

## Legal Liability for Personal Data Misuse in Digital Banking

Mas Rara Tri Retno Herryani<sup>1</sup>✉, Aufa Fajrul Hikmah<sup>2</sup>, Irham Rahman<sup>3</sup>

<sup>1,2,3</sup>Faculty of Law, Universitas Kadiri, Kediri, Indonesia

✉ corresponding email: [masrara@unik-kediri.ac.id](mailto:masrara@unik-kediri.ac.id)

Article	Abstract
<p><b>Keywords:</b> Banking; Digital Era; Personal Data Protection; Legal Liability</p> <p><b>Article History</b> Received: Feb 04, 2026; Reviewed: Mar 20, 2026; Accepted: Apr 05, 2026; Published: Apr 06 2026.</p>	<p>Digital transformation in the banking sector has led to the emergence of digital banking services that provide convenience, efficiency, and accessibility to the public. However, on the other hand, this development increases the risk of misuse of customer personal data, potentially resulting in material and immaterial losses. This study aims to analyze the forms of legal protection and legal accountability for misuse of customer personal data in banking institutions in the digital era. The research method used is normative legal research with a statutory and conceptual approach, through an examination of the Banking Law, Financial Services Authority regulations, Law Number 27 of 2022 concerning Personal Data Protection, and regulations related to consumer protection. The results show that the protection of customer personal data is part of citizens' constitutional rights that must be guaranteed by the state and electronic system providers, including digital banks. Legal liability for misuse of personal data can be imposed in the form of civil, administrative, and criminal liability, depending on the type of violation. Banks, as digital service providers, are obliged to apply the principle of prudence, maintain data confidentiality, and provide complaint and dispute</p>

resolution mechanisms for customers. The Personal Data Protection Law strengthens the legal basis for customer protection, but effective implementation and oversight remain challenges. Therefore, synergy between the government, the Financial Services Authority (OJK), and banking institutions is needed to strengthen data security systems and ensure legal certainty for customers facing the risk of personal data misuse in the digital era.



Copyright ©2026 by Author(s); This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License. All writings published in this journal are personal views of the authors and do not represent the views of this journal and the author's affiliated institutions. (Prastika, D. R., Wulandari, S. A. "Predatory Pricing in Live Online Marketplaces: A Competition Law Perspective", *Hang Tuah Law Journal*, 10 (1), 116-134, <https://doi.org/10.30649/htj.v10i1.361>)

## Introduction

Banking as a financial services industry in Indonesia, is an industry that plays a vital role in economic activities.<sup>1</sup> For banks, digitalization is not just an option but a necessity and obligation due to customer demands for speed, ease, flexibility, convenience, and 24/7 availability. From the results of the survey conducted, several banks in Indonesia are campaigning and even investing in transforming into digital services. This digital transformation, in addition to its potential to save costs and digitize existing banking products, also changes people's mindsets by making digitalization a solution to meet people's needs.<sup>2</sup>

The banking sector is regulated by Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking, hereinafter referred to as the Banking Law. This law regulates all matters related to banking, both conventional and Islamic banking. Islamic banking is then regulated separately in Law Number 21 of 2008 concerning Islamic Banking. Article 5 of the Banking Law only states that there are two types of banks Commercial Banks and Rural Banks. The Banking Law has not updated the digital banking system and therefore does not regulate digital banking at all.<sup>3</sup>

<sup>1</sup> Jelena Cvijovic, Milica Kostic-Stankovic, and Marija Reljic, "Customer Relationship Management in Banking Industry: Modern Approach," *Industrija* 45, no. 3 (2017): 151–65, <https://doi.org/10.5937/industrija45-15975>.

<sup>2</sup> Bandaru Srinivasa Rao CH Himabindu, "A Study on Digital Transformation: How Fintech Is Revolutionizing the Banking Landscape," *Journal of Informatics Education and Research* 5, no. 1 (January 31, 2025), <https://doi.org/10.52783/jier.v5i1.2109>.

