JAMBURA LAW REVIEW
ISSN Print: 2654-9266
ISSN Online: 2656-0461
JALREV
VOLUME 8 ISSUE 2

Asset Protection, Privacy, and Consumer Data in Digital Banking: A Comparative Study of Indonesia and Malaysia

1st Ronald Fadly Sopamena
2nd Lastuti Abubakar
3rd Tri Handayani
4th Kamil Strzepek

[1,2,3]Universitas Padjadjaran, Indonesia
[4]Cardinal Stefan Wyzzynki University, Poland

rfsopamena@gmail.com

Article Info

Submitted: *November 26, 2025*
Revised: July 17, 2026
Accepted: August 11, 2026

Keywords:
Consumer protection; Digital banking; Personal data protection; Privacy; Indonesia–Malaysia comparison

How to cite *[Chicago Manual of Style 17th edition (full note)]*: Ronald Fadly Sopamena, Lastuti Abubakar, and Tri Handayani, "Asset Protection, Privacy, and Consumer Data in Digital Banking: A Comparative Study of Indonesia and Malaysia". *Jambura Law Review* 8, no. 2 (2026): 535–573.

Abstract

The protection of consumers' assets, privacy, and personal data has become a fundamental issue in digital banking due to the increasing risks of cyberattacks and personal data breaches. Although Indonesia has established various legal instruments governing digital banking and personal data protection, the existing regulatory framework remains fragmented, creating challenges for effective consumer protection. This study aims to analyse the legal protection of consumers' assets, privacy, and personal data in Indonesia and Malaysia and to identify regulatory gaps affecting the effectiveness of Indonesia's digital banking framework. The research employs a normative juridical method using statutory, conceptual, and comparative legal approaches. The findings indicate that Indonesia's regulatory framework is constrained by fragmented regulations, overlapping institutional authority, and limited regulatory harmonisation, resulting in weaknesses in cybersecurity governance and legal enforcement. By contrast, Malaysia has developed a more integrated regulatory framework through the Financial Services Act 2013, the Islamic Financial Services Act 2013, the Personal Data Protection Act 2010, and policy documents issued by Bank Negara Malaysia, providing greater institutional coordination and regulatory consistency. The study concludes that strengthening Indonesia's digital banking regulatory framework requires greater regulatory harmonisation, stronger institutional coordination, and integrated governance to enhance legal certainty, cybersecurity resilience, and consumer trust.

Introduction

The rapid advancement of information and communication technology has fundamentally transformed the global financial sector, most notably through the emergence of digital banks, commonly referred to as *digital-only banks*. These institutions operate exclusively through digital platforms without maintaining physical branch networks, relying on financial technology (fintech), artificial intelligence (AI), and big data analytics to provide efficient, innovative, and customer-oriented financial services.[1] The proliferation of digital banking has not only reshaped the conventional banking business model but has also generated significant legal and regulatory challenges concerning prudential supervision, financial stability, consumer protection, and the evolving legal relationship between financial institutions and their customers.[2]

The global expansion of digital banking has been driven by increasing digitalisation, widespread internet penetration, and changing consumer preferences for financial services that are accessible, efficient, and technology driven. According to the World Bank in 2023, more than seventy jurisdictions have licensed digital banks, including the United States, the United Kingdom, China, South Korea, Singapore, and Australia. The digital banking model is widely regarded as an important mechanism for promoting financial inclusion by extending access to formal financial services for previously unbanked and underserved populations.[3]

In Indonesia, digital banking began to grow significantly in 2020 following the transformation of several conventional commercial banks into fully digital banking institutions, including Bank Jago, Bank Neo Commerce, SeaBank, and Bank Raya Indonesia. This transformation has substantially strengthened financial inclusion by enabling consumers to open bank accounts, conduct financial transactions, and access investment services entirely through digital platforms without visiting physical branch offices. According to the Financial Services Authority (*Otoritas Jasa Keuangan—OJK*) Report (2023), the number of digital banking accounts increased by more than 200 per cent between 2020 and 2023,[4] illustrating a significant shift in the financial behaviour and banking preferences of Indonesian consumers.

A principal legal issue confronting the digital banking industry is the increasing disparity between rapid technological innovation and the capacity of existing regulatory frameworks to accommodate such developments. In many jurisdictions, the absence of legislation specifically governing digital-only banks has resulted in supervisory authorities applying regulatory standards originally designed for conventional banking institutions. This approach has created regulatory gaps, whereby emerging financial

---

[1] M. T. Alt, R., Beck, R., & Smits, "FinTech and the Transformation of the Financial Industry," *Electronic Markets* 30, no. 1 (2020): 15–27.
[2] F. Claessens, S., Frost, J., Turner, G., & Zhu, "Fintech Credit Markets Around the World: Size, Drivers and Policy Issues," *BIS Quarterly Review*, 2018, 20–28.
[3] World Bank, "Global Financial Development Report 2023: Digitalization of Finance," *Washington, DC: World Bank.*, 2023.
[4] OJK, "Survei Nasional Literasi Dan Inklusi Keuangan 2023.," *Otoritas Jasa Keuangan.*, 2023.

innovations—including open banking, cryptocurrency integration,[5] and automated lending services—may operate without adequate legal oversight or regulatory safeguards.[6] Several jurisdictions, including the United States and several European Union Member States, have yet to establish comprehensive legal frameworks capable of effectively responding to the regulatory complexities arising from digital banking.

In Indonesia, the regulatory framework governing digital banking was significantly reinforced through Financial Services Authority Regulation (*Peraturan Otoritas Jasa Keuangan/POJK*) No. 21 of 2023 concerning Digital Services by Commercial Banks. Indonesia has yet to establish a distinct legal umbrella for digital banks, which is essential to guarantee legal certainty and to protect consumers' personal data from the risk of data breaches.[7] Nevertheless, Sitorus argues that overlapping regulatory authority continues to exist among the Financial Services Authority (*OJK*), Bank Indonesia, and the Ministry of Communication and Informatics (Kementerian Komunikasi dan Informatika—Kominfo; renamed the Ministry of Communication and Digital Affairs, Komdigi, in 2024), particularly in relation to data protection, cybersecurity governance, and the security of digital financial transactions. Such institutional fragmentation raises concerns regarding regulatory coherence, legal certainty, and the effectiveness of consumer protection within Indonesia's rapidly evolving digital banking ecosystem.[8]

The protection of consumers' assets, privacy, and personal data constitutes one of the fundamental principles underpinning comprehensive consumer protection within the banking sector, as expressly stipulated in Article 3(2) of Financial Services Authority Regulation (*Peraturan Otoritas Jasa Keuangan/POJK*) No. 22 of 2023 concerning Consumer and Public Protection in the Financial Services Sector. Nevertheless, effective protection of assets, privacy, and personal data—particularly for customers of digital banks—has yet to be fully realised in Indonesia. Digital banking institutions continue to face numerous challenges that may adversely affect consumers, including personal data breaches, phishing attacks, the unauthorised use of personal data by third parties, and other forms of cyber-related misconduct.

One of the most significant legal and operational challenges confronting digital banking is cybersecurity. Because digital banks operate exclusively through electronic platforms, their systems have become primary targets for cyberattacks, identity theft, phishing, and personal data breaches. According to the Deloitte Global Report (2023), approximately 35 per cent of cyberattacks against financial institutions in 2022 targeted digital banks, primarily due to weaknesses in encryption protocols and multi-factor authentication

[5] "Law and Digitalization: Cryptocurrency as Challenges Towards Indonesia's Criminal Law," *IJCLS (Indonesian Journal of Criminal Law Studies)* 10, no. 1 (2025), https://doi.org/10.15294/ijcls.v10i1.22557; Budi Hermono et al., "Regulating the Protection of Cryptocurrency Exchanges to Prevent Systemic Risks and Consumer Rights Violations in Indonesia," *Indonesia Private Law Review* 7, no. 1 (2026): 51–66, https://doi.org/10.25041/iplr.v7i1.4761.

[6] J. N. Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Barberis, *Regulating FinTech: Principles and Challenges* (Oxford University Press, 2020). P. 59

[7] Elsa Assari, "The Legal Status of Digital Banks in Indonesia," *JURISDICTIE* 13, no. 2 (2023): 264–93, https://doi.org/10.18860/j.v13i2.16285. p.265

[8] A. Sitorus, *Kewenangan OJK Dalam Perlindungan Nasabah Perbankan Di Era Digitalisasi* (Refika Aditama, 2023). P. 52

mechanisms.[9] In addition, the unauthorised disclosure and exploitation of customers' personal data remain persistent concerns, often attributable to inadequate internal governance and the commercial use of personal information by third parties. Many digital banking institutions continue to utilise customer data for commercial purposes, including targeted advertising, without ensuring sufficient transparency or obtaining explicit and informed customer consent.[10] Such practices are inconsistent with the principles of *lawfulness* and *purpose limitation*, as recognised under Indonesia's Personal Data Protection Law (Law No. 27 of 2022) and the European Union's General Data Protection Regulation (GDPR). Cybersecurity risks are further exacerbated by limited levels of digital literacy among users. In practice, many personal data breaches arise not from technological failure but from customers' failure to secure their accounts and digital devices. Accordingly, the integrity and security of the digital banking ecosystem depend not only upon technological sophistication but also upon the level of public awareness and digital literacy among users of financial services.

Despite the enactment of Law No. 27 of 2022 concerning Personal Data Protection, Financial Services Authority Regulation (POJK) No. 22 of 2023 concerning Consumer and Public Protection in the Financial Services Sector, and other regulations governing banking and electronic transactions, Indonesia has yet to establish a comprehensive legal framework specifically designed to regulate the integrated protection of consumer assets, privacy, and personal data in digital banking activities. The existing regulatory framework remains fragmented across multiple statutes and regulatory authorities, resulting in overlapping supervisory responsibilities among the Financial Services Authority (OJK), Bank Indonesia, and the Ministry of Communication and Informatics (Kominfo). This fragmented approach creates legal uncertainty in relation to cybersecurity governance, personal data breach management, institutional accountability, and consumer remedies when losses arise from digital banking activities.

In contrast, Malaysia has adopted a more integrated regulatory approach through the Financial Services Act 2013, the Islamic Financial Services Act 2013, the Personal Data Protection Act 2010, and sector-specific policy documents issued by Bank Negara Malaysia, enabling greater institutional coordination and regulatory consistency in protecting consumers within the digital banking ecosystem. Given the structural similarities between the two jurisdictions, particularly their adoption of a dual banking system comprising conventional and Islamic banking institutions, Malaysia provides an appropriate comparative jurisdiction for assessing Indonesia's regulatory framework. Bank Negara Malaysia (BNM), as the central bank, functions as the primary regulatory authority pursuant to the Financial Services Act 2013 (FSA), the Islamic Financial Services Act 2013 (IFSA), and the Central Bank of Malaysia Act 2009. Its supervisory framework applies uniformly across financial institutions to ensure regulatory consistency while facilitating integrated supervision of financial conglomerates. Although previous studies have examined personal data protection, cybersecurity, or digital banking regulation separately, limited attention has been devoted to an integrated legal analysis that simultaneously examines consumer asset protection, privacy, and

[9] Deloitte Global, "Cyber Risk in Digital Banking 2023 Report," *Deloitte Insights.*, 2023.
[10] B. Saragih, *Hukum Data Pribadi Di Indonesia: Implikasi Terhadap Perbankan Digital (Hlm. 97–104).* (Prenada Media Group, 2023). P 102

personal data protection through a comparative Indonesia–Malaysia perspective. This legal and academic gap provides the basis for this study to evaluate the effectiveness of the existing legal framework and formulate recommendations for strengthening consumer protection in Indonesia's digital banking sector.

Against this background, this study addresses the existing legal gap by comparatively examining the legal frameworks governing the protection of consumer assets, privacy, and personal data in Indonesia and Malaysia, with the aim of identifying regulatory weaknesses and proposing directions for regulatory strengthening in Indonesia.

Problem Statement

This study seeks to examine whether Indonesia's fragmented regulatory framework provides adequate legal protection for consumer assets, privacy, and personal data in digital banking when compared with Malaysia's more integrated regulatory model. It further aims to identify existing legal gaps and formulate recommendations to strengthen Indonesia's regulatory framework to enhance legal certainty, cybersecurity governance, and consumer protection in the digital banking sector.

Methods

This study employs a normative juridical[11] research method using three complementary approaches, namely the statutory approach,[12] the conceptual approach, and the comparative law approach. [13] The research adopts a descriptive-analytical design and relies primarily on secondary data, consisting of primary, secondary, and tertiary legal materials.[14] These materials were collected through document and library research. The collected data were subsequently analysed using a qualitative legal analysis to address the legal issues examined in this study.

Legal Framework Governing the Protection of Consumers' Assets, Privacy, and Personal Data in Indonesia's Digital Banking Sector

Under Financial Services Authority Regulation (POJK) No. 13/POJK.03/2021 concerning the Administration of Commercial Bank Products, banks are required to safeguard customers' assets and financial transactions by implementing the prudential principle and information technology-based risk management. Article 2 of POJK No. 13/2021 provides that:

a. Banks shall implement the prudential principle and risk management in the administration of banking products and activities.

---

[11] and Aisyah Dinda Karina. Zainuddin, Muhammad, "Penggunaan Metode Yuridis Normatif Dalam Membuktikan Kebenaran Pada Penelitian Hukum," *Smart Law Journal* 2, no. 2 (2023): 114–23.

[12] and Muhamad Azhar Benuf, Kornelius, "Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer," *Gema Keadilan* 7, no. 1 (2020): 20–33.

[13] Tan David, "Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum," *Nusantara: Jurnal Ilmu Pengetahuan Sosial* 8, no. 8 (2021): 2463-2478.

[14] Sholahuddin. Al-Fatih, *Perkembangan Metode Penelitian Hukum Di Indonesia* (UMMPress, 2023).

b. The implementation of the prudential principle referred to in paragraph (1) shall consider the bank's internal conditions, the characteristics of the relevant products, and the complexity of the risks that may arise.

This provision underscores that every banking product or service, including digital banking services, must undergo a comprehensive risk assessment before being introduced to the market. The objective is to ensure that banks do not offer products that may expose customers to unreasonable risks or undermine financial system stability. The application of the prudential principle encompasses product feasibility assessments, regulatory compliance, technological readiness, and adequate safeguards for customers' assets and personal data. The value of the prudential principle under Article 29 of Law No. 10 of 1998 lies precisely in its role in structuring banks' decision-making before applying specific operational rules, so that risks to customers' assets are anticipated at the outset rather than addressed only after losses have occurred. [15]

Customers who entrust their funds to banks are entitled to legal protection against potential financial losses. Accordingly, Indonesian banking law establishes specific statutory restrictions prohibiting banks from disclosing information concerning depositors and their deposits to third parties, except in circumstances expressly authorised by law.

