p-ISSN 2337-6368 | e-ISSN 2615-4439
https://jurnal.ugj.ac.id/index.php/HERMENEUTIKA

LEGAL PROTECTION AGAINST MISUSE OF PERSONAL DATA OF FINANCIAL TECHNOLOGY (FINTECH) USERS IN THE INDONESIAN LEGAL SYSTEM: A NORMATIVE ANALYSIS

[1]Taupan Selamat Wibawa, [2]Endang Sutrisno, [3]Sanusi
Master of Law Study Program, Swadaya Gunung Jati University
Email : [1] taupan1707@gmail.com , [2] endang.sutrisno@ugj.ac.id, [3] sanusi@ugj.ac.id

DOI: https://doi.org/10.33603/hermeneutika.v10i2.12513
Diterima: 7 Juli 2026 ; Direvisi: 11 Juli 2026; Dipublikasikan: 12 Juli 2026

Abstract *The development of Financial Technology (Fintech) services in Indonesia has driven the transformation of the financial services sector through ease of access, transaction efficiency, and increased financial inclusion. On the other hand, large-scale processing of users' personal data poses various legal risks, particularly data misuse, unauthorized access, data leaks, and data utilization without user consent. These conditions indicate that personal data protection is a fundamental aspect in ensuring legal certainty, privacy rights, and public trust in the Fintech ecosystem. This study aims to analyze the forms of legal protection against misuse of Fintech users' personal data and examine its legal provisions in the Indonesian legal system. The study uses a normative juridical method with a statutory approach, a conceptual approach, and an analytical approach. The legal materials used consist of primary, secondary, and tertiary legal materials analyzed qualitatively using a prescriptive method. The research results show that legal protection for Fintech users' personal data is realized through preventive and repressive mechanisms. Preventive protection includes the obligation to obtain valid consent, the application of transparent data processing principles, restrictions on the purposes of data use, the application of information security standards, and the fulfillment of data subjects' rights. Repressive protection is realized through dispute resolution mechanisms, the imposition of administrative sanctions, civil liability, and criminal sanctions against perpetrators of personal data misuse, as stipulated in Law Number 27 of 2022 concerning Personal Data Protection, which complements the regulatory framework for the digital financial services and electronic transactions sector. However, the implementation of legal protection still faces various obstacles, including the suboptimal harmonization of sectoral regulations, supervisory challenges, and the need to strengthen compliance of Fintech providers with personal data protection governance principles. Therefore, strengthening regulatory synchronization, effective supervision, and increasing compliance of Fintech providers are necessary to realize legal protection that provides certainty, fairness, and benefits for users of digital financial services.*

Keywords: *Legal Protection; Personal Data; Financial Technology (Fintech); Personal Data Protection; Indonesian Legal System.*

p-ISSN 2337-6368 | e-ISSN 2615-4439
https://jurnal.ugj.ac.id/index.php/HERMENEUTIKA

I. INTRODUCTION

The development of information and communication technology has driven a significant transformation in the financial services sector through the emergence of Financial Technology (Fintech). The digitalization of financial services has not only shifted people's transaction patterns from conventional to electronic systems but has also given rise to new business models that prioritize speed, efficiency, accessibility, and innovation. Fintech has become a crucial instrument in supporting national financial inclusion through the provision of various services, such as digital payments, peer-to-peer lending, crowdfunding, digital investment, wealth management, and artificial intelligence-based financial services. This development aligns with Indonesia's digital economic transformation agenda, which positions technology as an instrument for national economic development. However, despite these benefits, Fintech operations rely heavily on the collection, processing, storage, and utilization of large amounts of user personal data, giving rise to various legal risks that require adequate regulation and protection (Rosadi, 2021; Budhijanto, 2024; Aldboush & Ferdous, 2023).