<sup>3</sup> Nur Dyah Nastiti and Rahmatina Awaliah Kasri, "The Role of Banking Regulation in the Development of Islamic Banking Financing in Indonesia," *International*

The Banking Law, essentially focuses on regulating the conventional banking system and has not explicitly addressed the development of digital banking. Its provisions focus more on institutional aspects, business activities, and prudential principles in general bank operations, without specific provisions for digital-based services such as mobile banking, fintech, or purely digital banks.<sup>4</sup> As a result, digital banking practices in Indonesia are currently largely regulated through derivative regulations and policies from authorities such as Bank Indonesia and the Financial Services Authority (OJK), demonstrating the need for legal reform to be more responsive to digital transformation in the banking sector.<sup>5</sup>

Bank Indonesia, as the central bank, as regulated in Article 34 of Law Number 3 of 2004, mandates the establishment of a supervisory institution and the granting of regulatory and supervisory authority to the financial services sector, including banking, insurance, securities, venture capital, and other financing companies or entities that manage public funds. To realize Bank Indonesia's mandate, the government established an independent institution tasked with carrying out functions, duties, supervision, inspection, investigation, and regulatory authority in the financial services sector, namely by establishing the Financial Services Authority (OJK), regulated in Law Number 21 of 2011 concerning the Financial Services Authority. With the existence of the OJK, Bank Indonesia officially delegates supervisory authority in the financial sector to the OJK, allowing the OJK to continue Bank Indonesia's duties and authorities in the field of financial services sector supervision.<sup>6</sup>

To implement digitalization in banking, the OJK has issued regulations on digital banks, outlined in OJK Regulation No. 12/POJK.03/2021 concerning the Provision of Digital Banking Services by Commercial Banks. According to OJK Regulation No.

---

*Journal of Islamic and Middle Eastern Finance and Management* 12, no. 5 (November 11, 2019): 643–62, <https://doi.org/10.1108/IMEFM-10-2018-0365>.

<sup>4</sup> Wardah Yuspin et al., “Legal Reconstruction of Indonesian Banking Laws: Challenges and Opportunities for Digital Bank Regulation,” *Varia Justicia* 19, no. 1 (April 29, 2023): 52–69, <https://doi.org/10.31603/variajusticia.v19i1.8019>.

<sup>5</sup> Sriono et al., “Legal Protection for Digital Bank Customers in Indonesia: Analysis of Data Confidentiality Regulations and Bank Responsibility,” *LITIGASI* 25, no. 2 (October 31, 2024): 301–30, <https://doi.org/10.23969/litigasi.v25i2.18538>.

<sup>6</sup> Wetria Fauzi, “The Authority of the Financial Services Authority (OJK) in Publishing Insurance Regulation in the Perspective of Insurance Law In Indonesia,” *Jurnal Hukum & Pembangunan* 47, no. 2 (July 2, 2017): 211, 10.21143/jhp.vol47.no2.1452.

12/POJK.03/2021 concerning Commercial Banks, digital banking is defined as "a bank that is a legal entity in Indonesia that provides and conducts business activities primarily through electronic channels without physical office other than head office or using limited physical offices." This explanation indicates that establishing a digital bank can be achieved in two ways: through the establishment of a new bank or through the transformation of an existing bank.<sup>7</sup> In Indonesia, there are already several banks that have transformed into digital services, which of course are supervised by the OJK. This regulation serves as a regulatory/legal umbrella for banks in establishing digital banks or transforming into digital banks, simplifying and streamlining office networks, and creating digital banking products without neglecting prudential aspects, thereby enabling the development of the banking industry and meeting public needs during the current pandemic.<sup>8</sup>

Digital banking services are banking services or activities that utilize electronic or digital means owned by the bank, and/or digital media owned by prospective and/or existing customers, and are conducted independently. Unfortunately, these digital banking services are still only enjoyed by a small portion of the Indonesian population. Data from global financial institutions indicates that only 54% of Indonesians have access to banking services, with the remainder remaining untouched.<sup>9</sup>