To safeguard customers' interests, banks are required to observe the banking secrecy principle, which regulates the limited circumstances under which third parties may lawfully obtain access to customers' information or banking records. As both a legal and ethical obligation, banks must comply with statutory provisions restricting the disclosure of customer information except where such disclosure is expressly permitted by legislation. Adherence to the banking secrecy principle protects customers' rights and reinforces public confidence in the banking system, thereby strengthening the fiduciary relationship between banking institutions and the public as users of financial services.

Protecting customers' assets is one of the fundamental pillars of financial services regulation, reflecting the central importance of public trust in the financial system. In Indonesia, customer deposits are protected by the Indonesia Deposit Insurance Corporation (*Lembaga Penjamin Simpanan-LPS*), which guarantees eligible deposits of up to IDR 2 billion per depositor per bank. In addition, the Financial Services Authority (OJK) issued Financial Services Authority Regulation (*POJK*) No. 22 of 2023 concerning Consumer and Public Protection in the Financial Services Sector, replacing the previous framework established under POJK No. 6/POJK.07/2022. This regulation reinforces the legal position of consumers by imposing statutory obligations on Financial Services Business Actors (*Pelaku Usaha Jasa Keuangan-PUJK*) to maintain the security, confidentiality, and integrity of consumers' assets, funds, and personal data, particularly in the provision of digital financial services that are inherently exposed to heightened risks of cyberattacks and data misuse. Banking regulation in Indonesia remains prone to

[15] Pretty Fabiola Andini and Fence M. Wantu, "Implementation of the Precautionary Principle According to Article 2 and Article 29 Law Number 10 of 1998 Concerning Banking," *Damhil Law Journal* 3, no. 1 (2023): 70, https://doi.org/10.56591/dlj.v3i1.1936. P.70

exploitation by bank owners and has not yet fully accommodated the protection of customers' funds and personal data.[16]

Furthermore, Law No. 4 of 2023 concerning the Development and Strengthening of the Financial Sector (the P2SK Law), as amended by Law No. 4 of 2026, establishes a more integrated legal framework for Indonesia's financial services sector by strengthening the regulatory and supervisory authority of the Financial Services Authority (*OJK*), enhancing financial consumer protection, and promoting the stability and integrity of the financial system. The implementation of this statutory framework is reflected in Financial Services Authority Regulation (*POJK*) No. 22 of 2023 concerning Consumer and Public Protection in the Financial Services Sector, which requires Financial Services Business Actors (*PUJK*) to safeguard consumers' assets, funds, privacy, and personal data while implementing effective risk management, sound corporate governance, and adequate internal control systems in the provision of financial services, including digital banking. Together, the P2SK Law and POJK No. 22 of 2023 demonstrate Indonesia's transition towards a preventive and risk-based regulatory approach that prioritises institutional accountability, governance, operational resilience, cybersecurity, and the protection of consumers throughout the digital financial ecosystem.

Financial Services Authority Regulation (*POJK*) No. 22 of 2023 positions the protection of customers' assets as an integral component of the general principles of consumer protection that must be observed by all financial institutions. These principles require financial service providers to conduct their business in a transparent, accountable, and secure manner while respecting consumers' rights and legitimate interests. In this regulatory context, the concept of asset security extends beyond the physical protection of customers' funds to encompass the protection of information systems, the confidentiality of personal data, and the integrity of the digital infrastructure used to store and manage customers' financial assets.

Strengthening customer asset protection is further reflected in the consumer data protection provisions contained in Articles 19–24 of POJK No. 22 of 2023. These provisions require every Financial Services Business Actor (*Pelaku Usaha Jasa Keuangan-PUJK*) to implement adequate information security systems and cybersecurity measures to safeguard consumer data and prevent data breaches, manipulation, or unauthorised access. Within the context of financial digitalisation, data security has become inseparable from asset protection, as information leakage or system disruption may result in the loss of economic value and cause financial harm to consumers.

The Regulation further prohibits the use of unfair standard contractual clauses that are detrimental to consumers, particularly provisions that seek to exempt financial institutions from liability arising from system failures or internal negligence. Through these provisions, POJK No. 22 of 2023 strengthens the legal position and bargaining power of customers as legal subjects entitled to protection of both their financial assets and personal data. Furthermore, financial institutions are required to establish

[16] Nurfitriyani Nurfitriyani et al., "Analisis Hukum Ekonomi Terhadap Peraturan Perbankan Dalam Perlindungan Hukum Nasabah," *Jurnal IUS Kajian Hukum Dan Keadilan* 9, no. 2 (2021): 458–71, https://doi.org/10.29303/ius.v9i2.911. p.470

transparent and effective complaint-handling and dispute resolution mechanisms, thereby ensuring that consumers have access to appropriate legal remedies when violations affect the security of their assets.

In addition, the Financial Services Authority (*OJK*) is entrusted with a central role in supervising the market conduct of Financial Services Business Actors. OJK is empowered to conduct supervisory inspections, investigations, and regulatory examinations, as well as to impose administrative sanctions on financial institutions that violate consumer protection requirements or are found to have failed in safeguarding customers' assets. This demonstrates that POJK No. 22 of 2023 is not merely declaratory in nature but establishes a comprehensive regulatory framework supported by effective enforcement mechanisms.

Customer privacy concerns an individual's right to maintain the confidentiality of personal information and financial activities. This principle is founded upon the right to privacy as a fundamental human right recognised under Article 28G(1) of the 1945 Constitution of the Republic of Indonesia and is further reinforced by Law No. 27 of 2022 concerning Personal Data Protection (Personal Data Protection Law). From a conceptual perspective, customer privacy and customer data are closely interconnected and mutually reinforcing. Privacy constitutes a fundamental right, whereas customer data constitute the legal object of protection through which that right is given concrete expression. Consequently, any breach of the security of customers' personal data simultaneously constitutes an infringement of their right to privacy. Accordingly, banking institutions are required to incorporate privacy principles into their data governance frameworks by ensuring that data management practices are founded upon security, transparency, and accountability.

Customers' personal data include any information capable of identifying an individual, such as names, bank account numbers, National Identity Numbers (*Nomor Induk Kependudukan-NIK*), residential addresses, and financial transaction records. Within the context of digital banking, banks act as Personal Data Controllers and are therefore legally required to collect personal data lawfully and transparently, process such data solely for specified and legitimate purposes, store and process personal data using reliable information security systems, and erase personal data once it is no longer necessary for the purposes for which it was collected.

With respect to customers' personal data, Financial Services Authority Regulation (POJK) No. 44 of 2024 concerning Bank Secrecy defines bank secrecy in Article 1(11) as information relating to deposit customers and their deposits, as well as investor customers and their investments. Such information falls within the scope of customer data protected under the banking secrecy regime. Furthermore, Article 2(1) of POJK No. 44 of 2024 expressly provides that banks and their affiliated parties are legally obligated to maintain the confidentiality of information relating to deposit customers and their deposits and/or investor customers and their investments.

Law No. 11 of 2008 concerning Electronic Information and Transactions, as amended by Law No. 19 of 2016 (the Electronic Information and Transactions Law), provides the principal legal framework governing the rapid development of information and communication technology, including digital banking and electronic transactions. Article 26(1) of the Electronic Information and Transactions Law provides that "Unless otherwise stipulated by laws and regulations, any use of information through electronic media involving a person's personal data shall be subject to the consent of the data subject." Accordingly, no person or entity, including banking institutions, may collect, use, disclose, or otherwise process customers' personal data without the customer's valid and informed consent, except where otherwise authorised by law.

Within the context of digital banking services, this provision requires that customers' personal information—including identity details, bank account numbers, identity documents, and transaction histories—must not be disclosed to third parties without a clear legal basis. Banks are further required to adopt comprehensive privacy policies and robust data security systems, supported by effective electronic system protection mechanisms designed to prevent data breaches, misuse of personal information, and unauthorised access to customers' confidential information.

Law No. 27 of 2022 concerning Personal Data Protection constitutes Indonesia's comprehensive national legal framework governing the protection and governance of personal data. The Law guarantees legal protection for the rights of personal data subjects, including banking customers, by establishing a range of fundamental rights, such as the right to obtain information regarding the processing of personal data, the right to rectify and erase personal data, and the right to withdraw consent to the processing of personal data, as provided under Articles 5–15 of the Personal Data Protection Law. In addition, Articles 19–54 impose statutory obligations upon Personal Data Controllers and Personal Data Processors to ensure that the collection, storage, processing, and use of personal data are conducted in a lawful, limited, proportionate, and secure manner, supported by appropriate safeguards for electronic information security. Within the context of digital banking, these provisions require banks to maintain the security and confidentiality of customers' personal data and to prevent data breaches, unauthorised access, or misuse of personal information by unauthorised parties.

The enactment of the Personal Data Protection Law also signifies a fundamental shift in Indonesia's regulatory paradigm from a fragmented, sector-based approach to a more comprehensive data governance framework. Within the context of digital banking, personal data are no longer regarded merely as confidential customer information but as strategic digital assets requiring protection throughout their entire lifecycle, including collection, processing, storage, transfer, and deletion. Such protection also requires an integrated data governance framework that ensures interoperability, accountability, and secure data sharing across the digital financial ecosystem, particularly in the implementation of open banking services.[17] Consequently, digital banks are expected not only to comply with statutory obligations concerning personal data protection but also to embed privacy, accountability, transparency, and security into their institutional

[17] Billiam et al., "The Urgency of Open Application Programming Interface Standardization in the Implementation of Open Banking to Customer Data Protection for the Advancement of Indonesian Banking," *Padjadjaran Jurnal Ilmu Hukum* 9, no. 1 (2022): 69–91, https://doi.org/https://doi.org/10.22304/pjih.v9n1.a4.

governance, operational processes, and technological infrastructure. This governance-oriented approach is consistent with the view that the acceleration of digital banking transformation must be accompanied by a strengthened regulatory framework that integrates prudent corporate governance, information technology risk management, and consumer data protection as inseparable components of a sustainable digital financial ecosystem.[18] This paradigm reflects the growing recognition that effective personal data governance constitutes an essential prerequisite for strengthening cybersecurity resilience, maintaining consumer trust, and ensuring the sustainable development of digital banking services.

The Personal Data Protection Law further establishes dispute resolution mechanisms in cases involving violations of the rights of personal data subjects through both administrative and judicial proceedings, as provided under Article 64. Data subjects are entitled to lodge complaints with the competent personal data protection authority or pursue legal proceedings to obtain compensation for losses arising from unlawful data processing. Furthermore, to ensure effective legal deterrence, the Law prescribes administrative sanctions under Article 57 and criminal sanctions under Articles 67–73, including imprisonment for up to six years and/or fines of up to IDR 6 billion. From a legal perspective, the enactment of the Personal Data Protection Law constitutes a significant juridical foundation for strengthening the protection of privacy, digital asset security, and customers' personal data within Indonesia's digital banking sector. Its effective and consistent implementation is expected to enhance legal certainty and consumer protection while reinforcing public confidence in the national digital financial system.

In the era of banking digitalisation, risk management has become an essential regulatory instrument for maintaining the stability of financial institutions while safeguarding consumers' interests. Contemporary banks perform not only their traditional financial intermediation function but also serve as custodians and managers of customers' highly sensitive personal and financial information. Consequently, the effective management of risks relating to customers' assets, privacy, and personal data has become both a legal obligation and an ethical responsibility for every banking institution operating in Indonesia.

In general, banking risk management refers to a systematic process of identifying, measuring, monitoring, and controlling risks arising from banking operations. This obligation is regulated under Financial Services Authority Regulation (POJK) No. 18/POJK.03/2016 concerning the Implementation of Risk Management for Commercial Banks, which requires every bank to establish adequate risk management policies, procedures, and internal control systems capable of managing risks that may affect the bank's business continuity and undermine public confidence. From a consumer protection perspective, the risks requiring effective management extend beyond financial risks to include legal, reputational, operational, and information technology risks, all of

[18] Lastuti Abubakar and Tri Handayani, "Penguatan Regulasi: Upaya Percepatan Transformasi Digital Perbankan Di Era Ekonomi Digital," *Masalah-Masalah Hukum* 51, no. 3 (2022): 259–70, https://doi.org/https://doi.org/10.14710/mmh.51.3.2022.259-270.

which are closely associated with the protection of customers' assets and the confidentiality of their personal data.[19]

Legal Issues Concerning the Protection of Consumers' Assets, Privacy, and Personal Data in Indonesia's Digital Banking Sector

The legal challenges associated with implementing the principles governing the protection of consumers' assets, privacy, and personal data in Indonesia's digital banking sector primarily arise from regulatory inconsistencies, weak enforcement mechanisms, and inadequate implementation of data security standards. Although the issuance of Financial Services Authority Regulation (*POJK*) No. 22 of 2023 concerning Consumer and Public Protection in the Financial Services Sector and Law No. 27 of 2022 concerning Personal Data Protection (Personal Data Protection Law) represents a significant advancement in Indonesia's consumer protection regime, these legislative instruments have not yet fully addressed the complex legal relationships among banks, customers, and third-party digital service providers. As observed by Lestari, regulatory overlap remains between the Financial Services Authority (OJK) and the Ministry of Communication and Informatics (*Kominfo*) with respect to the supervision of personal data protection, resulting in legal uncertainty for consumers using digital banking services.[20]

Although Indonesia's regulatory framework—including the Personal Data Protection Law, the Banking Law, the Electronic Information and Transactions Law, and various Financial Services Authority Regulations (POJK)—establishes the legal basis for protecting customers' personal data and privacy, significant legal challenges continue to arise in practice. While Law No. 27 of 2022 mandates the establishment of a national institution responsible for personal data protection, Indonesia has yet to establish an independent Data Protection Authority (DPA) comparable to those operating in many other jurisdictions. The absence of such an independent supervisory authority has resulted in the fragmentation of regulatory oversight, with responsibilities relating to supervision, complaint handling, investigation of violations, and the enforcement of administrative sanctions remaining dispersed among multiple government institutions rather than being exercised by a specialised authority. Consequently, inter-agency coordination remains less effective, thereby reducing legal certainty and potentially weakening the protection afforded to digital banking customers in cases involving personal data breaches or misuse.[21]

One of the most significant legal concerns is the increasing incidence of customer data breaches resulting from cyberattacks. The cyberattack against Bank Syariah Indonesia in

---

[19] Muhamad Amirulloh et al., "Legal Basis and Readiness of the Banking Sector in Implementing Privacy Reliability Certification," *Jurnal IUS Kajian Hukum dan Keadilan* 13, no. 3 (2025): 545–58, https://doi.org/10.29303/ius.v13i3.1777.

