

LEGAL ANALYSIS OF PERSONAL DATA PROTECTION IN FINTECH-BASED FINANCIAL TRANSACTIONS

Rana Nugraha¹, Teddy Asmara², Sanusi³, Itto Turyandi⁴

¹ BAIS TNI (Badan Intelijen Strategis Tentara Nasional Indonesia)

^{2,3} Universitas Swadaya Gunung Jati, Sekolah Pascasarjana, Program Studi Magister Hukum

⁴ Universitas Alghifari, Fakultas Ekonomi, Prodi Manajemen



DOI: <https://doi.org/10.33603/hermeneutika.v10i1.10988>

Diterima: 14 Mei 2019; Direvisi: 10 Juli 2019; Dipublikasikan: Agustus 2019

Abstract. *The rapid development of information technology has transformed the financial sector through Financial Technology (Fintech), which offers convenient access to payment services, online lending, and investment. Behind the opportunities for financial inclusion, Fintech also presents risks of personal data breaches, identity theft, and increasingly complex cybercrimes. This study aims to analyze the legal protection of personal data in Fintech-based financial transactions in Indonesia, with a particular focus on the effectiveness of the implementation of Law Number 27 of 2022 on Personal Data Protection (PDP Law) and related sectoral regulations. Employing a constructivist and critical paradigm with a normative-empirical juridical approach, this research combines legal norm analysis, field-based empirical findings, and comparisons with international standards (GDPR) to provide a holistic overview of personal data protection in the Fintech sector. The findings reveal that although Indonesia's legal framework is relatively comprehensive, its implementation faces challenges such as fragmented regulations, limited supervisory capacity, technical constraints of regulators, and weak law enforcement against illegal actors. The study also highlights the dominance of administrative sanctions as the primary enforcement mechanism, which serve as short-term corrective measures but fail to create systemic deterrence. Strengthening regulatory capacity, establishing an independent data protection authority, harmonizing sectoral regulations, integrating administrative–civil–criminal enforcement pathways, and enhancing digital literacy are recommended to ensure legal certainty and strengthen public trust in digital financial transactions.*

Keywords: *Fintech, personal data protection, PDP Law, cybercrime, legal certainty.*

I. INRODUCTION

The rapid development of information and communication technology has fundamentally transformed the financial sector. Financial Technology (Fintech) has emerged as one of the key innovations, providing easy access to digital-based financial services, ranging from payments and online lending to digital investment and insurance. This innovation creates vast opportunities for financial inclusion while simultaneously introducing new risks related to data security and user privacy. Fintech-based financial transactions inherently involve the collection, storage, and processing of sensitive personal data, making them highly vulnerable to increasingly sophisticated cybercrimes.

In Indonesia, awareness of the importance of personal data protection has grown significantly with the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law), which serves as the primary legal framework safeguarding citizens' privacy rights in the digital era. The PDP Law stipulates the obligations of electronic system operators to protect personal data from unauthorized access, collection, processing, and dissemination. Sectoral regulations, such as the Financial Services Authority Regulation (POJK) on Information Technology-Based Lending Services and Bank Indonesia Regulation on Payment Service Providers, also govern aspects of consumer protection and cybersecurity. Nevertheless, the implementation of legal protection in the Fintech sector still faces various challenges, including the complexity of evolving technologies, the limited availability of human resources capable of simultaneously understanding legal and technological aspects, and the uneven level of awareness among society and industry players.

Alongside the benefits of Fintech in expanding financial access, there are emerging threats such as data breaches, identity theft, intimidation by debt collectors, and misuse of data by third parties. Cybercrime methods have also become increasingly diverse, including phishing, malware, application programming interface (API) attacks, and even the use of deepfakes for identity fraud. These phenomena necessitate an in-depth study of the effectiveness of existing legal protections and how regulations can be adapted to anticipate ever-changing threats.

Previous studies on Fintech in Indonesia have largely focused on legality, consumer protection, and digital literacy. However, there remains a limited body of research specifically addressing the legal challenges of personal data protection in Fintech transactions within the unique social, economic, and digital infrastructure context of Indonesia. This research seeks to fill that gap by comprehensively analyzing the legal protection of personal data in Fintech-based financial transactions, with a focus on efforts to anticipate increasingly complex and dynamic forms of cybercrime.