Digital banking services can be accessed through digital banking applications on mobile phones, making them more practical, effective, and efficient. Prospective customers who wish to register as customers of one of the digital banks can do so online, namely by downloading the application then registering themselves by uploading personal documents or personal data such as personal data, mother's name, ID card data, then verifying and being contacted by the bank's customer

---

<sup>7</sup> Habib Matwar and Mustapa Khamal Rokan, "The Financial Services Authority (OJK) in Supervising the Bank Payment System and Protecting Customers Against Criminal Acts," *International Journal of Economics, Business and Accounting Research (IJEBAR)* 8, no. 1 (January 12, 2024), <https://doi.org/10.29040/ijebar.v8i1.12193>.

<sup>8</sup> Emir Adzan Syazali, Johni Najwan, and Mus kibah Mus kibah, "Legal Reform and Strengthening of The Financial Services Authority (OJK): Protecting Investors from Insider Trading in Indonesia," *As-Siyasi: Journal of Constitutional Law* 4, no. 2 (December 25, 2024): 184–209, <https://doi.org/10.24042/as-siyasi.v4i2.25513>.

<sup>9</sup> Nandang Sutrisno and Nur Gemilang Mahardhika, "Liberalisation of Banking Services Under the Framework of Asean Economic Community: An Indonesian Perspective," *Hang Tuah Law Journal*, August 26, 2022, 33–45, <https://doi.org/10.30649/htlj.v6i1.65>.

service.<sup>10</sup> The inclusion of private personal data must be protected by the government, electronic system organizers (banking), and the public because personal data is a person's confidential data that cannot be owned by anyone so it is very high risk of being stolen and misused. The Indonesian government has a responsibility to provide personal data protection to its citizens. Indonesia has recognized personal data protection as a constitutional right of all Indonesian citizens. This can be seen in Article 28 G paragraph (1) and Article 28 H paragraph (4) of the 1945 Constitution of the Republic of Indonesia, hereinafter referred to as the Authors of the 1945 Constitution. It is important to note that data protection in Indonesia is still considered very poor. This is evident in the numerous cases of data breaches, which typically occur in e-commerce companies, including in the digital banking sector. Data breaches can lead to the misuse of personal data for malicious purposes such as fraud, theft, bank account hacking, unsolicited product promotions, and privacy violations.<sup>11</sup>

One recent case of a customer data breach in digital banking involved Theresia, a customer of Bank Jenius National Pension Savings Bank (*Bank Tabungan Pensiunan Nasional/BTPN*), who suffered losses of over 110 million rupiah, using the name of Bank Jenius BTPN. The incident began on July 14, 2021, when Theresia received a call from someone claiming to be a Jenius customer service representative. Initially, the victim didn't find the call unusual, as the third party pretended to be the same service she received when making a transaction with Jenius customer service. The third party told her to replace her debit card and fill out a link from Jenius. The victim began to notice something strange when the individual discovered she was a frequent Jenius customer and that she was using another account linked to her Jenius account. Another recent case occurred in May 2023, when Bank Syariah Indonesia's systems experienced a major disruption due to a ransomware attack. The hacker group claimed to have stolen customer data and threatened to share it on the dark web. The allegedly leaked data included customer identities, account details, and internal documents. Customer data was reportedly offered

---

<sup>10</sup> Andika Persada Putera, "The Prudential Principle as the Basis in Implementing Banking Transaction," *Hang Tuah Law Journal*, January 15, 2021, 52–60, <https://doi.org/10.30649/htlj.v4i2.16>.

<sup>11</sup> Siti Mariyam et al., "Safeguarding Personal Data in Indonesian E-Commerce from a Constitutional Rights Perspective," *Jambe Law Journal* 8, no. 2 (December 31, 2025): 683–711, <https://doi.org/10.22437/x5q9y093>.

on dark web forums after negotiations failed. The attack disrupted ATM and mobile banking services for several days.