Personal data in the Fintech ecosystem has evolved into an economic asset with strategic value for digital financial service providers. All user activities, from registration and identity verification (Know Your Customer/KYC), transaction history, location, electronic devices, and digital consumption patterns, are processed to support risk analysis, creditworthiness assessments, and the development of algorithm-based services. This situation means that personal data is no longer viewed solely as a person's identity, but rather as a digital commodity with high economic value. Consequently, the risk of data misuse is increasing, including excessive data collection (over-collection), unauthorized use of data, dissemination to third parties, and data leaks due to weak information security systems. This phenomenon demonstrates that personal data protection has become an integral part of human rights protection, particularly the rights to privacy and information security (Westin, 1967; European Union, 2016; Rosadi, 2015).

Constitutionally, protection of personal data is rooted in the guarantee of human rights as stipulated in Article 28G paragraph (1) and Article 28H paragraph (4) of the 1945 Constitution of the Republic of Indonesia, which guarantees personal protection, a sense of security, and the right to private property. From the perspective of a state based on law (rechtstaat), protection of personal data is a manifestation of the state's obligation to provide legal certainty, justice, and protection of citizens' rights from various forms of abuse by the state and business actors. Therefore, regulations regarding the protection of personal data are not only oriented towards administrative aspects, but also constitute a legal instrument aimed at maintaining a balance between the interests of the digital economy and the protection of people's constitutional rights. (Rosadi, 2021; Budhijanto, 2024; Nonet & Selznick, 1978).

In response to this need, Indonesia has established Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) as the basis for national law which regulates the rights of personal data subjects, obligations of data controllers and processors, data processing mechanisms, data transfer, dispute resolution, administrative sanctions, and criminal provisions. The presence of the PDP Law is an important milestone in the formation of a personal data protection regime in Indonesia because for the first time regulations that were previously spread across various sectoral regulations were consolidated into one comprehensive law. This law also emphasizes that personal data protection is an overall effort to protect personal data in the data processing chain in order to guarantee the constitutional rights of personal data subjects. (Westin, 1967; European Union, 2016; Rosadi, 2015).

However, the PDP Law has not fully addressed the various legal issues that arise in Fintech practices. The rapidly evolving nature of the Fintech industry often outstrips the regulatory capacity to address various forms of data misuse. These issues include consent mechanisms that do not fully comply with the principle of explicit consent, the use of data for commercial purposes without adequate transparency, data exchange with third parties, the use of algorithms in credit scoring, and weak cybersecurity governance. Furthermore, the implementation of data protection norms still faces challenges in the form of harmonization of sectoral regulations, effective oversight, and compliance by Fintech operators with personal data protection principles (Rohendi & Kharisma, 2024; Rosadi, 2015; European Union, 2016).

From the perspective of legal protection theory as proposed by Philipus M. Hadjon (1987), legal protection consists of preventive and repressive legal protection. Preventive protection provides the public with the opportunity to obtain legal guarantees before violations occur through the regulation of rights, obligations, and oversight mechanisms. Meanwhile, repressive protection is realized through dispute resolution, sanctions, and restoration of rights after violations occur. This concept is highly relevant for the protection of Fintech users' personal data, considering that data breaches not only cause economic losses but also threaten the right to privacy, digital security, reputation, and even individual freedom in utilizing digital financial services (European Union, 2016; Aldboush & Ferdous, 2023).

On the other hand, the theory of legal certainty developed by Gustav Radbruch emphasizes that the law must provide clarity of norms, consistency of regulations, and guarantee the protection of public rights. In the context of Fintech, legal certainty is a crucial prerequisite for building public trust in the digital financial system. Without certainty regarding the management of personal data, the public will lose a sense of security when using Fintech services, which could ultimately hinder the growth of the national digital economy. Therefore, personal data protection should not only be understood as an information technology issue, but also as part of developing a national legal system that is responsive to technological developments (Friedman, 1975; Nonet & Selznick, 1978).