[20] D. Lestari, "Sinkronisasi Kewenangan OJK Dan Kominfo Dalam Pengawasan Perlindungan Data Pribadi Di Sektor Keuangan Digital," *Jurnal Hukum & Regulasi Keuangan* 6, no. 1 (2024): 45–62.

[21] Uu Nurul Huda et al., "Legal Protection for Personal Data Leaks and Its Implications for Citizens' Privacy Rights within the Framework of the Indonesian Legal State," *Jambura Law Review* 8, no. 1 (2026): 144–59, https://doi.org/10.33756/jlr.v1i1.32666.

2023 illustrates the continuing inadequacy of cybersecurity safeguards and institutional preparedness within Indonesia's digital banking sector.[22] Against this background, several key legal issues continue to impede the effective implementation of the principles governing the protection of consumers' assets, privacy, and personal data in Indonesia's digital banking activities.

1. Regulatory Gaps and Overlapping Regulatory Frameworks

The rapid digitalisation of financial services has substantially increased the volume and complexity of personal data processing, thereby creating an urgent need for a comprehensive, sector-specific, and effective legal framework for personal data protection.[23] In practice, however, the Financial Services Authority (*OJK*), as the regulator and supervisor of financial institutions, and the Ministry of Communication and Informatics (*Kominfo*), as the authority responsible for personal data governance, frequently exercise overlapping regulatory powers. For example, when a personal data breach occurs within a digital banking system, both institutions possess separate statutory mandates for investigation and regulatory enforcement. *Kominfo* exercises its authority pursuant to the Personal Data Protection Law, whereas OJK relies on Financial Services Authority Regulation (*POJK*) No. 22 of 2023 and the regulatory framework governing information technology risk management. This institutional overlap creates legal uncertainty, as the implementation of data protection obligations within the banking sector continues to face significant regulatory and institutional challenges. At present, Indonesia lacks a single authority responsible for enforcing financial data protection laws. Consequently, financial institutions are frequently required to report the same incident to multiple regulators, resulting in procedural duplication, delayed mitigation efforts, and a less effective regulatory response to personal data breaches. Existing Indonesian law has not kept pace with the digital economy, leaving personal data protection in digital transactions inadequately addressed.[24]

Regulatory fragmentation is evident not only in the distribution of institutional authority but also in the substantive legal framework itself. POJK No. 22 of 2023 primarily focuses on general consumer protection within the financial services sector, whereas the Personal Data Protection Law establishes a cross-sectoral legal framework for personal data protection without specifically addressing the distinctive characteristics and risks associated with digital financial services. Consequently, Indonesia has yet to establish a uniform national standard governing the protection of customers' data in digital banking, particularly with respect to information system security, data retention requirements, and the processing of customer data by third-party service providers, including cloud

---

[22] Ilman Maulana Kholis, "Perlindungan Data Pribadi Dan Keamanan Siber Di Sektor Perbankan: Studi Kritis Atas Penerapan UU PDP Dan UU ITE Di Indonesia," *STAATSRECHT Jurnal Hukum Kenegaraan Dan Politik Islam* 4, no. 2 (2024).

[23] N. Wardhono, R. D. T. K., Badrawani, W., Deviana, A., Pramudyastuti, M., & Shalehanti, "Pelindungan Data Pribadi Di Bank Indonesia Dan Lembaga Jasa Keuangan: Rekomendasi Kebijakan Dan Teknis Pengaturan," *(Working Paper). Bank Indonesia.*, 2024.

[24] Abdul Mujib, "The Failure of Indonesian E-Commerce Law in Adapting to Digital Economy," *Ijtihad : Jurnal Wacana Hukum Islam Dan Kemanusiaan* 25, no. 2 (2025): 213–30, https://doi.org/10.18326/ijtihad.v25i2.213-230.

computing providers and fintech aggregators.[25] These differences in regulatory scope and legal definitions create legal gaps that may enable financial service providers to evade liability in cases involving personal data breaches or the misuse of customer information.[26]

These circumstances demonstrate that Indonesia's legal system continues to experience a significant regulatory harmonisation deficit, both vertically, between statutes and their implementing regulations, and horizontally, among government agencies and sectoral regulatory authorities.[27] Strengthening the legal framework governing corporate governance, risk management, and personal data protection therefore constitutes a fundamental prerequisite for accelerating the digital transformation of Indonesia's banking sector. In the absence of a coherent regulatory framework, consumers face uncertainty regarding the authority responsible for providing legal redress when their privacy rights are violated. Moreover, overlapping regulatory mandates undermine public confidence in the security of digital banking systems, thereby posing broader risks to the stability, integrity, and reputation of Indonesia's financial system.

Accordingly, Indonesia's legal policy requires a comprehensive process of regulatory harmonisation supported by a clearly defined institutional coordination mechanism involving the Financial Services Authority (*OJK*), the Ministry of Communication and Informatics (*Kominfo*), and Bank Indonesia. Integrating the supervision of financial data under the principle of "one data, one regulator" offers a potential solution for reducing regulatory duplication while strengthening the effectiveness of legal protection for digital banking consumers. This approach also points to the need for a specialised financial data protection authority operating within an integrated national legal framework. Ultimately, regulatory harmonisation and legal consistency constitute essential prerequisites for developing a digital banking ecosystem that is secure, transparent, accountable, and capable of providing effective legal protection for all consumers.

2. Cybersecurity Vulnerabilities

Beyond regulatory concerns, risk management and the cultivation of a robust security culture constitute critical challenges within Indonesia's digital banking sector. In practice, the legal protection of customers' personal data depends not only on the existence of an adequate regulatory framework but also on banks' ability to implement comprehensive, measurable, and sustainable cybersecurity risk management systems.[28] Nevertheless, many banking institutions continue to regard data security as merely a technical function rather than as an integral component of corporate governance.[29] Studies of several

---

[25] Arief Budiono Wardah Yuspin, Kelik Wardiono, Aditya Nurrahman, "Personal Data Protection Law in Digital Banking Governance in Indonesia," *Jurnal Studia Juridica Lublinen* 32, no. 1 (2023).

[26] Umi Khaerah Pati and Anugrah Muhtarom Pratama, "Indonesia's Open Banking Future: Designing Effective Regulatory Approaches," *Jambe Law Journal* 8, no. 1 (2025): 27–60, https://doi.org/10.22437/home.v8i1.371.

[27] Lastuti Abubakar and Tri Handayani, "Penguatan Regulasi: Upaya Percepatan Transformasi Digital Perbankan Di Era Ekonomi Digital."

[28] H. Fonda and Z. A. Hoesein, "Pertanggungjawaban Bank dalam Menjamin Keamanan Data Nasabah di Era Digitalisasi Perbankan," *Jurnal Retentum* 4, no. 2 (2024): 25–39.

[29] T. M. Y. Apsari, R. D., & Khudri, "An Evaluation of Cybersecurity Risk Management Implementation at Bank Pembangunan XYZ. Global," *Journal of Industrial Economics and Accounting* 3, no. 2 (2024): 45–59.

regional banks indicate that the implementation of cybersecurity risk management frameworks remains fragmented, particularly in the detection and response functions. Consequently, the legal responsibility of banks for safeguarding customers' personal data remains inadequately defined, as Indonesia has yet to establish a sufficiently robust supervisory mechanism to ensure the comprehensive implementation of cybersecurity risk management across the banking sector.

Cybersecurity vulnerabilities are further exacerbated by the extensive interconnectivity between banks and third-party service providers, including fintech companies, payment gateway operators, and cloud service providers. Cross-institutional digital collaboration in the absence of harmonised cybersecurity standards creates a chain vulnerability, whereby a security failure affecting one entity may generate systemic risks across the broader financial ecosystem.[30] Moreover, many Indonesian banking institutions continue to rely extensively on third-party service providers without implementing comprehensive data processing agreements that clearly allocate responsibilities for the protection and processing of personal data.[31] Consequently, legal responsibility becomes uncertain when personal data breaches occur within outsourced or interconnected digital services. These circumstances underscore the urgent need to harmonise Law No. 27 of 2022 concerning Personal Data Protection (Personal Data Protection Law) with Financial Services Authority Regulation (POJK) No. 22 of 2023 to strengthen legal certainty, enhance regulatory accountability, and ensure effective legal protection for consumers within Indonesia's digital banking ecosystem.[32]

3. Weaknesses in Legal Enforcement

The legal framework governing the protection of customers' personal data and privacy in Indonesia's digital banking sector has undergone significant development in recent years. Legislative instruments such as the Personal Data Protection Law, the Electronic Information and Transactions Law, and various Financial Services Authority Regulations (POJK) impose legal obligations upon banks and digital financial institutions to maintain the security of information systems and assume responsibility for the misuse of personal data. Nevertheless, studies indicate that the enforcement of these regulatory instruments remains deficient, particularly with respect to providing effective legal protection for consumers who become victims of personal data breaches. The 2023 cyberattack against Bank Syariah Indonesia, for example, illustrates that although a comprehensive regulatory framework governing personal data protection exists, the implementation of regulatory requirements and supervisory oversight of banks' compliance with cybersecurity standards remain inadequate. Consequently, affected customers continue to encounter significant difficulties in pursuing legal remedies and obtaining

[30] D. Wulandari Utami, G., Ma'ruf, H., & Yulianti, "Perlindungan Terhadap Nasabah Akibat Serangan Siber: Studi Di Bank Syariah Indonesia KC Pekalongan Pemuda," *Jurnal El-Hisbah* 12, no. 1 (2024): 67–80.

[31] M. D. Firdaus, S. E., Ramadhani, A., & Putri, "Implementasi Teknologi Untuk Penguatan Keamanan Data Pribadi Nasabah Dalam Sektor Perbankan," *Jurnal Inovasi Hukum Dan Teknologi* 3, no. 2 (2024): 115–29.

[32] Afif Noor et al., "Digital Economy Regulation and Consumer Rights Protection: Realizing Security in Financial Technology Transactions," *Lex Scientia Law Review* 9, no. 2 (2025): 1324–75, https://doi.org/10.15294/lslr.v9i2.24927.

compensation for losses arising from data breaches.[33] Furthermore, a legal gap persists concerning the civil liability of banks for material losses suffered by customers because of cybersecurity incidents.[34] Although many banks have adopted internal safeguards such as data encryption and multi-factor authentication, these technical measures are insufficient in the absence of effective enforcement mechanisms, meaningful sanctions, and clearly defined compensation schemes for victims of privacy violations.

The weaknesses in legal enforcement stem from a combination of structural and operational factors. First, the technical capacity of law enforcement agencies remains inadequate for investigating and prosecuting cybercrime, particularly with respect to specialised expertise in digital forensics, electronic evidence, and cyber investigations.[35] These limitations impede the effective investigation and prosecution of cybersecurity offences. Although specialised institutions such as the National Cyber and Crypto Agency (Badan Siber dan Sandi Negara—BSSN) have been established, their institutional capacity, technological infrastructure, and human resources remain insufficient to address increasingly sophisticated cyber threats comprehensively.[36]

Second, significant deficiencies persist in incident reporting and transparency. Many banks and financial institutions fail to notify customers or the public promptly following the occurrence of personal data breaches, and in some cases, disclosure is delayed until institutional reputation is placed at risk. Operational requirements concerning mandatory breach notification remain insufficiently developed, resulting in consumers being deprived of timely information necessary to protect their legal rights and pursue appropriate legal remedies. Consequently, in several high-profile data breach incidents, official reporting and legal responses have been delayed and characterised by limited transparency.[37]

Third, the existing regime of criminal and administrative sanctions is widely regarded as inadequate to achieve an effective deterrent effect. In many regulatory instruments, enforcement relies predominantly upon administrative measures, such as warnings and relatively modest financial penalties, rather than criminal sanctions or civil remedies capable of providing meaningful compensation to affected consumers. For example, although Indonesia's regulatory framework governing peer-to-peer (P2P) lending

---

[33] R. Antoine, R. A., Rahmawati, D., & Putri, "Penyalahgunaan Data Pribadi Dalam Teknologi Transaksi Digital Di Industri Perbankan Digital (Studi Kasus PT Bank Syariah Indonesia).," *Jurnal Manajemen Dan Ilmu Administrasi* 12, no. 3 (2023): 77–92.

[34] Z. A. Fonda, H., & Hoesein, "Pertanggungjawaban Bank Dalam Menjamin Keamanan Data Nasabah Di Era Digitalisasi Perbankan.," *Jurnal Retentum* 4, no. 2 (2024): 25–39.

[35] Ismail Marzuki et al., "Digital Evidence Management in the Criminal Justice System: Towards a Fair and Technology-Responsive Legal Framework Author," *Indonesian Journal of Criminal Law Studies* 11, no. 1 (n.d.): 467–514; Siti Nur Shoimah, "Freedom of Contract in the Digital Age: Perspectives on the Indonesian Civil Code and Fiqh Muamalah," *Trunojoyo Law Review* 8, no. 1 (2026): 59–94, https://doi.org/10.21107/tlr.v8i1.32568; Afif Noor et al., "Digital Economy Regulation and Consumer Rights Protection: Realizing Security in Financial Technology Transactions," *Lex Scientia Law Review* 9, no. 2 (2025): 1324–75, https://doi.org/10.15294/lslr.v9i2.24927.

[36] Adinda Lola Sariani Dinda, "Efektivitas Penegakan Hukum Terhadap Kejahatan Siber Di Indonesia," *AL-DALIL: Jurnal Ilmu Sosial, Politik, Dan Hukum* 2, no. 2 (2024): 69–77.

[37] A. R. Azmi, M. N. A., Hidayat, M. S., & Luthfi, "Analisa Kasus Kebocoran Data Pada Bank Indonesia Dalam Sistem Perbankan.," *Jurnal Manajemen Dan Ilmu Administrasi* 13, no. 1 (2024): 55–70.

includes penal provisions addressing unlawful data practices, empirical evidence indicates that enforcement has remained relatively weak and insufficiently robust to deter the misuse of personal data effectively.[38]

Fourth, legal protection remains inadequate for victims of mobile banking fraud, primarily because of uncertainty over the allocation of legal responsibility, evidentiary difficulties, and the complexity of litigation procedures.[39] Customers who become victims of fraudulent transactions frequently encounter substantial obstacles in proving negligence on the part of banking institutions and securing compensation through either civil or criminal proceedings.[40]

These circumstances demonstrate that the enforcement of laws governing cybersecurity violations within Indonesia's digital banking sector continues to face significant institutional and regulatory challenges. Strengthening legal enforcement therefore requires a comprehensive strategy that includes enhancing the technical expertise and institutional capacity of law enforcement authorities, imposing more effective and proportionate sanctions, establishing transparent and mandatory incident reporting mechanisms, and ensuring greater legal certainty through a coherent and harmonised regulatory framework. Equally important is the harmonisation of existing legislation to eliminate regulatory inconsistencies and legal loopholes that may otherwise be exploited by perpetrators of personal data violations, while ensuring that affected consumers have effective access to justice and appropriate legal remedies.