By integrating normative aspects, empirical phenomena, and theories of personal data protection, this research is expected to provide novel contributions through a critical evaluation of the implementation of the PDP Law and related regulations on Fintech in Indonesia, as well as concrete policy recommendations to strengthen personal data protection in technology-based financial transactions. The urgency of this research is underscored by the fact that Fintech, as a manager of highly sensitive and strategic personal data, requires a comprehensive and adaptive legal protection framework to maintain consumer trust while also supporting the healthy and sustainable growth of the digital financial industry.

II. RESEARCH METHOD

This study is grounded in the constructivist and critical paradigms. The constructivist paradigm views law as a social construct shaped by societal and technological dynamics, while the critical paradigm is employed to evaluate the limitations of the legal system in anticipating cybercrime. The research applies a descriptive-analytical approach with a combination of:

1. **Normative juridical** (analyzing the content of legal norms, such as the PDP Law, the Electronic Information and Transactions Law, and the OJK Regulation on Fintech).

2. **Empirical juridical** (assessing the implementation of laws through interviews, questionnaires, and observations).
3. **Comparative** (contrasting Indonesian regulations with international frameworks such as the GDPR).

This is a **normative-empirical legal study** (socio-legal research) that integrates doctrinal law with the legal behavior of society to provide a holistic understanding of personal data protection in Fintech transactions.

Types and Sources of Legal Materials

1. **Primary sources:** Law No. 27/2022, Law No. 11/2008, OJK Regulation No. 77/2016.
2. **Secondary sources:** books on IT law, journals on cyber law, research reports from LIPI and BSSN.
3. **Tertiary sources:** legal dictionaries, legal encyclopedias, credible mass media.

Data Analysis Techniques

1. Content analysis and Miles & Huberman's interactive model (data reduction, data presentation, and conclusion drawing).
2. Legal interpretation using grammatical, systematic, and teleological methods.
3. Thematic analysis of public perceptions combined with a comparative review of the European Union's GDPR.

Validation and Data Testing Techniques

- Triangulation of sources (legal data, interviews, observations) and methods (normative–empirical).
- Consistency testing of Fintech regulations with the PDP Law, compliance testing with principles of digital consumer protection, and effectiveness testing of law enforcement.

Conclusion Drawing

The reasoning process applies:

- **Deductive reasoning**, moving from general norms to concrete cases.
- **Evaluative-critical reasoning**, to assess the effectiveness of legal provisions.
- **Analogical reasoning**, by drawing comparisons with international practices in cases where national regulations are absent.

III. RESEARCH FINDINGS

The study reveals that the legal framework for personal data protection in Indonesia's fintech sector is relatively comprehensive; however, its implementation faces three main challenges: normative fragmentation, limited supervision, and regulators' technical capacity.

1. Normative Provisions and Legal Uncertainty

Law No. 27 of 2022 on Personal Data Protection (PDP Law) incorporates global principles such as lawfulness, fairness, transparency, data minimization, integrity, and

accountability. In theory, this regulation enhances legal certainty for fintech users. However, the research highlights practical uncertainties, beginning with overlapping supervisory roles among OJK, Bank Indonesia (BI), and the Ministry of Communication and Information Technology (Kominfo); data controller/processor models that do not fully align with fintech operations; and the absence of clear mechanisms for cross-border data transfers and breach notifications. These weaknesses undermine the rule of law principle that legislation must be clear, stable, and predictable.

2. **Regulatory Overlap and Enforcement**

A comparison of the PDP Law, OJK regulations, BI regulations, and Government Regulation No. 71/2019 shows overlap in three key areas: (1) personal data protection obligations (all regulators mandate similar requirements), (2) consent standards and data subject rights (definitions vary across regulations), and (3) sanctions and enforcement (multiple sanctions with layered complaint channels). Unsynchronized enforcement across regulators delays victim recovery and creates uncertainty for businesses.