Much research has been conducted on personal data protection in the Fintech sector, but most of it focuses on the technical implementation of information security, consumer protection, or analysis of specific provisions in the Personal Data Protection Law (PDP). This research has a distinct focus because it comprehensively analyzes the forms of legal protection against misuse of Fintech users' personal data through a normative legal perspective by examining the synchronization of various legal instruments governing personal data protection within the Indonesian legal system. The analysis examines the relationship between the PDP Law, the legal regime for electronic transactions, and the regulation of the digital financial services sector to assess the extent

p-ISSN 2337-6368 | e-ISSN 2615-4439
https://jurnal.ugj.ac.id/index.php/HERMENEUTIKA

to which the Indonesian legal system has provided legal certainty regarding the protection of Fintech users' personal data (Mahfud MD, 2017; Friedman, 1975; Budhijanto, 2024).

Based on this description, this study focuses on the forms of legal protection against misuse of personal data by Financial Technology (Fintech) users and how this legal protection is regulated within the Indonesian legal system. The research findings are expected to provide theoretical contributions to the development of personal data protection law and serve as recommendations for policymakers in realizing a legal system that is adaptive to the development of the digital economy, oriented towards legal certainty, justice, and the protection of the public's constitutional rights. (Mahfud MD, 2017; Nonet & Selznick, 1978; Budhijanto, 2024; Rosadi, 2021).

II. RESEARCH METHODS

This research employs a normative legal research or doctrinal legal research method. This method was chosen because the research focuses on analyzing legal norms governing the protection of personal data of Financial Technology (Fintech) users, as well as examining the suitability, consistency, and effectiveness of legal regulations in providing protection against personal data misuse within the Indonesian legal system. Normative legal research views law as a system of norms (law as it is written in the books) consisting of principles, rules, doctrines, and regulations that are interrelated in forming a legal system. This approach aims to identify legal reasoning, legal principles, and legal concepts that can be used to address research questions regarding the form of legal protection against misuse of personal data of Fintech users (Marzuki, 2021).

1. Types of research

The type of research used is normative legal research with a prescriptive-analytical character. Prescriptive research aims to provide arguments regarding what should (das sollen) be done by policymakers and Fintech service providers to ensure legal protection for users' personal data. This research not only describes applicable legal provisions but also analyzes weaknesses in norms, identifies legal vacuums, regulatory disharmony, and formulates a concept for strengthening legal regulations that can provide legal certainty, justice, and benefit to the community.

The analytical nature of this research is demonstrated through an examination of the relationship between various legal instruments governing personal data protection, consumer protection, electronic transactions, and the digital financial services sector. The analysis aims to determine whether the Indonesian legal system provides adequate legal protection against the risk of personal data misuse in the provision of fintech services.

2. Research Approach

To obtain a comprehensive analysis, this research uses several approaches as follows.

1) Statute Approach

A legislative approach was used to examine all legal provisions relating to the protection of Fintech users' personal data. The analysis was conducted on the hierarchy of laws and regulations to determine vertical and horizontal synchronization between regulations.

Regulations that are the object of study include:

- The 1945 Constitution of the Republic of Indonesia;

p-ISSN 2337-6368 | e-ISSN 2615-4439
https://jurnal.ugj.ac.id/index.php/HERMENEUTIKA

- Law Number 27 of 2022 concerning Personal Data Protection;
- Law Number 11 of 2008 concerning Electronic Information and Transactions, as last amended by Law Number 1 of 2024;
- Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions;
- Financial Services Authority Regulations concerning the implementation of technological innovation in the financial sector and consumer protection;
- Bank Indonesia Regulations relating to digital payment systems;
- Other regulatory provisions relating to cybersecurity and consumer protection.

This approach aims to determine the consistency of legal norms in providing protection for Fintech users' personal data.

2) Conceptual Approach

The conceptual approach is used to study legal concepts that develop in legal doctrine regarding:

- Legal protection;
- Right to privacy;
- Right to personal data;
- Information security;
- Digital consumer protection;
- Legal responsibility of fintech providers;
- Accountability principle;
- Prudential principle;
- Data governance.