4. Lack of Transparency and Accountability in Digital Banking

The digital transformation of Indonesia's banking sector has fundamentally reshaped the delivery of financial services. While digital innovation has enhanced convenience, operational efficiency, and financial inclusion, it has also generated significant legal concerns regarding the transparency and accountability of banking institutions, particularly in relation to the management of customers' personal data and financial information.[41] Legislative and regulatory instruments, including the Personal Data

[38] M. N. Rifa, F., & Hidayati, "Kebijakan Penal Dalam Perlindungan Data Pribadi Nasabah Fintech Lending Di Indonesia.," *Binamulia Hukum* 13, no. 2 (2024): 461–81.

[39] Uu Nurul Huda et al., "Legal Protection for Personal Data Leaks and Its Implications for Citizens' Privacy Rights Within The Framework of The Indonesian Legal State," *Jambura Law Review* 1, no. 1 (2026), https://doi.org/10.33756/jlr.v1i1.32666; Heppy Endah Palupy et al., "Personal Data Protection Governance in the Asia Pacific Region: A Review of the Scope, Effectiveness, and Legal Challenges," *Volksgeist: Jurnal Ilmu Hukum Dan Konstitusi*, June 27, 2026, 197–225, https://doi.org/10.24090/volksgeist.v9i1.15362; Noor et al., "Digital Economy Regulation and Consumer Rights Protection"; Mourad Benseghir et al., "REGULATIONS AND CONSUMER RIGHTS IN E-COMMERCE: A Comparative Analysis Between UAE and Indonesia," *Jurisdictie: Jurnal Hukum Dan Syariah* 16, no. 2 (2025): 374–410, https://doi.org/10.18860/j.v16i2.33063.

[40] Y. Siregar, "Analisis Yuridis Tanggung Jawab Bank Atas Tindak Fraud Pada Transaksi Mobile Banking Serta Upaya Penegakan Hukumnya.," *Jurnal Ekonomi Dan Hukum Islam* 8, no. 1 (2024): 33–49.

[41] Umi Khaerah Pati and Anugrah Muhtarom Pratama, "Indonesia's Open Banking Future: Designing Effective Regulatory Approaches," *Jambe Law Journal* 8, no. 1 (2025): 27–60, https://doi.org/10.22437/home.v8i1.371; Muhamad Amirulloh et al., "Legal Basis and Readiness of the Banking Sector in Implementing Privacy Reliability Certification," *Jurnal IUS Kajian Hukum Dan Keadilan* 13, no. 3 (2025): 545–58, https://doi.org/10.29303/ius.v13i3.1777; Souad Ezzerouali et al., "Can Moroccan Law Ensure Substantive Justice

Protection Law, Financial Services Authority Regulation (POJK) No. 22 of 2023, and the Digital Banking Transformation Blueprint issued by the Financial Services Authority (OJK), have established the legal framework for promoting the principles of transparency and institutional accountability within the financial services sector. Nevertheless, the practical implementation of these principles remains suboptimal, revealing a persistent gap between the normative legal framework and its effective implementation in practice.[42]

The regulatory framework governing transparency and accountability in digital banking remains sector-specific, fragmented, and insufficiently integrated across regulatory institutions.[43] Consequently, there is no uniform standard governing the implementation of disclosure obligations, particularly with respect to personal data protection policies, cybersecurity risk management, and the involvement of third-party service providers. This fragmented regulatory environment affords banking institutions considerable discretion in determining the scope of information disclosure, thereby creating an information asymmetry between banks and consumers and weakening consumers' ability to make informed decisions regarding the management of their personal data.

The legal responsibility of banks for personal data breaches or financial losses suffered by customers is frequently not accompanied by transparent reporting and effective accountability mechanisms.[44] Many digital banks fail to disclose personal data breaches openly, either to the public or, in some cases, to the competent regulatory authorities. Such practices reflect a weak culture of institutional accountability, as banks may seek to conceal failures in their internal security systems to preserve their corporate reputation. Furthermore, many mobile banking platforms operating in Indonesia do not provide customers with adequate information regarding the collection, processing, storage, and use of their personal data. This lack of transparency exacerbates information asymmetry, leaving customers in a weaker position because they cannot fully understand how their personal information is processed, shared, and protected by banking institutions.[45]

From the perspective of corporate governance, the implementation of accountability principles remains largely administrative and formalistic. Compliance reports and internal audits are routinely prepared; however, they are not consistently followed by meaningful corrective actions when violations of personal data protection obligations are identified. Similarly, internal oversight mechanisms often lack sufficient enforcement authority to ensure compliance with personal data protection policies, thereby limiting

in Protecting Private Life from AI's Impact?," *Substantive Justice International Journal of Law* 8, no. 1 (2025), https://doi.org/10.56087/substantivejustice.v8i1.333.

[42] OJK, *Cetak Biru Transformasi Digital Perbankan* (Otoritas Jasa Keuangan, 2023).

[43] H. Sriono, R., Risdalina, Kusno, I. K. M., & Syahyunan, "Uncovering Legal Gaps in Digital Banking: Customer Protection and Bank Accountability in Indonesia.," *Litigasi: Jurnal Hukum* 25, no. 1 (2024): 134–50.

[44] M. A. Widya Annafa, S., Simanjuntak, H. P. G. H., & Ayudia, "Tanggung Jawab Hukum Bank Dalam Kasus Kebocoran Data Nasabah.," *Jurnal Multidisiplin Ilmu Akademik* 5, no. 2 (2023): 77–89.

[45] N. Abrianto, H., Farhani, N. H., Bidhari, S. C., Pasaribu, E. H. H., & Neila, "Transparansi Informasi Penggunaan Aplikasi Mobile Banking Terhadap Perlindungan Konsumen Sektor Jasa Keuangan.," *Prosiding Simposium Nasional Perbankan, Akuntansi, Dan Keuangan. Politeknik Negeri Jakarta.*, 2022.

the effectiveness of institutional accountability within the digital banking sector.[46]

The deficiencies in transparency and accountability are further aggravated by the absence of effective coordination among the Financial Services Authority (OJK), Bank Indonesia (BI), and the Ministry of Communication and Informatics (Kominfo). Each institution exercises regulatory authority within its respective jurisdiction, yet no integrated institutional mechanism exists to coordinate regulatory enforcement when personal data breaches or cybersecurity incidents occur. Consequently, no single institution bears comprehensive responsibility for overseeing and enforcing compliance within Indonesia's digital banking ecosystem.[47]

The lack of transparency and accountability has significant implications for public confidence in Indonesia's digital banking system. When consumers are unable to obtain clear and reliable information regarding the management and protection of their financial assets and personal data, trust in financial institutions inevitably declines. Accordingly, strengthening the legal framework and establishing an integrated supervisory system are essential to ensuring that the principles of transparency and accountability are not merely declaratory but are effectively implemented through independent external audits, mandatory public reporting of cybersecurity incidents, and the consistent application of administrative and criminal sanctions against digital banking institutions that fail to comply with their legal obligations.

5. Low Levels of Consumer Digital Literacy

One of the principal legal challenges affecting the implementation of the principles governing the protection of consumers' assets, privacy, and personal data in Indonesia's digital banking sector is the relatively low level of consumer digital literacy. Despite the rapid advancement of digital banking technologies, significant challenges remain due to the limited ability of many consumers to understand cybersecurity mechanisms, personal data protection, and the legal and technological risks associated with technology-driven financial services. This deficiency substantially increases consumers' exposure to online fraud, identity theft, personal data breaches, and the unlawful exploitation of personal information by malicious actors.[48]

According to the Financial Services Authority (OJK) in its 2022 National Survey on Financial Literacy and Financial Inclusion (Survei Nasional Literasi dan Inklusi Keuangan, SNLIK), Indonesia's financial literacy rate reached only 49.68 per cent, whereas the financial inclusion rate stood at 85.10 per cent. This disparity indicates that a substantial proportion of the population has adopted digital financial services without possessing an adequate understanding of the security principles and legal protections governing their use. Consequently, many consumers continue to neglect essential cybersecurity practices, including the use of strong passwords, multi-factor authentication, and regular

[46] A. Nabila, Z., Virnanda, R. R., Yusuf, F. D., Kusumaningtias, R., & Kusumaningsih, "Peran Prinsip Akuntabilitas Sebagai Strategi Mitigasi Risiko Operasional Pada Bank Digital: Studi Kasus SeaBank Indonesia.," *Jurnal Pendidikan Tambusai* 7, no. 5 (2023): 211–23.
[47] Wildan Muhammad et al., "Analisis Tanggung Jawab Bank Terhadap Kebocoran Data Nasabah: Ditinjau Dalam Perspektif Hukum Perbankan.," *Media Hukum Indonesia* 3, no. 1 (2024): 44–59.
[48] OJK, "Survei Nasional Literasi Dan Inklusi Keuangan 2023."

software updates, thereby increasing their vulnerability to cybercrime.

The limited level of digital literacy also prevents many consumers from distinguishing between legitimate banking applications or official banking websites and fraudulent websites designed to facilitate phishing attacks. As a result, consumers frequently disclose personal information without fully appreciating the implications for the security and confidentiality of their personal data. Under these circumstances, consumer protection measures implemented by banking institutions cannot achieve their intended effectiveness because they remain heavily dependent upon consumers' awareness of, and ability to navigate, digital technologies securely.[49]

Furthermore, many consumers routinely accept terms and conditions governing digital banking services without reading or understanding their contents or legal consequences. This practice has generated significant debate within consumer protection scholarship regarding the extent to which consumers should bear responsibility for consenting to contractual terms they have not read, and the corresponding extent to which financial service providers are legally obliged to ensure that contractual information is presented in a manner that is genuinely comprehensible to consumers.[50]

From the perspective of law and economics, the obligation imposed upon businesses to provide information through mandated disclosure does not necessarily result in effective consumer protection. As argued by Ben-Shahar and Schneider, disclosures that are excessively lengthy, highly technical, and legally complex are frequently ignored by consumers. Consequently, consumer consent often becomes a purely formal act rather than one based upon an informed understanding of the rights, obligations, and risks arising from the contractual relationship.[51] Accordingly, consumer protection in the digital financial services sector cannot rely solely upon the legal presumption that consumers have read and understood all contractual terms before providing their consent.

This view is consistent with Margaret Jane Radin's critique of the widespread use of standard-form contracts in digital transactions. Radin argues that contractual terms unilaterally drafted by businesses rarely provide consumers with a meaningful opportunity either to negotiate contractual provisions or to understand fully the substantive content of the agreement. Under such circumstances, consumers occupy a significantly weaker bargaining position than financial service providers. Accordingly, the State must intervene through appropriate legal and regulatory instruments to ensure that consumers receive effective protection of their rights within the digital marketplace.[52]

---

[49] R. Yuliana, L., & Nandari, "Tantangan Literasi Digital Dalam Perlindungan Konsumen Layanan Keuangan Digital Di Indonesia.," *Jurnal Ekonomi Dan Kebijakan Publik* 14, no. 1 (2023): 33–47.

[50] Omri Ben-Shahar & Carl E. Schneider, *More Than You Wanted to Know: The Failure of Mandated Disclosure*, in *Princeton University Press* (2014).

[51] Omri Ben-Shahar & Carl E. Schneider, *More Than You Wanted to Know: The Failure of Mandated Disclosure*. 33-56

[52] Margaret Jane Radin, *Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law* (Princeton University Press, 2013).

In Indonesia, this approach is reflected in Financial Services Authority Regulation (POJK) No. 22 of 2023 concerning Consumer and Public Protection in the Financial Services Sector, which requires Financial Services Business Actors (Pelaku Usaha Jasa Keuangan—PUJK) to provide information that is accurate, transparent, not misleading, and readily understandable to consumers. Accordingly, the low level of consumer digital literacy cannot serve as a legal basis for shifting the entire responsibility to consumers. Rather, digital banks remain under a statutory obligation to implement adequate security measures and communicate information in an effective and accessible manner so that consumers are able to understand the risks associated with digital banking services and protect themselves against phishing attacks and the misuse of personal data.

A substantial proportion of digital banking users in Indonesia continue to exhibit unsafe digital practices. Many consumers access their banking accounts through public or shared devices, disclose one-time verification codes to third parties, or fail to update their passwords for extended periods. Such practices demonstrate a limited awareness of digital security and significantly increase the risk of financial loss and infringements of consumers' privacy rights.[53]

The low level of digital literacy also undermines public participation in monitoring the implementation of transparency and accountability principles within digital banking institutions. Many customers remain unaware of their rights as personal data subjects, including the right to receive information, the right to give or withhold consent, and the right to object to the unlawful processing or misuse of their personal data. This lack of awareness frequently results in consumers adopting a passive approach and failing to pursue legal accountability when their privacy rights are violated.[54] Consequently, inadequate consumer digital literacy should not be regarded merely as a social challenge but rather as a factor that directly affects the effectiveness of legal enforcement within Indonesia's digital banking sector. Although Financial Services Authority Regulation (POJK) No. 22 of 2023 concerning Consumer and Public Protection in the Financial Services Sector expressly requires financial institutions to provide consumers with adequate education and clear information, the effectiveness of this regulatory framework will remain limited unless accompanied by comprehensive improvements in public digital literacy. Otherwise, the Regulation risks functioning as a predominantly formalistic legal instrument rather than as an effective mechanism for ensuring meaningful consumer protection.

6. Imbalance in the Legal Position Between Banks and Consumers

The imbalance in the legal position between banks as financial service providers and consumers as users of digital banking services constitutes one of the most significant legal challenges within Indonesia's digital banking sector. This imbalance is reflected in the contractual relationship between the parties, unequal access to information, and

---

[53] R. Dewi, P. M., Andini, F., & Syahputra, "Perilaku Digital Konsumen Dan Risiko Keamanan Dalam Penggunaan Layanan Perbankan Online Di Indonesia.," *Jurnal Manajemen Dan Teknologi Informasi* 1, nos. 56–68 (8 AD).

[54] Jefry Buala et al., "Penyalahgunaan Data Pribadi Konsumen Oleh Perusahaan: Kajian Yuridis Dalam Perspektif UU Perlindungan Konsumen Dan UU Perlindungan Data Pribadi.," *Jurnal Pendidikan Indonesia* 6, no. 5 (2025).

consumers' limited capacity to assert and enforce their legal rights. Banks occupy a dominant position owing to their superior technological capabilities, greater legal resources, and a regulatory environment that often affords stronger institutional protection to financial service providers.[55]

Most digital banking service agreements are concluded through standard-form contracts unilaterally drafted by banks, leaving consumers with no meaningful opportunity to negotiate their contractual terms. This practice creates information asymmetry and weakens consumer protection, particularly in cases involving system failures, personal data breaches, or digital fraud.[56] Moreover, contractual clauses limiting or excluding the liability of banks frequently make it difficult for consumers to obtain compensation for losses they have suffered. These circumstances demonstrate that the legal framework intended to protect the weaker party often fails to operate effectively in practice.