This research has elements of novelty and has shifted from a general legal protection approach to a more specific and operational analysis of the legal liability of banking institutions compared to several existing articles. For example, the article by Arya Salman Aziz and Muhammad Abyan Zaidan entitled "Legal Protection of Customers Against Misuse of Personal Data by Third Parties in Digital Banking Cooperation" emphasizes the existence of regulatory gaps and weak supervision in bank cooperation with third parties, with a primary focus on the aspect of preventive legal protection.<sup>12</sup> In addition, the article by in Arus Jurnal Sosial dan Humaniora entitled "Legal Responsibility of Banks for the Protection of Customers' Personal Data in Electronic Systems" examines the forms of violations and responsibilities of banks, but is still limited to a general normative approach and does not describe systemic accountability mechanisms.<sup>13</sup> Finally, the article by Sukarelawati Permana et al. entitled "Legal Protection of Consumer Personal Data in E-Commerce Transactions" (2020) focuses more on the e-commerce sector and consumer rights in general, rather than specifically on the digital banking sector.<sup>14</sup> Compared with the four previous articles, this article not only identifies regulatory weaknesses but also systematically constructs forms of administrative, civil, and criminal liability, linking them to the principles of accountability, internal governance, and evidentiary mechanisms in the context of digital banking.

The legal framework governing liability for misuse of personal data in banking institutions in the digital age is still not fully adapted to the complexity of technological risks, necessitating regulatory strengthening that goes beyond formal compliance. This research is

---

<sup>12</sup> Arya Salman Aziz and Muhammad Abyan Zaidan, "Perlindungan Hukum Nasabah Terhadap Penyalahgunaan Data Pribadi Oleh Pihak Ketiga Dalam Kerja Sama Perbankan Digital," *Ekopedia: Jurnal Ilmiah Ekonomi* 1, no. 2 (April 2025): 120–29, <https://doi.org/10.63822/qwcqac23>.

<sup>13</sup> Ruly Wahyu and Men Wih Widiatno, "Tanggung Jawab Hukum Pidana Penyelenggara Elektronik Perbankan Terhadap Perlindungan Data Pribadi Nasabah," *Arus Jurnal Sosial Dan Humaniora* 5, no. 2 (August 29, 2025): 3190–99, <https://doi.org/10.57250/ajsh.v5i2.1620>.

<sup>14</sup> Sukarelawati Permana, "Pengaturan Perlindungan Data Pribadi Konsumen Jasa Keuangan Dalam Penggunaan Uang Elektronik Berbasis Server," *Veritas et Justitia* 8, no. 2 (December 26, 2022): 386–414, <https://doi.org/10.25123/vej.v8i2.5213>.

expected to provide constructive recommendations for the future development of banking regulations in Indonesia.

## Method

Research methods play a crucial role in every legal research and writing, including collecting and obtaining data, then compiling, processing, and analyzing the data. Legal research is a series of scientific activities undertaken to understand a potential legal problem and ultimately conclude and provide a solution to address the current legal problem. Legal research requires a research method, which the author will then use to support the research findings and achieve the objectives of the legal research. The type of research used by the author in compiling this legal writing is normative or doctrinal legal research. According to Peter Mahmud Marzuki, legal research is normative legal research. Normative legal research is a process of discovering legal rules that conform to legal norms, legal principles, and legal doctrines, aimed at addressing the legal issues at. Normative legal research is conducted by examining legal materials focusing on primary legal materials in the form of laws and regulations, court decisions, legal theories, expert opinions, and secondary legal materials as a complement to the study of legal materials.<sup>15</sup> Normative legal research aims to produce new arguments or concepts that are realized as an assessment (prescription) of the problems faced. In this normative legal research, the author examines the legal rules, legal principles, and legal doctrines contained in Indonesian laws and regulations that regulate the legal protection of personal data of digital banking service customers in the Indonesian banking sector.