This approach is carried out by examining the opinions of national and international legal experts so that a legal concept is obtained that can be used as a basis for analysis of the regulation of personal data protection in the Indonesian legal system..

3) Analytical Approach

An analytical approach was used to describe and evaluate the substance of legal norms governing the protection of Fintech users' personal data.
The analysis was conducted on:

- Rights of personal data subjects;
- Obligations of personal data controllers;
- Obligations of personal data processors;
- Consent mechanisms;
- Data processing;
- Data transfer;
- Data storage;
- Data deletion;
- Dispute resolution mechanisms;
- Administrative sanctions;
- Civil sanctions;
- Criminal sanctions.

Through this approach, it will be known to what extent legal norms have been able to provide legal certainty regarding the protection of Fintech users' personal data.

4) Comparative Approach

p-ISSN 2337-6368 | e-ISSN 2615-4439
https://jurnal.ugj.ac.id/index.php/HERMENEUTIKA

To enrich the analysis, this study uses a comparative approach, comparing Indonesia's personal data protection regime with several countries with more advanced data protection systems, such as the European Union's General Data Protection Regulation (GDPR) and Singapore's Personal Data Protection Act (PDPA). This approach aims to identify best practices that can serve as references in developing national regulations.

3. Types and Sources of Legal Materials

Normative legal research uses legal materials as the main source of research.

1) Primary Legal Materials

Primary legal materials consist of all laws and regulations that have binding legal force, including:

- The 1945 Constitution of the Republic of Indonesia;
- Law Number 27 of 2022 concerning Personal Data Protection;
- Electronic Information and Transactions Law;
- Government Regulation Number 71 of 2019;
- Financial Services Authority Regulations;
- Bank Indonesia Regulations;
- Court decisions relating to personal data protection, if relevant.

2) Secondary Legal Materials

Secondary legal materials include:

- Legal textbooks;
- Reputable national and international journal articles;
- Research results;
- Dissertations;
- Theses;
- Government agency reports;
- Financial Services Authority (OJK) documents;
- Bank Indonesia publications;
- Ministry of Communication and Digital publications;
- Opinions of legal experts.

3) Tertiary Legal Materials

Tertiary legal materials include:

- Big Indonesian Dictionary (KBBI);
- Black's Law Dictionary;
- Legal Dictionary;
- Legal Encyclopedia;
- Legal Index;
- Other reference sources that support the interpretation of legal terms.

4. Legal Material Collection Techniques

Legal materials were collected through library research, inventorying, identifying, classifying, and reviewing various primary, secondary, and tertiary legal materials relevant to the research object. Literature searches were conducted through various scientific databases such as Google Scholar, Garuda, HeinOnline, Scopus,

p-ISSN 2337-6368 | e-ISSN 2615-4439
https://jurnal.ugj.ac.id/index.php/HERMENEUTIKA

ScienceDirect, SpringerLink, as well as the JDIH and BPK RI portals to obtain the most up-to-date regulations and literature.

All legal materials obtained were then classified by topic, facilitating the analysis of legal protections against misuse of Fintech users' personal data.

5. Legal Material Analysis Techniques

Analysis of legal materials is carried out qualitatively using legal interpretation and legal reasoning methods.

Tahapan analisis meliputi:
1) Inventory of all laws and regulations related to personal data protection;
2) Identification of relevant legal principles;
3) Systematic interpretation of legal norms;
4) Analysis of vertical and horizontal synchronization between regulations;
5) Identification of legal vacuums, conflicts of norms, and vague norms;
6) Formulation of legal arguments based on legal protection theory, legal certainty theory, justice theory, and responsive legal theory;
7) Formulation of normative recommendations as solutions to weaknesses in regulations for protecting personal data for Fintech users.

The analysis was conducted using a deductive method, drawing conclusions from general legal norms and applying them to specific issues concerning the misuse of personal data by fintech users. This approach enabled researchers to produce legal arguments that were systematic, logical, and academically justifiable.