From the perspective of financial services regulation, the use of standard-form agreements constitutes a common contractual practice in digital banking. Nevertheless, such agreements must comply with the principles of fairness, balance, transparency, and good faith as required under Financial Services Authority Circular Letter (SEOJK) No. 13/SEOJK.07/2014 concerning Standard Agreements and Financial Services Authority Regulation (POJK) No. 22 of 2023 concerning Consumer and Public Protection in the Financial Services Sector. These regulatory instruments require Financial Services Business Actors (Pelaku Usaha Jasa Keuangan/PUJK) to formulate contractual clauses that do not unreasonably transfer legal responsibilities to consumers, restrict consumers' statutory rights, or create a significant imbalance in the contractual relationship between the parties. Standard agreements must therefore reflect equitable risk allocation while ensuring adequate legal protection for consumers.

In practice, the terms and conditions governing digital banking services continue to include provisions that seek to limit banks' liability for losses arising from account misuse, phishing attacks, system failures, or unauthorised access to customers' accounts. In many instances, these clauses allocate a substantial portion of operational risks to consumers on the assumption that they failed to maintain the confidentiality of their personal credentials, including personal identification numbers (PINs), passwords, or one-time passwords (OTPs), notwithstanding that such incidents may also result from weaknesses in the bank's cybersecurity infrastructure or deficiencies in operational risk management. Contractual provisions that disproportionately shift liability to consumers are inconsistent with the principles governing standard agreements established by the Financial Services Authority, which require contractual fairness and prohibit clauses that unreasonably reduce the accountability of Financial Services Business Actors.

Accordingly, the enforceability of standard-form agreements in digital banking should not be assessed solely on the basis of the principle of freedom of contract under Article 1338 of the Indonesian Civil Code. It must also be evaluated in light of the mandatory

[55] &. Abdurrahman Khalidy Ahmad Farizal, Sudaberi, Febri Aulyandra, Fulthokon Daeli, "PERLINDUNGAN HUKUM TERHADAP KONSUMEN DALAM TRANSAKSI PERBANKAN DIGITAL : TANGGUNG JAWAB BANK DAN HAK NASABAH.," *SYARIAH : Jurnal Ilmu Hukum* 2, no. 4 (2025): 1–6.

[56] M. A. F. Kadari, P. N., Saharuddin, S., & Syahril, "Perlindungan Hukum Nasabah Atas Penggunaan E-Banking .," *Jurnal Litigasi Amsir* 10, no. 2 (2023): 167–79.

regulatory framework governing the financial services sector, particularly POJK No. 22 of 2023 and SEOJK No. 13/SEOJK.07/2014, which require financial institutions to uphold transparency, fairness, accountability, and balanced contractual relations in their dealings with consumers. Consequently, contractual autonomy in digital banking is not absolute but is limited by regulatory obligations designed to ensure responsible risk allocation, institutional accountability, and effective protection of consumers within the digital financial ecosystem.[57]

The imbalance in the legal position between banks and consumers is equally apparent in the dispute resolution process. Although Financial Services Authority Regulation (POJK) No. 22 of 2023 concerning Consumer and Public Protection in the Financial Services Sector establishes mechanisms for consumer complaints and dispute resolution, these procedures do not yet fully guarantee substantive justice, as they continue to be dominated by internal complaint-handling mechanisms administered by financial institutions themselves. Complex evidentiary requirements, the high costs associated with dispute resolution, and consumers' limited legal literacy remain significant barriers to obtaining effective legal redress.[58] These circumstances demonstrate that, notwithstanding the existence of an extensive consumer protection framework, its implementation remains largely formalistic and has yet to recognise consumers as legal subjects possessing a position genuinely equal to that of financial institutions.

Legal Framework Governing the Protection of Consumers' Assets, Privacy, and Personal Data in Malaysia's Digital Banking Sector

Digital banks in Malaysia operate within a comprehensive legal and regulatory framework established through a combination of statutes, regulatory instruments, and central bank policy documents. One of the principal legislative foundations is the Financial Services Act 2013 (FSA), which governs conventional financial services, including banking activities, payment systems, and the issuance of electronic money.[59] The FSA and the Islamic Financial Services Act 2013 (IFSA) constitute the primary statutory framework for conventional and Islamic banking in Malaysia, regulating licensing requirements, prudential standards, supervisory mechanisms, and administrative sanctions. These legislative provisions apply equally to banks operating through digital platforms. Bank Negara Malaysia (BNM) maintains the position that digital banks should be subject to the same prudential principles as conventional banks, while adapting the operational requirements to reflect the distinctive characteristics of digital banking business models.[60] Accordingly, both statutes provide an equivalent legal foundation for conventional and digital banking institutions, with the principal distinction lying in their operational models and the utilisation of digital technologies. As the national financial regulator, BNM is empowered to issue supplementary regulatory

[57] Siti Nur Shoimah, "Freedom of Contract in the Digital Age: Perspectives on the Indonesian Civil Code and Fiqh Muamalah," *Trunojoyo Law Review* 8, no. 1 (2026): 59–94, https://doi.org/10.21107/tlr.v8i1.32568.
[58] E. Hakim, R., Franciska, D., & Hendrotriwidodo, "Perlindungan Hukum Konsumen Terhadap Nasabah Atas Terjadi Fraud Pada Transaksi Bank Digital.," *Jurnal Kajian Sosial Dan Hukum* 6, no. 2 (2024): 201–15.
[59] Shin Associates, *Fintech and Cybersecurity Legal Frameworks and Emerging Regulatory Trends in Malaysia.*, 2025.
[60] Bank Negara Malaysia, *Policy Document on Licensing Framework for Digital Banks*, 2020.

policies to govern emerging business models within the banking sector.

One of the most significant regulatory initiatives is the Policy Document on Licensing Framework for Digital Banks, issued on 31 December 2020. This policy sets out the licensing requirements for digital banks, including the minimum capital requirement of RM100 million during the foundational phase, together with the objective of promoting financial inclusion for underserved and unserved segments of society.[61] The licensing framework reflects a proportionate regulatory approach, designed to facilitate innovation while simultaneously preserving financial system stability and ensuring effective consumer protection.[62] In April 2022, Bank Negara Malaysia granted five digital banking licences to consortiums led by companies including Grab Holdings, AEON Financial Service, and Sea Ltd., demonstrating the practical implementation of this regulatory framework.[63]

Beyond the banking framework itself, the regulation of electronic payment services forms an integral component of Malaysia's digital banking regime. Through the Policy Document on Electronic Money (E-Money) (Revised 2025), Bank Negara Malaysia regulates the issuance of electronic money, the segregation of customer funds (*float segregation*), and operational risk reporting requirements.[64] These regulatory measures are particularly significant because most digital banking services are integrated with electronic wallets (*e-wallets*) and mobile payment applications. In the area of personal data protection, the Personal Data Protection Act 2010 (PDPA) establishes the legal framework governing the collection, processing, use, and storage of customers' personal data. The PDPA requires digital banks to obtain users' explicit consent, implement appropriate technical and organisational data security measures, and report personal data breaches in accordance with the requirements of the competent supervisory authority. Compliance with the PDPA constitutes a fundamental prerequisite for maintaining consumer confidence in Malaysia's digital financial ecosystem.[65]

The integrity of Malaysia's financial system is further safeguarded by the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA), which establishes statutory obligations relating to Know Your Customer (KYC) procedures, the reporting of Suspicious Transaction Reports (STRs), and internal audit requirements applicable to digital financial institutions. In this context, Bank Negara Malaysia actively promotes the implementation of electronic Know Your Customer (e-KYC) mechanisms to facilitate remote customer identification while maintaining the

---

[61] Bank Negara Malaysia, *Policy Document on Licensing Framework for Digital Banks*.
[62] KPMG Malaysia, "Digital Banking (2nd Ed.): Regulatory and Market Perspectives.," *Kuala Lumpur: KPMG.*, 2021.
[63] N. M. Saif, M. A. M., Rahman, M., & Zayed, "Determinants of the Intention to Adopt Digital-Only Banks in Malaysia.," *Sustainability* 14, no. 17 (2022).
[64] Bank Negara Malaysia., "Policy Document on Electronic Money (E-Money) (Revised).," *Kuala Lumpur: Bank Negara Malaysia.*, 2025.
[65] Alibeigi, Ali and Munir, Abu Bakar and Asemi, Adeleh, "Compliance with Malaysian Personal Data Protection Act 2010 by Banking and Financial Institutions, a Legal Survey on Privacy Policies (August 23, 2021).," *International Review of Law, Computers and Technology*, ahead of print, 2021, https://doi.org/https://doi.org/10.1080/13600869.2021.1970936.

effectiveness and integrity of anti-money laundering supervision.[66] Studies indicate that the implementation of e-KYC in Malaysia has strengthened anti-money laundering risk management within the digital banking ecosystem. In addition, Bank Negara Malaysia enforces cybersecurity governance through the Risk Management in Technology (RMiT) Policy Document, which requires digital banks to establish comprehensive technology risk management frameworks, including incident response procedures, cybersecurity controls, and business continuity and system recovery plans to ensure operational resilience in the event of technology-related disruptions.

1. Digital Banking in Malaysia

Digital banking in Malaysia represents more than the technological adaptation of financial service delivery; it reflects a broader systemic transformation shaped by an evolving regulatory framework, market practices, and changing consumer expectations. Teo argues that Bank Negara Malaysia (BNM) has established a regulatory framework founded upon digital banking licensing, consumer protection, and financial inclusion policies, thereby facilitating the emergence of digital-only banks. At the same time, technological innovations—including cloud computing, artificial intelligence (AI), and application programming interfaces (APIs)—have become key enablers of innovation in digital financial services.[67]

Compared with Indonesia, Malaysia shows a higher level of regulatory preparedness and stronger institutional coordination among financial technology (fintech) stakeholders, particularly in the implementation of regulatory sandbox initiatives, electronic Know Your Customer (e-KYC) guidelines, and digital transaction monitoring mechanisms. This integrated regulatory approach has strengthened the governance of digital financial services while fostering innovation within a secure and well-supervised financial ecosystem.[68]

The literature on Islamic digital banking further highlights the distinctive regulatory characteristics required to ensure compliance with the principles of Maqāṣid al-Sharīʿah, particularly in relation to financial inclusion and Sharīʿah compliance. Islamic financial institutions in Malaysia advocate a digital banking operational framework that incorporates the general regulatory standards applicable to fintech and banking services while simultaneously accommodating fundamental Sharīʿah values, including justice (*ʿadl*), public welfare (*maṣlaḥah*), and the prohibition of *ribā* (usury).[69] This dual regulatory approach enables Islamic digital banks to pursue technological innovation

---

[66] M. S. Hannan, M. A., Shahriar, M. A., Ferdous, M. S., Chowdhury, M. J. M., & Rahman, "A Systematic Literature Review of Blockchain-Based e-KYC Systems.," *Computing, 1–30. Advance Online Publication.*, ahead of print, 2023, https://doi.org/https://doi.org/10.1007/s00607-023-01176-8.

[67] Poh-Chuin Teo, "Exploring Digital-Only Banking in Malaysia: Technological Advancements," *Regulatory Landscape, and Business Implications* 16, no. 1 (2025).

[68] R. Diniyya, A. A., Mahdiah, & Wahyudi, "Financial Technology Regulation in Malaysia and Indonesia: A Comparative Study.," *Journal of Islamic Economics, Finance, and Banking* 3, no. 2 (2023).

[69] M. R. Ab. Aziz, "Islamic Digital Banking Framework in Malaysia: A Practitioners' Perspective.," *International Journal of Islamic Economics and Finance Research.*, ahead of print, 2023, https://doi.org/10.53840/ijiefer140.

without compromising their religious and ethical obligations.

2. Protection of Consumers' Assets, Privacy, and Personal Data in Malaysia's Digital Banking Sector

The rapid development of Malaysia's digital banking sector over the past decade has created substantial opportunities for innovation in financial services while simultaneously giving rise to significant legal challenges concerning the protection of consumers' assets, privacy, and personal data. The increasing use of digital applications and online platforms by financial institutions has heightened the risks associated with the misuse of personal data and the unauthorised disclosure of customers' financial information. Consequently, the protection of customers' personal data and financial assets has evolved beyond a purely technological concern to become a matter of legal compliance, risk governance, and public confidence in the digital banking system.[70]

From a legal perspective, Malaysia has established a comprehensive statutory framework governing the protection of personal data and financial assets within the digital financial services sector. The Financial Services Act 2013 (FSA) and the Islamic Financial Services Act 2013 (IFSA) confer regulatory authority upon Bank Negara Malaysia (BNM) to supervise the security, prudential regulation, and risk governance of digital financial institutions. In addition, the Malaysia Deposit Insurance Corporation (Perbadanan Insurans Deposit Malaysia—PIDM) provides deposit protection of up to RM250,000 through the Deposit Insurance System (DIS), which applies equally to conventional banks and digital-only banks, thereby mitigating the risk of financial losses arising from bank failures.

Furthermore, the Personal Data Protection Act 2010 (PDPA) constitutes the principal legislative framework governing the rights of personal data subjects and regulating the manner in which financial institutions collect, process, store, and use personal information. The PDPA expressly requires financial institutions to register as data users and to comply with the principles of transparency, accuracy, security, and lawful processing in the management of personal data.[71] Within the banking sector specifically, the Personal Data Protection Code of Practice for the Banking and Financial Sector supplements these statutory obligations by prescribing additional requirements, including data breach notification procedures and the implementation of robust digital security standards.[72]

In practice, the legal protection of personal data within Malaysia's banking sector has been tested through several significant judicial decisions. One of the most influential is Public Bank Berhad v National Feedlot Corporation Sdn. Bhd. & Ors 5 MLRA 561, in which the Federal Court of Malaysia held that a bank remains legally responsible for the

---

[70] Nurkhairina Binti Noor Sureani, Atikah Shahira Binti Awis Qurni, Ayman Haziqah Binti Azman, Mohd Bahrin Bin Othman, Hariz Sufi bin Zahar, "The Adequacy of Data Protection Laws in Protecting Personal Data in Malaysia," *Malaysian Journal of Social Sciences and Humanities (MJSSH)* 6, no. 10 (2021): 488–95.

[71] Jabatan Perlindungan Data Peribadi Malaysia, "Personal Data Protection Code of Practice for the Banking and Financial Sector.," *Putrajaya: PDP Department.*, 2021.

