protection. Uniform and accessible remedies therefore constitute an essential component of social justice.

Cross-border data flows further intensify these challenges. Digital economic activities enable personal data to move seamlessly across national boundaries. Enforcement of domestic standards becomes increasingly difficult when data is processed under foreign jurisdictions. Although the PDP Law contains provisions on cross-border data transfers, enforcement capacity remains limited. Multinational corporations may subject Indonesian citizens' data to weaker regulatory regimes. Pancasila-based justice imposes a moral obligation on the state to safeguard dignity regardless of jurisdiction.

The need for justice-oriented reconstruction also arises from the dynamic nature of digital risks. Technological development continuously generates new forms of data processing and threats to personal dignity. Static regulatory models are insufficient to address evolving risks. Reconstruction of personal data protection law must therefore incorporate adaptive and forward-looking mechanisms. Pancasila-based justice provides a normative compass for guiding such adaptation. Legal reconstruction grounded in dignity and social equality ensures responsiveness without sacrificing moral coherence.

The findings indicate that realization of social justice requires reconstruction of the legal framework oriented toward substantive outcomes. Harmonization of sectoral regulations under a unified justice-based standard is essential. Strengthening supervisory institutions and enhancing international cooperation are equally necessary. Justice cannot be achieved through fragmented and reactive regulation. A coherent and proactive framework is required to ensure equal protection for all citizens.

The discussion ultimately demonstrates that personal data protection in Indonesia stands at a critical normative and institutional juncture. The PDP Law reflects justice-oriented values, yet implementation remains uneven and constrained. Without structural reform, justice risks remaining symbolic. Integration of Pancasila-based justice into enforcement, institutional design, and regulatory coherence is indispensable. Only through such integration can personal data protection fulfill its constitutional and moral function in the digital era.

Conclusion

This study concludes that Law Number 27 of 2022 on Personal Data Protection has normatively embedded Pancasila-based justice within Indonesia's legal framework by recognizing personal data as an extension of human dignity and constitutional rights; however, such integration remains predominantly formal and has not yet materialized into substantive justice in practice, particularly in the protection of specific personal data. Structural power asymmetries between data controllers and data subjects, overreliance on consent-based mechanisms, fragmented sectoral regulation, and limited preventive and enforcement capacities significantly constrain the law's effectiveness. From a Pancasila-based perspective, justice requires more than procedural legality, demanding legal arrangements that actively correct inequality, ensure proportional protection, and safeguard human dignity within evolving digital environments. The findings therefore underscore the necessity of reconstructing personal data protection law through strengthened accountability, regulatory harmonisation, preventive safeguards, and institutional capacity building. Integration of Pancasila-based justice at both normative and operational levels is essential for transforming personal data protection from a declaratory legal framework into an effective instrument of constitutional justice in the digital era.

References

- Abdillah, I., et al. (2024). Pancasila sebagai pedoman dasar dalam perlindungan hukum terhadap hak asasi manusia. *Jurnal Moralita: Jurnal Pendidikan Pancasila dan Kewarganegaraan*, 5(2), 57–63.
- Almahdali, H., et al. (2024). Pendidikan Pancasila dan kewarganegaraan. Agam: Yayasan Tri Edukasi Ilmiah.
- Astuti, et al. (2023). *Keamanan data dalam revolusi teknologi*. Jakarta: Prenadamedia Group.
- Chaturvedi, A. (2023). Controversies in the personal data protection bill: Government exemptions, data localization, and the right to be forgotten. *International Journal of Law, Management & Humanities*, 6(3), 789–806.
- Denindah, O., Rosadi, S. D., & Permata, R. R. (2020). Personal data protection in health surveillance applications: A comparative study of Indonesia and Australia. *DATIN Law Journal*, 1(2), 1–15.
- European Union. (2016). General Data Protection Regulation (Regulation (EU) 2016/679).
- Hadiyantina, S., et al. (2023). Perlindungan data pribadi dalam bidang rekam medis.

- Malang: Universitas Brawijaya Press.
- Huda, U. N., et al. (2024). *Data pribadi, hak warga, dan negara hukum: Menjaga privasi di tengah ancaman digital*. Bandung: Widina.
- Ikrom, M. B. F. D., & Tamam, B. (2024). Legal protection of privacy rights in personal data breaches in Indonesia. *Constitution Journal*, 3(2), 139–154.
- Indriani, M., & Putri, A. A. (2023). Dynamic consent as an instrument for optimizing personal data protection and privacy rights. *Jurnal HAM*, 14(2), 201–215.
- Kanaya, S., Husna, I., & Najicha, F. U. (2023). Pancasila and human rights in Indonesia. *JCE: Jurnal Civic Education*, 7(2), 104–112.
- Kamarulzaman, M. S., & Yusuf, H. (2024). Legal analysis of doxing crimes under Indonesia's personal data protection law. *JICN: Jurnal Intelek dan Cendekiawan Nusantara*, 1(2), 2442–2456.
- Matheus, J., & Gunadi, A. (2024). Establishment of personal data protection supervisory authority in the digital economy era. *Justisi*, 10(1), 1–15.
- Mangaluk, E., Sepriano, S., & Nasrullah, A. (2025). *Wawasan Pancasila*. Jambi: Sonpedia Publishing Indonesia.
- Putri, D. D. F., & Fahrozi, M. H. (2021). Preventive measures against consumer data breaches through personal data protection law. *Borneo Law Review*, 5(1), 46–68.
- Ramadhani, W. K. S., & Wiraguna, S. A. (2025). Implementation of personal data protection in financial information systems. *Perspektif Administrasi Publik dan Hukum*, 2(2), 158–175.
- Rawls, J. (1999). *A theory of justice* (Revised ed.). Cambridge, MA: Harvard University Press.
- Rosadi, S. D. (2021). *Perlindungan data pribadi di Indonesia*. Yogyakarta: Genta Publishing.
- Situmeang, S. M. T. (2021). Personal data misuse as a perfect cybercrime. *SASI*, 27(1), 38–52.
- Utama, M. W. (2024). Rekonstruksi regulasi perlindungan data pribadi berbasis nilai keadilan. Semarang: Universitas Islam Sultan Agung.
- Yamani, A. Z. (2025). Regulatory challenges in law-making during digital transformation. *Journal of Law and Nation*, 4(2), 312–324.
- Yulianingsih, S., & Putra, R. K. (2024). Legal protection of consumers in e-commerce transactions in Indonesia. *Hakim: Jurnal Ilmu Hukum dan Sosial*, 2(4), 842–856.