6. Validity of Legal Arguments

To ensure the validity of the research results, a legal triangulation technique was used, namely comparing and testing the consistency between laws and regulations, expert doctrines, court decisions (if available), and previous research results. Furthermore, interpretation of norms was carried out using several legal interpretation methods, namely grammatical, systematic, historical, teleological, and futuristic interpretations, so that the resulting legal argumentation is not only in accordance with the textual interpretation of the norms, but also in line with the objectives of law formation and the development of the needs of the digital society.

III. RESULTS AND DISCUSSION

1. Forms of Legal Protection against Misuse of Personal Data of Financial Technology (Fintech) Users

The development of Financial Technology (Fintech) has brought significant changes to the financial services system in Indonesia. The use of digital technology allows people to access financial services quickly, easily, and efficiently. However, behind this convenience comes legal challenges in the form of an increased risk of misuse of users' personal data. Personal data collected by Fintech providers includes names, National Identification Numbers (NIK), telephone numbers, addresses, bank accounts, locations, and transaction history. This data has high economic value and is therefore vulnerable to misuse if not managed in accordance with legal provisions.

From a legal perspective, personal data protection is part of the right to privacy guaranteed by Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia. This provision emphasizes that everyone has the right to personal protection,

p-ISSN 2337-6368 | e-ISSN 2615-4439
https://jurnal.ugj.ac.id/index.php/HERMENEUTIKA

honor, dignity, and a sense of security. Therefore, misuse of personal data is not only an administrative violation, but also a violation of the constitutional rights of citizens (Hadjon, 1987).

According to the legal protection theory proposed by Philipus M. Hadjon, legal protection consists of preventive and repressive protection. Preventive protection aims to prevent violations from occurring through the establishment of regulations and oversight mechanisms, while repressive protection aims to provide resolution to violations that have already occurred.

In Fintech operations, preventative protection is implemented through the obligation for providers to obtain user consent before processing personal data, maintain data confidentiality, implement electronic security systems, and limit data use to approved purposes only. These provisions are stipulated in Law Number 27 of 2022 concerning Personal Data Protection and various regulations issued by the Financial Services Authority.

Meanwhile, repressive protection is provided through complaint mechanisms, dispute resolution, administrative sanctions, civil lawsuits, and criminal law enforcement in the event of misuse of personal data. These mechanisms provide Fintech users with legal certainty in obtaining protection if their rights are violated.

However, in practice, various problems remain, such as excessive data collection, data use without explicit consent, data leaks due to weak security systems, and data dissemination to third parties without user consent. These conditions indicate that the legal protections stipulated in laws and regulations have not been fully implemented optimally.

2. Legal Protection Regulations for Fintech Users' Personal Data in the Indonesian Legal System

Regulations regarding personal data protection in Indonesia have undergone significant developments following the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). Prior to this law's enactment, regulations regarding personal data were scattered across various sectoral regulations, thus lacking adequate legal certainty.

The PDP Law regulates various important aspects, including the rights of data subjects, the obligations of data controllers, data processing principles, dispute resolution, and administrative and criminal sanctions. This law demonstrates the state's commitment to providing legal protection for people's privacy rights in the digital age.

In addition to the PDP Law, legal protection for Fintech users is also regulated in the Electronic Information and Transactions Law and its amendments, Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, and various regulations of the Financial Services Authority that govern the implementation of information technology-based financial services.

From a legal perspective, these regulations demonstrate that personal data protection is carried out through a multidisciplinary approach involving administrative law, civil law, criminal law, and consumer protection law. This approach aims to provide legal certainty while increasing public trust in digital financial services.

However, the analysis shows that several weaknesses remain in Indonesia's legal system. First, there is still overlap between the PDP Law and several sectoral regulations. Second, the coordination mechanism between supervisory agencies is not yet fully

p-ISSN 2337-6368 | e-ISSN 2615-4439
https://jurnal.ugj.ac.id/index.php/HERMENEUTIKA

effective. Third, technological developments such as artificial intelligence and big data have not been fully addressed in existing regulations.