[72] Bank Negara Malaysia, "Risk Management in Technology (RMiT) Policy Document," *Kuala Lumpur: Bank Negara Malaysia.*, 2022.

unauthorised disclosure of customers' banking information by its employees. The Court held that the duty to preserve the confidentiality of customer information forms part of the bank's fiduciary obligations and can be neither delegated nor avoided, as reflected in Section 97(1) of the Banking and Financial Institutions Act 1989 (BAFIA), the statute in force at the material time. This landmark decision reinforces the principle that the protection of customers' personal data constitutes an enforceable legal right and underscores the obligation of banking institutions to strengthen internal oversight and data security systems.[73]

In addition to the formal legal framework, technical safeguards play a critical role in ensuring the security of consumers' assets and personal privacy. Most digital banks in Malaysia have implemented multi-factor authentication, end-to-end encryption, and artificial intelligence (AI)-driven transaction monitoring systems to mitigate cybersecurity risks.[74] Nevertheless, significant disparities remain in the level of cybersecurity implementation across banking institutions, particularly between established conventional banks with mature technological infrastructure and newly licensed digital banks that remain in the early stages of operational development. Furthermore, studies have found that many banking websites in Malaysia do not fully comply with recognised privacy best practices, particularly regarding the use of cookies and online behavioural tracking technologies, thereby potentially compromising consumers' ability to exercise effective control over their personal data.[75]

Academic scholarship has likewise highlighted the growing challenges associated with safeguarding digital assets in an environment characterised by increasingly sophisticated cyber threats. According to Thong, the adoption of blockchain technology and decentralised systems offers a promising approach to strengthening asset protection and personal data privacy by enhancing transparency, preserving transaction integrity, and increasing resistance to unauthorised alteration of data.[76] However, the implementation of such technologies must remain harmonised with Malaysia's domestic regulatory framework, including the Personal Data Protection Act 2010 (PDPA) and Bank Negara Malaysia's Risk Management in Technology (RMiT) Policy Document. Accordingly, technological innovation and regulatory development must evolve in parallel to ensure that the digital financial system remains secure, resilient, and trustworthy.

Beyond legal and technological considerations, ethical governance has emerged as an equally important dimension of consumer protection in digital banking. In practice, digital banks are expected not only to comply with applicable statutory and regulatory requirements but also to develop a governance culture grounded in data ethics, encompassing the principles of fairness, algorithmic transparency, and accountability in

[73] Jabatan Perlindungan Data Peribadi Malaysia, "Personal Data Protection Code of Practice for the Banking and Financial Sector."

[74] M. K. Krishnan, S., & Kasiran, "Comparison of Security Measures in Online Banking Sector Malaysia.," *Borneo International Journal* 6, no. 3 (2023): 43–48.

[75] S. L. Tay, Y. H., Ooi, S. Y., Pang, Y. H., Gan, Y. H., & Lew, "Ensuring Privacy and Security on Banking Websites in Malaysia: A Cookies Scanner Solution.," *Journal of Informatics and Web Engineering* 2, no. 2 (2023): 153–67.

[76] M. S. Thong, "Blockchain Technology and Financial Inclusion in Malaysia and Singapore: Transforming Regulatory and Shariah Compliance.," *Singapore: Springer Nature.*, 2025.

automated decision-making processes.[77] This approach is consistent with the principle of responsible innovation promoted by Bank Negara Malaysia, which emphasises that technological advancement must not come at the expense of consumers' fundamental rights to privacy and financial security. Viewed from this perspective, the protection of consumers' assets, privacy, and personal data in Malaysia's digital banking sector constitutes a multi-layered governance framework integrating law, technology, institutional governance, and ethical standards. Although Malaysia has established a relatively comprehensive regulatory framework, significant challenges remain, including the effective enforcement of data protection laws, limited public awareness of digital privacy rights, and the need for stronger institutional coordination among Bank Negara Malaysia, Cyber Security Malaysia, and the Department of Personal Data Protection. Many digital technology users remain unaware that seemingly ordinary online conduct, such as disclosing account credentials in response to a deceptive request, may constitute phishing and other prohibited acts under the Electronic Information and Transactions Law, leaving them more vulnerable to personal data misuse in digital financial services.[78] Accordingly, strengthening institutional capacity, improving digital privacy literacy, and adopting internationally recognised information security standards, including ISO/IEC 27001, together with greater alignment with the General Data Protection Regulation (GDPR), represent important strategic measures for sustaining public confidence in Malaysia's digital banking system.[79]

Comparative Analysis of the Protection of Consumers' Assets, Privacy, and Personal Data in Digital Banking: Indonesia and Malaysia

Both Indonesia and Malaysia have experienced rapid digitalisation of their financial sectors; however, the two jurisdictions have adopted different regulatory approaches in responding to the legal and technological challenges arising from this transformation. Indonesia has generally developed its legal framework through a gradual and sector-specific approach, characterised by a series of dispersed legislative and regulatory instruments. By contrast, Malaysia has established a more integrated regulatory framework supported by relatively stable institutional coordination among the relevant regulatory authorities. These differing regulatory approaches have had direct implications for the effectiveness of consumer protection, the level of legal certainty afforded to financial service providers, and each country's institutional preparedness to address cybersecurity threats and other risks associated with digital financial services.[80]

The legal protection of consumers' assets and personal data within Indonesia's digital

[77] N. A. Mahadzir, A., & Yusof, "Ethical Data Governance in Digital Banking: A Malaysian Perspective.," *Journal of Financial Integrity Studies* 2, no. 1 (2024): 56–71.

[78] dan Transaksi Elektronik di Kelurahan Bener, Yogyakarta," DAS SEIN: Jurnal Pengabdian Hukum dMuhammad Ramadhan et al., "Edukasi Hukum Implikasi Undang-Undang Informasi Dan Transaksi Elektronik Di Kelurahan Bener, Yogyakarta," *DAS SEIN: Jurnal Pengabdian Hukum Dan Humaniora* 1, no. 1 (2023): 119–30, https://doi.org/10.33756/jds.v1i1.19442. P. 120

[79] Ampuan Situmeang et al., "Sharenting and Child Privacy: The GDPR as a Benchmark for Indonesian and Thai Legal Frameworks," *Lex Scientia Law Review* 10, no. 1 (2026): 233–58, https://doi.org/10.15294/lslr.v10i1.29211.

[80] Heppy Endah Palupy, Ronald Nawing, and Susi Susantijo, "Personal Data Protection Governance in the Asia Pacific Region: A Review of the Scope, Effectiveness, and Legal Challenges," *Volksgeist: Jurnal Ilmu Hukum dan Konstitusi* 9, no. 1 (2026): 197–225, https://doi.org/10.24090/volksgeist.v9i1.15362.

banking system is dispersed across several legislative and regulatory instruments, including the Personal Data Protection Law, the Electronic Information and Transactions Law, the Banking Law, as well as various regulations issued by the Financial Services Authority (OJK) and Bank Indonesia (BI). This regulatory structure demonstrates that Indonesia continues to treat personal data protection and digital security as components of separate sector-specific legal regimes rather than as elements of a unified regulatory framework. Consequently, the regulation of banking data security often lacks genuinely uniform standards. In practice, this fragmented approach creates broad scope for regulatory interpretation and may give rise to legal uncertainty when violations of privacy rights occur or when consumers suffer losses resulting from failures of electronic systems. The principal points of comparison between the two jurisdictions are summarised in Table 1.[81]

Table 1. *Comparison of the Protection of Consumers' Assets, Privacy, and Personal Data in Digital Banking: Indonesia and Malaysia*

Aspect	Indonesia	Malaysia
Regulatory Framework	The legal framework is dispersed across the Banking Law, the Electronic Information and Transactions Law, the Personal Data Protection Law, the Financial Sector Development and Strengthening Law (P2SK Law), Financial Services Authority (OJK) Regulations, Bank Indonesia Regulations (PBI), and other sector-specific regulatory instruments.	An integrated regulatory framework established through the Financial Services Act 2013 (FSA), the Islamic Financial Services Act 2013 (IFSA), the Personal Data Protection Act 2010 (PDPA), and various policy documents issued by Bank Negara Malaysia (BNM).
Regulatory Model	Predominantly sector-specific and developed incrementally through successive legislative and regulatory reforms.	More integrated, combining financial sector regulation with personal data protection within a coherent regulatory framework.
Personal Data Protection	The Personal Data Protection Law of 2022 recognises the rights of personal data subjects; however, an independent Data Protection Authority (DPA) has yet to be established.	The Personal Data Protection Act 2010 (PDPA) has long been in force and is supported by the Personal Data Protection Commissioner and sector-specific Codes of Practice.
Digital Banking Regulation	No dedicated Digital Banking Act exists; digital banking is regulated through OJK and Bank Indonesia regulations.	Digital banks operate within Bank Negara Malaysia's prudential regulatory framework from the licensing stage onwards.
Cybersecurity	Governed through multiple regulatory instruments, although implementation varies considerably across financial	Regulated comprehensively through the Risk Management in Technology (RMiT) Policy Document.

[81] Mourad Benseghir, Aouatef Zerara, and Maamar Bentria, "Consumer Protection in Digital Markets: A Comparative Legal Analysis of E-Commerce Regulation in the United Arab Emirates and Indonesia," *Jurisdictie: Jurnal Hukum dan Syariah* 16, no. 2 (2025): 374–416, https://doi.org/10.18860/j.v16i2.33063.

	institutions.	
Deposit Protection	The Indonesia Deposit Insurance Corporation (LPS) guarantees customer deposits of up to IDR 2 billion per depositor per bank.	The Malaysia Deposit Insurance Corporation (PIDM) guarantees deposits of up to RM250,000 per depositor per member bank.
Digital Contracts	Governed by the Indonesian Civil Code, the Electronic Information and Transactions Law, and Financial Services Authority Regulation (POJK) No. 22 of 2023 concerning Consumer and Public Protection in the Financial Services Sector.	Governed by general contract law, supplemented by the FSA, IFSA, PDPA, and Bank Negara Malaysia regulatory guidelines.
Enforcement of Personal Data Protection	Supervisory responsibilities remain fragmented across multiple institutions, creating challenges for effective inter-agency coordination.	Supported by coordinated oversight involving the Personal Data Protection Commissioner, Bank Negara Malaysia, and sector-specific Codes of Practice.
Supervisory Approach	Primarily adaptive, with regulatory reforms introduced progressively in response to technological developments.	Emphasises risk management, institutional governance, and regulatory compliance from the initial implementation of digital banking services.
Consumer Protection	Consumer protection has been strengthened through Financial Services Authority Regulation (POJK) No. 22 of 2023 concerning Consumer and Public Protection in the Financial Services Sector and the Personal Data Protection Law; however, implementation continues to face institutional challenges.	Supported by an integrated regulatory framework, prudential supervision, and more detailed technical standards governing the banking industry.

Source: compiled by the authors from the primary legal materials analysed in this study.

By contrast, Malaysia has adopted a more systematic regulatory model through the integration of the Financial Services Act 2013 (FSA), the Islamic Financial Services Act 2013 (IFSA), the Personal Data Protection Act 2010 (PDPA), and a range of policy documents issued by Bank Negara Malaysia (BNM). The relationship between personal data protection legislation and financial sector regulation is embedded within a more coherent and coordinated governance framework. This demonstrates that Malaysia does not regard data security merely as an issue of privacy protection but as an integral component of national financial system stability. Such an approach strengthens consumers' legal position by ensuring that standards governing personal data protection, transaction security, and technology oversight operate within a unified and mutually reinforcing regulatory framework.

A closer comparative analysis reveals that the principal distinction between Indonesia and Malaysia lies not merely in the existence of regulatory instruments but in the underlying orientation of their respective regulatory policies. Indonesia has generally adopted a reactive regulatory approach, whereby legislation is introduced in response to emerging legal issues or significant cybersecurity incidents. This is exemplified by the enactment of the Personal Data Protection Law, which followed a series of large-scale personal data breaches across multiple digital sectors. Malaysia, by contrast, has adopted a preventive regulatory approach, establishing a comprehensive digital governance framework before permitting the large-scale expansion of digital banking services. Malaysia's regulatory framework is therefore more anticipatory in addressing technological risks and cybersecurity threats.

With respect to the protection of consumers' financial assets, both jurisdictions operate deposit insurance schemes designed to mitigate the risks associated with bank failures. In Indonesia, the Indonesia Deposit Insurance Corporation (Lembaga Penjamin Simpanan—LPS) guarantees customer deposits of up to IDR 2 billion, whereas in Malaysia the Malaysia Deposit Insurance Corporation (Perbadanan Insurans Deposit Malaysia—PIDM) provides deposit protection of up to RM250,000. The principal distinction, however, lies in the regulatory treatment of digital banking risks. Malaysia has explicitly incorporated digital banks into its national financial protection framework from the initial stage of digital banking licensing, thereby ensuring that consumer asset protection mechanisms are designed specifically for the digital-only banking business model. By comparison, Indonesia's regulatory framework for digital banks continues to rely substantially upon supervisory paradigms originally developed for conventional banking institutions. Consequently, it has yet to fully accommodate the distinctive risks associated with digital banking, including distributed cyberattacks, large-scale phishing campaigns, and the exploitation of vulnerabilities in application programming interfaces (APIs) used within banking systems.[82]

From the perspective of privacy and personal data protection, Indonesia has made significant legislative progress through the enactment of the Personal Data Protection Law of 2022. The Law recognises a modern catalogue of personal data subject rights, including the right to be informed, the right to restrict the processing of personal data, the right to erasure, and the right to withdraw consent for the processing of personal information. Nevertheless, Indonesia continues to face significant institutional challenges because it has yet to establish a genuinely independent and sufficiently empowered Data Protection Authority (DPA). Consequently, the effective implementation of personal data protection remains heavily dependent upon inter-agency coordination, which has frequently proven to be fragmented and ineffective. This situation demonstrates that, although Indonesia has made considerable normative progress in strengthening its legal framework, it has not yet developed the institutional supervisory capacity necessary to ensure effective enforcement of personal data protection laws.[83]

Malaysia occupies a comparatively more stable position, having implemented the Personal Data Protection Act 2010 (PDPA) since 2010. Moreover, the Personal Data Protection Code of Practice for the Banking and Financial Sector demonstrates that

[82] Budi Hermono et al., "Regulating the Protection of Cryptocurrency Exchanges to Prevent Systemic Risks and Consumer Rights Violations in Indonesia," *Indonesia Private Law Review* 7, no. 1 (2026): 51–66, https://doi.org/10.25041/iplr.v7i1.4761.

[83] Rudi Natamiharja and Ikhsan Setiawan, "Guarding Privacy in the Digital Age: A Comparative Analysis of Data Protection Strategies in Indonesia and France," *Jambe Law Journal* 7, no. 1 (2024): 233–51, https://doi.org/10.22437/home.v7i1.349.

personal data protection within the financial sector extends beyond general statutory principles to encompass detailed technical and operational requirements. The Code of Practice provides banks with clear guidance regarding personal data collection, the processing of customer information, the retention of digital records, and mandatory data breach notification procedures. This regulatory approach reflects Malaysia's more progressive efforts to cultivate a robust digital compliance culture within its banking sector.