3. **Limitations of OJK**

OJK effectively supervises licensed fintech operators but cannot adequately address illegal operators that frequently misuse data. Without an independent data protection authority, enforcement responsibilities are dispersed across agencies, leading to slow complaint handling and coordination. Moreover, regulators' technical capacity—such as in algorithm auditing, digital forensics, and cloud risk assessment—remains limited, resulting in enforcement decisions that are not always based on robust technical evidence.

4. **Strengthening Norms and Institutions**

The PDP Law requires “privacy by design” and “privacy by default” in the fintech sector. Meanwhile, the Omnibus Law No. 4 of 2023 strengthens OJK's position as the primary regulator for non-bank fintech, mandating data center standards, IT security, and broader enforcement authority. Together, these two laws present an opportunity for regulatory harmonization, reducing overlapping compliance burdens and clarifying enforcement pathways.

5. **Implications for Legal Certainty**

Legal certainty in fintech personal data protection depends not only on statutory texts but also on institutional structures and supervisory capacity. The research finds that the certainty envisioned under the PDP Law will be difficult to achieve effectively for both users and providers without the establishment of an independent data protection authority, harmonization of OJK–BI–Kominfo sectoral regulations, and the strengthening of digital literacy along with accessible complaint mechanisms.

The study further finds that **administrative sanctions** are the dominant form of enforcement against fintech operators that fail to protect users' data. Following the enactment of the PDP Law (Law No. 27/2022), sectoral regulators such as OJK and technical interventions by

Kominfo have become the primary actors in enforcement. Administrative sanctions include written warnings, fines, service restrictions, suspension, and license revocation, while Kominfo focuses on technical measures such as blocking, public clarification, and mitigation coordination.

This dominance of administrative sanctions is driven by three main factors. First, procedural simplicity and faster response compared to criminal or civil proceedings. Criminal processes and civil lawsuits require complex and costly digital forensic evidence, whereas administrative routes allow swift responses to a high volume of complaints (thousands in each supervisory period). Second, the massive scale of fintech-related complaints necessitates quick and systematic enforcement mechanisms. Third, evidentiary challenges push regulators to prefer corrective administrative measures over litigation. This finding is supported by OJK reports consistently imposing dozens to hundreds of administrative sanctions on online lending operators in each supervisory period (Kontan, 4 September 2025; Investortrust, 15 July 2025).

The study corroborates previous research (Zamil, et al., 2025), which highlights the limitations of administrative approaches: while administrative sanctions can improve short-term operational practices, they do not necessarily restore victims' losses or create long-term deterrence. Much of the leaked data remains circulated even after platforms are blocked. The study shows that without enhanced forensic capacity, effective mechanisms for collective civil litigation, and credible criminal sanctions, violators remain prone to repeat offenses (recidivism).

Illegal online lending cases illustrate recurring violations, including excessive data collection (NIK, ID cards, selfies, contacts, galleries), doxxing by debt collectors, and identity theft. Although OJK and the Investment Alert Task Force block these applications, victims' data remain irretrievable. Fragmented authority among OJK, Kominfo, and law enforcement further slows victim recovery and perpetrator investigation.

Thus, while administrative sanctions currently serve as the primary enforcement pathway for data protection in Indonesia's fintech sector, without structural reforms and inter-agency coordination, their effectiveness will remain corrective and short-term rather than achieving the systemic deterrent effect envisioned.

IV. CONCLUSION

The guarantee of legal norms in fintech-based financial transactions is essential to ensure legal certainty. Law No. 27 of 2022 provides a clear and firm legal framework regarding personal data governance, compelling fintech operators to follow transparent procedures and obtain explicit user consent. Strict supervision mechanisms by authorities such as Kominfo and OJK, along with the application of administrative and criminal sanctions, ensure effective law enforcement and create legal certainty for all parties involved.

The aspect of legal protection of personal data in fintech transactions serves as a fundamental pillar in anticipating cybercrime. Law No. 27 of 2022 regulates user rights, such as the right to access, correct, and delete data, while also requiring fintech providers to implement adequate security technologies. This framework helps prevent data misuse and cyberattacks, while simultaneously enhancing public trust in digital financial transactions.