When analyzed using Gustav Radbruch's theory of legal certainty, the PDP Law provides a clearer legal basis than previous regulations. However, legal certainty is determined not only by the existence of norms, but also by the effectiveness of their implementation and enforcement.

From the perspective of Nonet and Selznick's responsive legal theory, the law must adapt to societal and technological developments. Therefore, personal data protection regulations must be continuously adapted to the development of Fintech to continue to provide effective legal protection for the public.

Based on the results of the normative analysis, legal protection for Fintech users' personal data in Indonesia already has a sufficient legal basis. However, the effectiveness of this protection still requires strengthening through regulatory harmonization, increased oversight, increased compliance of Fintech providers, and increased public digital literacy. These efforts are necessary to optimally achieve the objectives of the Personal Data Protection Law, namely to achieve legal certainty, justice, and the protection of public rights in the digital economy era.

Author's Analysis

Based on the research findings, it is clear that Indonesia already has a relatively comprehensive legal framework for protecting the personal data of fintech users through Law Number 27 of 2022 and its supporting regulations. However, the main challenge no longer lies in the availability of legal norms, but rather in their implementation.

The continued discovery of cases of personal data leaks and misuse demonstrates the need for:

1) Strengthening regulatory oversight;
2) Increasing compliance by fintech operators with good data governance principles;
3) Harmonizing the Data Protection and Transactions Law, OJK regulations, and other digital sector provisions; and
4) Increasing public awareness of their rights as data subjects.

Thus, legal protection against misuse of personal data is not only the government's responsibility, but also requires collaboration between regulators, Fintech providers, and the public to create a safe, trustworthy, and sustainable digital financial ecosystem.

IV. CONCLUSION

This study shows that legal protection against misuse of personal data of Financial Technology (Fintech) users in the Indonesian legal system has undergone significant development with the enactment of Law Number 27 of 2022 concerning Personal Data Protection as a legal regime that comprehensively regulates the rights of data subjects, the obligations of data controllers and processors, the principles of personal data processing, and law enforcement mechanisms. The existence of the Personal Data Protection Law supported by the Electronic Information and Transactions Law and its amendments, Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, and the Financial Services Authority regulations in the field of digital financial services demonstrates the state's commitment to providing legal certainty and protection of people's right to privacy as part

p-ISSN 2337-6368 | e-ISSN 2615-4439
https://jurnal.ugj.ac.id/index.php/HERMENEUTIKA

of the constitutional rights guaranteed by the 1945 Constitution of the Republic of Indonesia.

Legal protection for Fintech users is realized through two approaches: preventive legal protection and repressive legal protection. Preventive protection is implemented through the regulation of personal data protection principles, the obligation to obtain valid informed consent, limitations on data processing purposes, the implementation of information security standards, and the recognition of data subjects' rights. Repressive protection, on the other hand, is realized through administrative sanctions, civil liability, and criminal sanctions against any form of misuse of personal data. Both forms of protection normatively reflect the implementation of the theory of legal protection, which places the state as the party obligated to guarantee the fulfillment of citizens' rights in the provision of technology-based financial services.

Nevertheless, the results of the normative analysis indicate that the effectiveness of legal protection still faces various challenges. Harmonization between the Personal Data Protection Law and sectoral regulations in the digital financial services sector has not been fully realized, coordination between supervisory authorities still requires strengthening, and the highly dynamic development of digital technology presents new risks that have not been fully anticipated by existing regulations. Furthermore, excessive data collection practices, data processing without adequate consent, and weak information security governance are still found among some Fintech operators, indicating a gap between normative regulations and implementation on the ground.