A further point of divergence concerns cybersecurity and technology risk management. Indonesia continues to face significant challenges arising from the limited readiness of cybersecurity infrastructure across many banking institutions. Incidents involving ransomware attacks, personal data breaches, and digital fraud indicate that a number of financial institutions have yet to treat cybersecurity as an integral component of corporate governance. Instead, digital security is frequently regarded merely as an operational or technical matter rather than as a matter of corporate legal responsibility. This situation demonstrates the insufficient integration of the principles of good corporate governance with cyber risk governance.

By contrast, through its Risk Management in Technology (RMiT) Policy Document, Bank Negara Malaysia requires financial institutions to implement comprehensive technology risk management systems, including incident response mechanisms, penetration testing, cyber resilience assessments, and business continuity and system recovery plans following cybersecurity incidents. This regulatory framework recognises technology risk management as an integral element of prudential regulation, such that failures in cybersecurity governance may constitute breaches of sound institutional governance. Consequently, the Malaysian framework creates stronger regulatory incentives for compliance throughout the digital banking industry.

From the perspective of legal enforcement, Indonesia continues to encounter significant challenges in ensuring effective protection for consumers using digital financial services. In many cases involving personal data breaches or mobile banking fraud, consumers occupy a substantially weaker legal position than banking institutions. Customers frequently encounter considerable evidentiary difficulties, while banks often rely upon standard-form contractual clauses to limit or exclude their liability for consumers' losses. These circumstances reveal a persistent imbalance in the legal relationship between financial service providers and consumers. As a result, the legal remedies currently available are often administrative and formalistic in nature and have yet to provide victims of digital data breaches with meaningful substantive justice.

Malaysia, by contrast, has adopted a more progressive approach towards strengthening institutional accountability for the protection of consumers' personal data. The decision in Public Bank Berhad v National Feedlot Corporation Sdn. Bhd. & Ors illustrates the willingness of Malaysian courts to recognise the confidentiality of customers' banking information as an integral component of a bank's fiduciary duty. The judgment further demonstrates that personal data breaches are no longer regarded solely as the consequence of individual employee misconduct but also as evidence of institutional failures in internal supervision and governance. This approach significantly broadens the scope of corporate responsibility within the digital banking sector.

More fundamentally, the comparison between Indonesia and Malaysia demonstrates that the effectiveness of legal protection in digital banking depends not merely upon the existence of numerous regulatory instruments but upon the coherence of regulatory policies, the effectiveness of institutional oversight, and the willingness of the State to recognise the protection of personal data as an aspect of citizens' fundamental rights. Indonesia remains in a transitional phase towards a more modern system of digital governance and consumer protection, whereas Malaysia has advanced towards a more integrated governance model founded upon proactive risk management and institutional coordination.

Consumer protection encompasses all legal measures designed to ensure legal certainty and safeguard consumers against business practices that may infringe upon or prejudice their rights.[84] Within contemporary consumer protection theory, the protection of personal data is recognised as an integral component of consumers' fundamental rights. Accordingly, the legal protection of personal data should not be confined to the imposition of administrative obligations upon data controllers and financial institutions; it must also be supported by effective mechanisms for legal redress and the restoration of consumers' rights in the event of personal data breaches. Indonesia has strengthened its legal framework through the enactment of the Personal Data Protection Law of 2022. Nevertheless, the implementation of this legislation continues to face significant challenges, particularly the absence of an independent Data Protection Authority (DPA) and the lack of an effective cross-sectoral supervisory mechanism. These institutional shortcomings have resulted in weak enforcement of personal data protection laws, with regulatory responses remaining predominantly administrative rather than remedial or corrective in nature.

Viewed from a broader comparative perspective, Malaysia has developed a more mature consumer protection regime for digital banking than Indonesia. This is reflected in its greater degree of regulatory harmonisation, more integrated institutional coordination, stronger enforcement of banks' institutional accountability, and the systematic implementation of cybersecurity standards. Although Indonesia has made significant legislative progress through the enactment of the Personal Data Protection Law and Financial Services Authority Regulation (POJK) No. 22 of 2023 concerning Consumer and Public Protection in the Financial Services Sector, the practical implementation of consumer protection continues to encounter structural challenges, including overlapping institutional mandates, weak legal enforcement, and limited effectiveness of digital regulatory oversight.[85]

From the perspective of consumer protection theory, these developments suggest that Indonesia remains at the stage of consumer protection through regulation, whereas Malaysia has progressed towards a model of consumer protection through governance and accountability. Accordingly, strengthening consumer protection in Indonesia cannot be achieved solely through the enactment of additional legislation. Rather, it requires

---

[84] Ahmadi Miru and Sutarman Yodo, *Hukum Perlindungan Konsumen* (Raja Grafindo Persada, 2015).

[85] Muhammad Faisal Aziz, Hamzah, and Sepriyadi Adhan S., "Perlindungan Hukum terhadap Nasabah atas Penyalahgunaan Data Pribadi oleh Pihak Bank di Era Digitalisasi Perbankan," *Al-Zayn: Jurnal Ilmu Sosial & Hukum* 3, no. 6 (2025): 8840–52.

comprehensive institutional reform, the integration of financial data oversight, the strengthening of the legal accountability of digital banks, and the enhancement of public digital literacy. Such reforms are essential to establishing a digital banking system that is secure, transparent, accountable, and capable of providing effective and equitable protection for consumers.

Conclusion

Indonesia has established a relatively comprehensive legal framework for the protection of consumers in the digital banking sector through the Personal Data Protection Law, the Electronic Information and Transactions Law, the Banking Law, and various Financial Services Authority (*OJK*) regulations governing consumer protection and technology risk management. These legislative and regulatory instruments reflect the State's recognition of the importance of safeguarding consumers' financial assets and personal data in the digital banking environment. Nevertheless, the effectiveness of this legal framework remains constrained by a range of structural and institutional challenges. Overlapping regulatory mandates, inadequate regulatory harmonisation, the absence of an integrated supervisory system, and the limited effectiveness of legal enforcement against personal data breaches and cybercrime demonstrate that Indonesia's consumer protection regime for digital banking remains in a transitional phase towards a more comprehensive and modern model of digital governance.

These challenges are further compounded by limited transparency and accountability in banking institutions' management of consumers' personal data, relatively low levels of public digital literacy, and a persistent imbalance in the legal relationship between banks and consumers in digital contractual arrangements. In practice, consumers frequently occupy a weaker bargaining position because banks unilaterally determine the terms of standard-form electronic service agreements, while consumers encounter considerable difficulties in obtaining evidence when pursuing claims arising from personal data breaches or digital fraud. These circumstances indicate that the existing legal protection afforded to consumers in Indonesia's digital banking sector remains predominantly formalistic and administrative in nature and has yet to provide effective substantive protection for consumers' legal rights.

In contrast, Malaysia has developed a comparatively more integrated and systematic consumer protection framework for digital banking. Through the Financial Services Act 2013 (FSA), the Islamic Financial Services Act 2013 (IFSA), the Personal Data Protection Act 2010 (PDPA), and a series of technical policy documents issued by Bank Negara Malaysia (BNM), Malaysia has successfully established a coherent relationship between personal data protection, technology risk governance, and the supervision of digital financial system stability. This regulatory framework demonstrates that consumer protection in Malaysia is not viewed merely as a normative legal obligation but is implemented through effective institutional oversight, the systematic application of cybersecurity standards, and the reinforcement of banks' institutional accountability for safeguarding customers' personal data.

The comparison between Indonesia and Malaysia demonstrates that the effectiveness of consumer protection within the digital banking sector is not determined solely by the number of regulatory instruments enacted by a jurisdiction. Rather, it depends upon the coherence of regulatory policies, the effectiveness of inter-agency coordination, the development of a strong digital compliance culture, and the State's commitment to recognising the protection of personal data as an integral component of consumers' fundamental rights. In this respect, Malaysia has progressively evolved towards a model of consumer protection through governance and accountability, whereas Indonesia remains at the stage of consumer protection through regulation, in which legislative development has not yet been matched by corresponding institutional reform and effective regulatory implementation.

From the perspective of consumer protection theory, the State bears a constitutional responsibility to ensure a fair balance in the legal relationship between financial service providers and consumers by providing both preventive and remedial forms of legal protection. Accordingly, strengthening consumer protection within Indonesia's digital banking sector cannot be achieved merely through the enactment of additional legislation. Instead, it requires comprehensive institutional reform aimed at establishing an integrated financial data oversight framework, strengthening the legal accountability of digital banks, adopting more rigorous cybersecurity standards, and improving public digital literacy. Without such structural reforms, the continued acceleration of digital transformation within Indonesia's banking sector is likely to increase the risks of privacy violations, the misuse of personal data, and financial losses suffered by consumers in the years ahead.

References

Ab. Aziz, Muhammad Ridhwan. "Islamic Digital Banking Framework in Malaysia: A Practitioners' Perspective." *International Journal of Islamic Economics and Finance Research* 7, no. 1 (2024): 28–41. https://doi.org/10.53840/ijiefer140.

Abdul Mujib. "The Failure of Indonesian E-Commerce Law in Adapting to Digital Economy." *Ijtihad: Jurnal Wacana Hukum Islam dan Kemanusiaan* 25, no. 2 (2025): 213–30. https://doi.org/10.18326/ijtihad.v25i2.213-230.

Abrianto, H., N. H. Farhani, S. C. Bidhari, E. H. H. Pasaribu, and N. Neila. "Transparansi Informasi Penggunaan Aplikasi Mobile Banking terhadap Perlindungan Konsumen Sektor Jasa Keuangan." In *Prosiding Simposium Nasional Perbankan, Akuntansi, dan Keuangan*. Politeknik Negeri Jakarta, 2022.

Abubakar, Lastuti, and Tri Handayani. "Penguatan Regulasi: Upaya Percepatan Transformasi Digital Perbankan di Era Ekonomi Digital." *Masalah-Masalah Hukum* 51, no. 3 (2022): 259–70. https://doi.org/10.14710/mmh.51.3.2022.259-270.

Adinda Lola Sariani Dinda. "Efektivitas Penegakan Hukum terhadap Kejahatan Siber di Indonesia." *AL-DALIL: Jurnal Ilmu Sosial, Politik, dan Hukum* 2, no. 2 (2024): 69–77.

Ahmad Farizal, Sudaberi, Febri Aulyandra, Fulthokon Daeli, and Abdurrahman Khalidy. "Perlindungan Hukum terhadap Konsumen dalam Transaksi Perbankan Digital: Tanggung Jawab Bank dan Hak Nasabah." *Syariah: Jurnal Ilmu Hukum* 2, no. 4 (2025): 1–6.

Al-Fatih, Sholahuddin. *Perkembangan Metode Penelitian Hukum di Indonesia*. UMMPress, 2023.

Alibeigi, Ali, Abu Bakar Munir, and Adeleh Asemi. "Compliance with Malaysian Personal Data Protection Act 2010 by Banking and Financial Institutions: A Legal Survey on Privacy Policies." *International Review of Law, Computers & Technology* 35, no. 3 (2021): 365–94. https://doi.org/10.1080/13600869.2021.1970936.

Alt, Rainer, Roman Beck, and Martin T. Smits. "FinTech and the Transformation of the Financial Industry." *Electronic Markets* 28, no. 3 (2018): 235–43. https://doi.org/10.1007/s12525-018-0310-9.

Amirulloh, Muhamad, Eman Suparman, Helitha Novianty Muchtar, and Hetty Hasanah. "Legal Basis and Readiness of the Banking Sector in Implementing Privacy Reliability Certification." *Jurnal IUS Kajian Hukum dan Keadilan* 13, no. 3 (2025): 545–58. https://doi.org/10.29303/ius.v13i3.1777.

Andini, Pretty Fabiola, and Fence M. Wantu. "Implementation of the Precautionary Principle According to Article 2 and Article 29 Law Number 10 of 1998 concerning Banking." *Damhil Law Journal* 3, no. 1 (2023): 70. https://doi.org/10.56591/dlj.v3i1.1936.

Antoine, R. A., D. Rahmawati, and R. Putri. "Penyalahgunaan Data Pribadi dalam Teknologi Transaksi Digital di Industri Perbankan Digital (Studi Kasus PT Bank Syariah Indonesia)." *Jurnal Manajemen dan Ilmu Administrasi* 12, no. 3 (2023): 77–92.

Apsari, Ratna Ditha, and Tubagus Muhamad Yusuf Khudri. "An Evaluation of Cybersecurity Risk Management Implementation at Bank Pembangunan XYZ." *Greenation International Journal of Economics and Accounting* 3, no. 1 (2025): 111–24. https://doi.org/10.38035/gijea.v3i1.366.

Assari, Elsa. "The Legal Status of Digital Banks in Indonesia." *Jurisdictie: Jurnal Hukum dan Syariah* 13, no. 2 (2023): 264–93. https://doi.org/10.18860/j.v13i2.16285.

Azmi, M. N. A., M. S. Hidayat, and A. R. Luthfi. "Analisa Kasus Kebocoran Data pada Bank Indonesia dalam Sistem Perbankan." *Jurnal Manajemen dan Ilmu Administrasi* 13, no. 1 (2024): 55–70.

Bank Negara Malaysia. *Policy Document on Electronic Money (E-Money)*. Rev. ed. Kuala Lumpur: Bank Negara Malaysia, 2025.

Bank Negara Malaysia. *Policy Document on Licensing Framework for Digital Banks*. Kuala Lumpur: Bank Negara Malaysia, 2020.

Bank Negara Malaysia. *Risk Management in Technology (RMiT) Policy Document*. Kuala Lumpur: Bank Negara Malaysia, 2022.

Ben-Shahar, Omri, and Carl E. Schneider. *More Than You Wanted to Know: The Failure of Mandated Disclosure*. Princeton, NJ: Princeton University Press, 2014.

Benseghir, Mourad, Aouatef Zerara, and Maamar Bentria. "Consumer Protection in Digital Markets: A Comparative Legal Analysis of E-Commerce Regulation in the United Arab Emirates and Indonesia." *Jurisdictie: Jurnal Hukum dan Syariah* 16, no. 2 (2025): 374–416. https://doi.org/10.18860/j.v16i2.33063.

Benuf, Kornelius, and Muhamad Azhar. "Metodologi Penelitian Hukum sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer." *Gema Keadilan* 7, no. 1 (2020): 20–33.