The research further suggests several measures for improvement and refinement, including:

1. Strengthening the technical capacity of regulators (e.g., digital forensics and more in-depth administrative investigations).
2. Harmonizing the PDP Law with sectoral regulations and establishing an independent Personal Data Protection Authority.
3. Integrating administrative, civil, and criminal pathways to achieve long-term deterrence while also providing fair remedies for victims.
4. Conducting education and outreach through community empowerment initiatives, directly targeting both fintech users and prospective users of fintech-based financial transactions.

Bibliography

Book :

- Asmara, T., (2024). *Implementation Of Non Penal Policy Against Non-Fulfillment Of Ship Seavailability And Safety*. Ejournalugj.Com
- Gilster, P. (1997). *Digital Literacy*. New York: John Wiley & Sons.
- Howells, G. G., & Weatherill, S. (2005). *Consumer Protection Law*. Aldershot: Ashgate Publishing.
- Janus Sidabalok. (2014). *Hukum PelindunganPenerima dana di Indonesia*. Citra Aditya Bhakti, Bandung.
- Kementerian Komunikasi dan Informatika Republik Indonesia. (2023). *Peraturan Kominfo tentang Perlindungan Data Pribadi*. Jakarta: Kementerian Kominfo.
- Nugroho, H. (2022). *Literasi Digital Masyarakat dalam Menghadapi Perkembangan Fintech*. Bandung: Alfabeta.
- Sanusi. (2024). *Penegakan Hukum Dalam Tindak Pidana Penipuan Penawaran Kerja Berbasis Media Elektronik (Whatsapp)*. Jakarta : Hukum Dan Masyarakat Madani.
- Saragih, R. M. (2020). *Perlindungan Konsumen dalam Layanan Fintech di Indonesia*. Yogyakarta: Deepublish.
- Sihombing, A. (2022). *Kehangatan hukum dalam transaksi fintech dan dampaknya terhadap konsumen*. Jakarta : UKI Press.
- Turyandi, Itto. (2025). *Metodologi Penelitian : Teori, Strategi dan Implementasi*. Purbalingga : Eureka Media Aksara.
- Wahyu Sasongko. (2022). *Hukum Siber dan Perlindungan Data Pribadi*. Yogyakarta: Deepublish.

Journal/Article/AcademicPaper/Research Result:

- Arner, DW, Barberis, J., & Buckley, RP (2016). *Fintech: Evolusi dan Masa Depan Jasa Keuangan*. Jurnal Regulasi Keuangan, 2(1), 1-20. <https://doi.org/10.1093/jfr/vfw008>
- Arfianto, D. (2021). *Analisis Perlindungan Hukum Data Pribadi dalam Transaksi Keuangan Digital di Indonesia*. Jurnal Hukum dan Teknologi , 10(2), 85-99.
- Budiman, R., & Sari, NM (2020). *Kejahatan Siber dalam Transaksi Fintech : Studi Kasus dan Strategi Pencegahan*. Jurnal Keamanan Informasi , 5(1), 45-58.
- Dewi, M., & Prasetyo, H. (2023). *Perlindungan data pribadi pengguna fintech lending di Indonesia: Tinjauan hukum dan praktik*. Jurnal Hukum & Pembangunan, 53(4), 599–620.
- Effendi, R., & Taufiq, M. (2024). *Kebocoran data pribadi pada layanan pinjaman online: Analisis hukum perlindungan konsumen*. Jurnal Yustisia, 13(1), 45–61.
- Gefen, D. (2000). *The role of trust in e-commerce relational exchange: A preliminary model*. The 21st International Conference on Information Systems (ICIS), 1-12. Retrieved from <https://aisel.aisnet.org/icis2000/1>