Therefore, this study confirms that the effectiveness of legal protection against misuse of Fintech users' personal data is determined not only by the existence of comprehensive laws and regulations, but also by regulatory harmonization, the effectiveness of supervisory institutions, consistent law enforcement, compliance of providers with the principles of good data governance, and increased legal awareness among the public as subjects of personal data. Therefore, personal data protection in the Fintech sector must be viewed as part of the development of a digital legal system oriented towards legal certainty, justice, benefit, and respect for human rights, thereby supporting the creation of a safe, trustworthy, and sustainable digital financial services ecosystem in Indonesia.

REFERENCES

Aldboush, H. H. H., & Ferdous, M. (2023). Building Trust in Fintech: An Analysis of Ethical and Privacy Considerations at the Intersection of Big Data, AI, and Customer Trust. International Journal of Financial Studies, 11(3), 90.

Ali, Achmad. (2009). Uncovering Legal Theory and Judicial Prudence. Jakarta: Kencana.

Ali, Zainuddin. (2021). Legal Research Methods. Jakarta: Sinar Grafika.

Arner, D. W., Barberis, J., & Buckley, R. P. (2016). The Evolution of FinTech: A New Post-Crisis Paradigm? Georgetown Journal of International Law, 47(4), 1271–1319.

Asshiddiqie, Jimly. (2015). Introduction to Constitutional Law. Jakarta: Rajawali Pers.

Asshiddiqie, Jimly. (2020). The Indonesian Constitution and Constitutionalism. Jakarta: Sinar Grafika.

p-ISSN 2337-6368 | e-ISSN 2615-4439
https://jurnal.ugj.ac.id/index.php/HERMENEUTIKA

Aulia, H., & Umboh, N. K. (2025). Analytical study of Law Number 27 of 2022 concerning Personal Data Protection in the financial sector. Indonesian Intellectual and Scholars Journal.

Blumenstock, J. E., & Kohli, N. (2023). Big Data Privacy in Emerging Market Fintech and Financial Services: A Research Agenda. arXiv.

Budhijanto, Danrivanto. (2010). Telecommunications, Broadcasting, and Information Technology Law: Regulation and Convergence. Bandung: Refika Aditama.

Budhijanto, Danrivanto. (2024). Personal Data Protection and National Data Law. Bandung: Logoz Publishing.

European Union. (2016). General Data Protection Regulation (EU) 2016/679.

Fauzy, E., & Shandy, N. A. R. (2023). The Right to Privacy and the Legal Politics of Law Number 27 of 2022 concerning Personal Data Protection. Lex Renaissance, 7(3), 445–461.

Financial Services Authority Regulation Number 10/POJK.05/2022 concerning Information Technology-Based Joint Funding Services.

Friedman, Lawrence M. (1975). The Legal System: A Social Science Perspective. New York: Russell Sage Foundation.

Fuady, Munir. (2013). Grand Theories in Law. Jakarta: Kencana.

Gomber, P., Koch, J. A., & Siering, M. (2018). Digital Finance and FinTech: Current Research and Future Research Directions. Journal of Business Economics, 87(5), 537–580.

Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions.

Hadjon, Philipus M. (1987). Legal Protection for the People in Indonesia. Surabaya: Bina Ilmu.

HS, Salim, & Nurbani, Erlies Septiana. (2017). Application of Legal Theory to Thesis and Dissertation Research. Jakarta: Rajawali Press.

Kelsen, Hans. (1967). Pure Theory of Law. Berkeley: University of California Press.

Kollnig, K., Zhang, L., Zhao, J., & Shadbolt, N. (2023). Before and After China's New Data Laws: Privacy in Apps. arXiv.

Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions.

Law Number 27 of 2022 concerning Personal Data Protection.

Mahfud MD. (2017). Legal Politics in Indonesia. Jakarta: Rajawali Pers.

Manurung, E. A. P., & Thalib, E. F. (2023). A Legal Review of Personal Data Protection Under Law Number 27 of 2022. Saraswati Law Journal, 5(2), 240–252.