Billiam, Lastuti Abubakar, and Tri Handayani. "The Urgency of Open Application Programming Interface Standardization in the Implementation of Open Banking to Customer Data Protection for the Advancement of Indonesian Banking." *Padjadjaran Jurnal Ilmu Hukum* 9, no. 1 (2022): 69–91. https://doi.org/10.22304/pjih.v9n1.a4.

Buala, Jefry, Elisatris Gultom, and Deviana Yuanitasari. "Penyalahgunaan Data Pribadi Konsumen oleh Perusahaan: Kajian Yuridis dalam Perspektif UU Perlindungan Konsumen dan UU Perlindungan Data Pribadi." *Jurnal Pendidikan Indonesia* 6, no. 5 (2025).

Claessens, Stijn, Jon Frost, Grant Turner, and Feng Zhu. "Fintech Credit Markets around the World: Size, Drivers and Policy Issues." *BIS Quarterly Review*, September 2018, 29–49.

Deloitte Global. "Cyber Risk in Digital Banking 2023 Report." Deloitte Insights, 2023.

Dewi, P. M., F. Andini, and R. Syahputra. "Perilaku Digital Konsumen dan Risiko Keamanan dalam Penggunaan Layanan Perbankan Online di Indonesia." *Jurnal Manajemen dan Teknologi Informasi*, 56–68.

Diniyya, A. A., Mahdiah, and R. Wahyudi. "Financial Technology Regulation in Malaysia and Indonesia: A Comparative Study." *Journal of Islamic Economics, Finance, and Banking* 3, no. 2 (2023).

Firdaus, S. E., A. Ramadhani, and M. D. Putri. "Implementasi Teknologi untuk Penguatan Keamanan Data Pribadi Nasabah dalam Sektor Perbankan." *Jurnal Inovasi Hukum dan Teknologi* 3, no. 2 (2024): 115–29.

Fonda, H., and Z. A. Hoesein. "Pertanggungjawaban Bank dalam Menjamin Keamanan Data Nasabah di Era Digitalisasi Perbankan." *Jurnal Retentum* 4, no. 2 (2024): 25–39.

Hakim, R., D. Franciska, and E. Hendrotriwidodo. "Perlindungan Hukum Konsumen terhadap Nasabah atas Terjadi Fraud pada Transaksi Bank Digital." *Jurnal Kajian Sosial dan Hukum* 6, no. 2 (2024): 201–15.

Hannan, Md. Abdul, Md. Atik Shahriar, Md Sadek Ferdous, Mohammad Jabed Morshed Chowdhury, and Mohammad Shahriar Rahman. "A Systematic Literature Review of Blockchain-Based e-KYC Systems." *Computing* 105, no. 10 (2023): 2089–2118. https://doi.org/10.1007/s00607-023-01176-8.

Hermono, Budi, Ellectrananda Anugerah Ash-sidiqqi, Rindia Fanny Kusumaningtyas, and Mutiara Dwi Sari. "Regulating the Protection of Cryptocurrency Exchanges to Prevent Systemic Risks and Consumer Rights Violations in Indonesia." *Indonesia Private Law Review* 7, no. 1 (2026): 51–66. https://doi.org/10.25041/iplr.v7i1.4761.

Huda, Uu Nurul, Tatang Astarudin, Muhammad Irsan Nasution, Ahmad Abdul Khozin, and Muhammad Irsan. "Legal Protection for Personal Data Leaks and Its Implications for Citizens' Privacy Rights within the Framework of the Indonesian Legal State." *Jambura Law Review* 8, no. 1 (2026): 144–59. https://doi.org/10.33756/jlr.v1i1.32666.

Jabatan Perlindungan Data Peribadi Malaysia. *Personal Data Protection Code of Practice for the Banking and Financial Sector*. Putrajaya: Jabatan Perlindungan Data Peribadi, 2021.

Kadari, P. N., S. Saharuddin, and M. A. F. Syahril. "Perlindungan Hukum Nasabah atas Penggunaan E-Banking." *Jurnal Litigasi Amsir* 10, no. 2 (2023): 167–79.

Kholis, Ilman Maulana. "Perlindungan Data Pribadi dan Keamanan Siber di Sektor Perbankan: Studi Kritis atas Penerapan UU PDP dan UU ITE di Indonesia." *STAATSRECHT: Jurnal Hukum Kenegaraan dan Politik Islam* 4, no. 2 (2024).

KPMG Malaysia. *Digital Banking (2nd Ed.): Regulatory and Market Perspectives*. Kuala Lumpur: KPMG, 2021.

Krishnan, Suren, and Mohd Khairudin Kasiran. "Comparison of Security Measures in Online Banking Sector Malaysia." *Borneo International Journal* 6, no. 3 (2023): 43–48.

Lestari, D. "Sinkronisasi Kewenangan OJK dan Kominfo dalam Pengawasan Perlindungan Data Pribadi di Sektor Keuangan Digital." *Jurnal Hukum & Regulasi Keuangan* 6, no. 1 (2024): 45–62.

Mahadzir, A., and N. A. Yusof. "Ethical Data Governance in Digital Banking: A Malaysian Perspective." *Journal of Financial Integrity Studies* 2, no. 1 (2024): 56–71.

Miru, Ahmadi, and Sutarman Yodo. *Hukum Perlindungan Konsumen*. Raja Grafindo Persada, 2015.

Muhammad Faisal Aziz, Hamzah, and Sepriyadi Adhan S. "Perlindungan Hukum terhadap Nasabah atas Penyalahgunaan Data Pribadi oleh Pihak Bank di Era Digitalisasi Perbankan." *Al-Zayn: Jurnal Ilmu Sosial & Hukum* 3, no. 6 (2025): 8840–52.

Muhammad, Wildan, Ramadhan Daud Renata Candra, and Zulfa Wijayanti Rena. "Analisis Tanggung Jawab Bank terhadap Kebocoran Data Nasabah: Ditinjau dalam Perspektif Hukum Perbankan." *Media Hukum Indonesia* 3, no. 1 (2024): 44–59.

Nabila, Z., R. R. Virnanda, F. D. Yusuf, R. Kusumaningtias, and A. Kusumaningsih. "Peran Prinsip Akuntabilitas sebagai Strategi Mitigasi Risiko Operasional pada Bank Digital: Studi Kasus SeaBank Indonesia." *Jurnal Pendidikan Tambusai* 7, no. 5 (2023): 211–23.

Natamiharja, Rudi, and Ikhsan Setiawan. "Guarding Privacy in the Digital Age: A Comparative Analysis of Data Protection Strategies in Indonesia and France." *Jambe Law Journal* 7, no. 1 (2024): 233–51. https://doi.org/10.22437/home.v7i1.349.

Noor, Afif, Ali Maskur, Dwi Wulandari, Aqila-Syarief Muhammad Afif, and Muhammad Fazli Azmi. "Digital Economy Regulation and Consumer Rights Protection:

Realizing Security in Financial Technology Transactions." *Lex Scientia Law Review* 9, no. 2 (2025): 1324–75. https://doi.org/10.15294/lslr.v9i2.24927.

Nurfitriyani, Siti Hamidah, and Reka Dewantara. "Analisis Hukum Ekonomi terhadap Peraturan Perbankan dalam Perlindungan Hukum Nasabah." *Jurnal IUS Kajian Hukum dan Keadilan* 9, no. 2 (2021): 458–71. https://doi.org/10.29303/ius.v9i2.911.

Nurkhairina Binti Noor Sureani, Atikah Shahira Binti Awis Qurni, Ayman Haziqah Binti Azman, Mohd Bahrin Bin Othman, and Hariz Sufi bin Zahar. "The Adequacy of Data Protection Laws in Protecting Personal Data in Malaysia." *Malaysian Journal of Social Sciences and Humanities (MJSSH)* 6, no. 10 (2021): 488–95.

OJK. *Cetak Biru Transformasi Digital Perbankan*. Otoritas Jasa Keuangan, 2023.

OJK. *Survei Nasional Literasi dan Inklusi Keuangan 2022*. Otoritas Jasa Keuangan, 2022.

Palupy, Heppy Endah, Ronald Nawing, and Susi Susantijo. "Personal Data Protection Governance in the Asia Pacific Region: A Review of the Scope, Effectiveness, and Legal Challenges." *Volksgeist: Jurnal Ilmu Hukum dan Konstitusi* 9, no. 1 (2026): 197–225. https://doi.org/10.24090/volksgeist.v9i1.15362.

Pati, Umi Khaerah, and Anugrah Muhtarom Pratama. "Indonesia's Open Banking Future: Designing Effective Regulatory Approaches." *Jambe Law Journal* 8, no. 1 (2025): 27–60. https://doi.org/10.22437/home.v8i1.371.

Radin, Margaret Jane. *Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law*. Princeton, NJ: Princeton University Press, 2013.

Ramadhan, Muhammad, Dwi Oktafia Ariyanti, Nita Ariyani, and Henry Arianto. "Edukasi Hukum Implikasi Undang-Undang Informasi dan Transaksi Elektronik di Kelurahan Bener, Yogyakarta." *DAS SEIN: Jurnal Pengabdian Hukum dan Humaniora* 1, no. 1 (2023): 119–30. https://doi.org/10.33756/jds.v1i1.19442.

Ramadhani, Evyta Rosiyanti, Ayudya Rizqi Rachmawati, and Roro Hera Kurnikova. "Integrating Islamic Values with the Right to Be Forgotten: A Legal Approach to Addressing Deepfake Pornography in Indonesia." *De Jure: Jurnal Hukum dan Syar'iah* 17, no. 1 (2025): 112–31. https://doi.org/10.18860/j-fsh.v17i1.28880.

Rifa, F., and M. N. Hidayati. "Kebijakan Penal dalam Perlindungan Data Pribadi Nasabah Fintech Lending di Indonesia." *Binamulia Hukum* 13, no. 2 (2024): 461–81.

Saif, M. A. M., M. Rahman, and N. M. Zayed. "Determinants of the Intention to Adopt Digital-Only Banks in Malaysia." *Sustainability* 14, no. 17 (2022).

Saragih, B. *Hukum Data Pribadi di Indonesia: Implikasi terhadap Perbankan Digital*. Prenada Media Group, 2023.

Shin Associates. *Fintech and Cybersecurity Legal Frameworks and Emerging Regulatory Trends in Malaysia*, 2025.

Shoimah, Siti Nur. "Freedom of Contract in the Digital Age: Perspectives on the Indonesian Civil Code and Fiqh Muamalah." *Trunojoyo Law Review* 8, no. 1 (2026): 59–94. https://doi.org/10.21107/tlr.v8i1.32568.

Siregar, Y. "Analisis Yuridis Tanggung Jawab Bank atas Tindak Fraud pada Transaksi Mobile Banking serta Upaya Penegakan Hukumnya." *Jurnal Ekonomi dan Hukum Islam* 8, no. 1 (2024): 33–49.

Sitorus, A. *Kewenangan OJK dalam Perlindungan Nasabah Perbankan di Era Digitalisasi*. Refika Aditama, 2023.

Situmeang, Ampuan, Abdurrakhman Alhakim, Ruetaitip Chansrakaeo, Winda Fitri, and Winsherly Tan. "Sharenting and Child Privacy: The GDPR as a Benchmark for

Indonesian and Thai Legal Frameworks." *Lex Scientia Law Review* 10, no. 1 (2026): 233–58. https://doi.org/10.15294/lslr.v10i1.29211.

Sriono, Risdalina, Kusno, Indra Kumalasari M., and Hengki Syahyunan. "Uncovering Legal Gaps in Digital Banking: Customer Protection and Bank Accountability in Indonesia." *Litigasi* 25, no. 2 (2024): 301–30. https://doi.org/10.23969/litigasi.v25i2.18538.

Tan, David. "Metode Penelitian Hukum: Mengupas dan Mengulas Metodologi dalam Menyelenggarakan Penelitian Hukum." *Nusantara: Jurnal Ilmu Pengetahuan Sosial* 8, no. 8 (2021): 2463–78.

Tay, Yi Hong, Shih Yin Ooi, Ying Han Pang, Ying Huey Gan, and Sook Ling Lew. "Ensuring Privacy and Security on Banking Websites in Malaysia: A Cookies Scanner Solution." *Journal of Informatics and Web Engineering* 2, no. 2 (2023): 153–67. https://doi.org/10.33093/jiwe.2023.2.2.12.

Teo, Poh-Chuin. "Exploring Digital-Only Banking in Malaysia: Technological Advancements, Regulatory Landscape, and Business Implications." *Business Management and Strategy* 16, no. 1 (2025): 46–60. https://doi.org/10.5296/bms.v16i1.22498.

Thong, Ming Sen. *Blockchain for Financial Governance in Malaysia and Singapore: Transforming Regulatory and Shariah Compliance to Drive Financial Inclusion*. Singapore: Palgrave Macmillan, 2025. https://doi.org/10.1007/978-981-96-1281-9.

Wardhono, R. D. T. K., W. Badrawani, A. Deviana, M. Pramudyastuti, and N. Shalehanti. "Pelindungan Data Pribadi di Bank Indonesia dan Lembaga Jasa Keuangan: Rekomendasi Kebijakan dan Teknis Pengaturan." Working Paper. Bank Indonesia, 2024.

Widya Annafa, S., H. P. G. H. Simanjuntak, and M. A. Ayudia. "Tanggung Jawab Hukum Bank dalam Kasus Kebocoran Data Nasabah." *Jurnal Multidisiplin Ilmu Akademik* 5, no. 2 (2023): 77–89.

World Bank. *Global Financial Development Report 2023: Digitalization of Finance*. Washington, DC: World Bank, 2023.

Wulandari Utami, G., H. Ma'ruf, and D. Yulianti. "Perlindungan terhadap Nasabah akibat Serangan Siber: Studi di Bank Syariah Indonesia KC Pekalongan Pemuda." *Jurnal El-Hisbah* 12, no. 1 (2024): 67–80.

Yuliana, L., and R. Nandari. "Tantangan Literasi Digital dalam Perlindungan Konsumen Layanan Keuangan Digital di Indonesia." *Jurnal Ekonomi dan Kebijakan Publik* 14, no. 1 (2023): 33–47.

Yuspin, Wardah, Kelik Wardiono, Aditya Nurrahman, and Arief Budiono. "Personal Data Protection Law in Digital Banking Governance in Indonesia." *Studia Iuridica Lublinensia* 32, no. 1 (2023): 99–130. https://doi.org/10.17951/sil.2023.32.1.99-130.

Zainuddin, Muhammad, and Aisyah Dinda Karina. "Penggunaan Metode Yuridis Normatif dalam Membuktikan Kebenaran pada Penelitian Hukum." *Smart Law Journal* 2, no. 2 (2023): 114–23.

Zetzsche, Dirk A., Ross P. Buckley, Douglas W. Arner, and Janos N. Barberis. *Regulating FinTech: Principles and Challenges*. Oxford: Oxford University Press, 2020.