- Gunawan, H. (2019). *Kepastian Hukum dalam Penyelesaian Sengketa Fintech di Indonesia*. Jurnal Hukum Bisnis , 8(1), 12-27.
- Kurniawan, A. (2022). *Implementasi Regulasi Perlindungan Data Pribadi pada Layanan Fintech*. Jurnal Sistem Informasi dan Komputerisasi Akuntansi , 7(3), 152-165.
- Lembaga Bantuan Hukum (LBH) Bandung. (2023). *Laporan Tahunan 2023: Catatan Kasus Pinjaman Online dan Pelanggaran Hak Digital*. Bandung: LBH Bandung. Diakses dari <https://lbhbandung.or.id>
- Muchsin. (2003). *Pelindungan dan Kepastian Hukum bagi Investor di Indonesia*, Magister Ilmu Hukum Program Pascasarjana Universitas Sebelas Maret, Surakarta.
- Otoritas Jasa Keuangan. (2023). *Statistik Fintech Lending Periode Desember 2023*. Jakarta: Otoritas Jasa Keuangan. Diakses dari <https://www.ojk.go.id>
- Otoritas Jasa Keuangan. (2024). *Laporan tahunan OJK bidang perlindungan konsumen sektor jasa keuangan 2023–2024*. Jakarta: OJK.
- Panjaitan, S., & Marbun, J. (2024). *Tanggung jawab penyelenggara pinjaman online terhadap kebocoran data pribadi pengguna*. Jurnal Perlindungan Konsumen Indonesia, 5(2), 121–138.
- Prabowo, Y. (2023). *Analisis implementasi Undang-Undang Perlindungan Data Pribadi di sektor fintech Indonesia*. Jurnal Hukum Media Justitia, 15(3), 277–298.
- Pratama, A. (2023). *Analisis Regulasi Fintech di Indonesia dan Dampaknya terhadap Pertumbuhan Industri*. Jurnal Teknologi dan Inovasi Keuangan, 11(2), 115-130.
- Rosalinda Elsin Latumahina. (2014). *Aspek Hukum Perlindungan Data Pribadi di Dunia Maya*, Jurnal Gema Aktualita, Vol. 3 No. 2, hlm. 16
- Santoso, A. (2023). *Regulasi Fintech Dan Perlindungan Konsumen Di Era Digital*. Jurnal Teknologi Finansial, 5(2), 120-135.
- Sari, A., & Rachman, A. (2023). *Perlindungan hukum pengguna pinjaman online ilegal : Studi kasus kebocoran data pribadi di Indonesia*. Jurnal Hukum Siber Indonesia, 4(1), 55–74.
- Smith, J., & Jones, M. (2020). *Keamanan Siber dan Perlindungan Data dalam Teknologi Keuangan*. Jurnal Internasional Studi Keuangan , 8(4), 1-15. doi.org
- Susanto, L. (2021). *Perlindungan Konsumen dalam Fintech : Perspektif Hukum dan Teknologi*. Jurnal Hukum dan Pembangunan, 51(4), 567-583.
- Wijaya, T., & Hartono, B. (2023). *Pengawasan dan Penegakan Hukum pada Transaksi Fintech di Indonesia*. Jurnal Regulasi Keuangan , 11(2), 34-50.
- World Bank. (2020). *Financial Inclusion: A Key to Economic Growth*. Retrieved from <https://www.worldbank.org/en/topic/financialinclusion>
- Wulandari, L. (2023). *Transformasi Paradigma Hukum di Era Reformasi: Langkah Krusial dalam Mewujudkan Keadilan Sosial dalam Transaksi E-Commerce*. Jurnal Hukum dan Masyarakat Digital.
- Yulianto, A. (2014). *Hak Asasi Digital dan Regulasi Perlindungan Data Pribadi*. Jurnal Konstitusi.
- Zetsche, DA, Buckley, RP, Arner, DW, & Barberis, JN (2020). *Evolusi dan Masa Depan Keuangan Berbasis Data di UE*. [Jurnal Elektronik SSRN].

Law :

- Pemerintah Republik Indonesia. (2022). *Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi* . Jakarta: Sekretariat Negara.
- Pemerintah Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 213.
- Otoritas Jasa Keuangan (OJK). (2023). *Peraturan OJK tentang Penyelenggaraan Teknologi Keuangan* . Jakarta: OJK.

Peraturan Bank Indonesia No. 22/23/PBI/2020 tentang Penyedia Jasa Pembayaran, yang mengatur aspek keamanan siber dan perlindungan konsumen
Kementerian Komunikasi dan Informatika (Kominfo). (2022). Survei Indeks Literasi Digital Indonesia 2022 . Jakarta: Kementerian Kominfo.