Marzuki, Peter Mahmud. (2021). Legal Research. Jakarta: Kencana.

p-ISSN 2337-6368 | e-ISSN 2615-4439
https://jurnal.ugj.ac.id/index.php/HERMENEUTIKA

Mertokusumo, Sudikno. (2019). Understanding Law: An Introduction. Yogyakarta: Cahaya Atma Pustaka.

Nonet, Philippe, & Selznick, Philip. (1978). Law and Society in Transition: Toward Responsive Law. New York: Harper & Row.

Pound, Roscoe. (1959). Jurisprudence. St. Paul: West Publishing.

Putri, B. M. L., Rohaini., Nhung, P. H., & Putri, R. W. (2025). Analysis of Consumer Rights Protection Against the Misuse of Personal Data in Fintech Services. Lex Publica, 12(1), 32–62.

Radbruch, Gustav. (1950). Legal Philosophy. Edinburgh: Edinburgh University Press.

Rahardjo, Satjipto. (2000). Legal Science. Bandung: Citra Aditya Bakti.

Rahardjo, Satjipto. (2009). Progressive Law: A Synthesis of Indonesian Law. Yogyakarta: Genta Publishing.

Riswandi, Budi Agus, Zulhuda, Sonny, Wibowo, Ari, Hartanto, Ratna, Luthfidyfa, Nabilla Maryam, & Erlangga, Vania Lutfi Safira. (2024). Personal Data Protection Law: Comparative Study on Indonesian and Malaysian Law. Yogyakarta: Universitas Islam Indonesia Publisher.

Rosadi, Sinta Dewi. (2015). Cyber Law: Aspects of Data Privacy According to International, Regional, and National Law. Bandung: Refika Aditama.

Rosadi, Sinta Dewi. (2021). Personal Data Protection in Indonesia. Bandung: Refika Aditama.

Saly, J. N., Artamevia, H., Gulo, B. J. S., & Rhemrev, M. A. (2023). Analysis of Personal Data Protection Related to Law Number 27 of 2022. Serina Social Humanities Journal, 1(3), 1800–1808.

Sianipar, O. J., Satory, A., & Darmawan, I. (2025). The Urgency of Consumer Personal Data Protection in Indonesia's Fintech Ecosystem in the Era of Digital Business Transformation. International Journal of Cultural and Social Science, 7(2).

Sjahdeini, Sutan Remy. (2018). The Legal System and Legal Protection in Indonesia. Jakarta: Prenadamedia Group.

Soekanto, Soerjono, & Mamudji, Sri. (2019). Normative Legal Research: A Brief Review. Jakarta: RajaGrafindo Persada.

Soekanto, Soerjono. (2019). Introduction to Legal Research. Jakarta: UI Press.

State Responsibilities Regarding Personal Data Protection Based on Law Number 27 of 2022 concerning Personal Data Protection. (2024). Kutei Scientific Journal, 23(2), 158–172.

Subekti. (2005). Principles of Civil Law. Jakarta: Intermasa.

Sutedi, Adrian. (2009). Sharia Banking: Review and Several Legal Aspects. Jakarta: Ghalia Indonesia.

Sutedi, Adrian. (2014). Banking Law. Jakarta: Sinar Grafika.

The 1945 Constitution of the Republic of Indonesia.

p-ISSN 2337-6368 | e-ISSN 2615-4439
https://jurnal.ugj.ac.id/index.php/HERMENEUTIKA

United Nations. (1948). Universal Declaration of Human Rights.

United Nations. (1966). International Covenant on Civil and Political Rights.

Walters, Robert, Trakman, Leon, & Zeller, Bruno. (2019). Data Protection Law: A Comparative Analysis of Asia-Pacific and European Approaches. Singapore: Springer.

Westin, Alan F. (1967). Privacy and Freedom. New York: Atheneum.

Yang, L., Tian, M., Xin, D., Cheng, Q., & Zheng, J. (2024). AI-Driven Anonymization: Protecting Personal Data Privacy While Leveraging Machine Learning. arXiv.