## Result and Discussion

### A. Legal Responsibility for Misuse of Personal Data in Banking Institutions in the Digital Era

The rapid development of technology and information today makes individual privacy vulnerable to misuse by irresponsible individuals. Legal protection of digital bank customers' personal data is inextricably linked to the concept of confidentiality or privacy. The concept of privacy was first proposed by Warren and Brandeis, writing in an article in the Harvard University School of Law journal

---

<sup>15</sup> Peter Mahmud Marzuki, *Penelitian Hukum*, ke-5 (Jakarta: Kencana Prenada Media Group, 2009).

entitled "The Right to Privacy," or the right to be left alone. In their article, Warren and Brandeis stated that technological advancements have given rise to a public awareness of the birth of an individual's right to enjoy life. The right to enjoy life is defined as an individual's right to privacy, or the right not to be disturbed in their personal life by either others or the state. From the explanation above, it can be seen that the law must recognize and protect an individual's right to privacy.<sup>16</sup>

The right to be left alone relates to human spiritual needs, which include the need to have their thoughts and feelings respected and to enjoy life to the fullest. This is referred to as the right to be let alone. Warren proposed to the judge that privacy is a right that must be protected. The reasons why privacy must be protected are:<sup>17</sup>

1. When interacting with others, a person must conceal parts of their private life to maintain their position in certain aspects.
2. A person needs time alone to carry out their daily activities and therefore must have privacy.
3. Privacy is a separate right, but this right is lost when a person makes personal matters public.
4. Privacy is a right in marriage, allowing for privacy regarding personal relationships.
5. Privacy requires legal protection because the losses suffered are far greater than physical losses, as it interferes with a person's private life and requires compensation.

In his book, Satjipto Rahardjo explains that legal protection is the provision of protection for human rights violated by others, ensuring that the public enjoys all the rights granted by law. The law serves as a form of protection that is not only adaptive and flexible, but also predictive and anticipatory. Law is necessary for those seeking social justice.<sup>18</sup> Regarding legal protection, this discussion focuses on protection in the digital banking sector. The digital banking sector has an obligation to protect its customers' personal data. Currently, there are no specific legal regulations governing personal data protection, thus, there are no legal regulations that accommodate this.

---

<sup>16</sup> Sinta Dewi Rosadi, "Prinsip-Prinsip Perlindungan Data Pribadi Nasabah Kartu Kredit Dikaitkan Dengan Undang-Undang No 11 Tahun 2008 Tentang ITE Dan Peraturan Bank Indonesia NO 7/6/PBI/2005," *Sosiohumaniora* 19, no. 3 (November 8, 2017), <https://doi.org/10.24198/sosiohumaniora.v19i3.11380>.

<sup>17</sup> Ibid.

<sup>18</sup> Satjipto Rahardjo, *Ilmu Hukum*, Cetakan Ke (Bandung: Citra Aditya Bhakti, 2012).

The Indonesian government has a responsibility to provide personal data protection to its citizens. The origins of law in Indonesia stem from the constitution and legislation, which recognize personal data protection as a constitutional right of all Indonesian citizens, as outlined in Article 28 G paragraph (1) and Article 28 H paragraph (4) of the 1945 Constitution of the Republic of Indonesia. Personal data protection is indeed a constitutional right of every citizen.

Legal accountability created by the government and outlined in legislation to regulate and provide protection and justice for vulnerable parties so that they are not continuously exploited, but in accordance with the nature of legal regulations that must not be biased or partial and proportionally provide balanced legal protection for other parties.<sup>19</sup> External legal protection is implemented to prevent arbitrariness against the interests of other parties that can cause harm to vulnerable parties. Law Number 27 of 2022 concerning Personal Data Protection, which has been established to protect the privacy of consumers using services used by Tokopedia, is as follows:

*Objection*, Personal Data Subjects have the right to object to decisions based solely on automated processing, including profiling, that result in legal consequences or significantly impact the Personal Data Subject (Article 10 Paragraph (1)).

*Lawsuit*, Personal Data Subjects have the right to sue and receive compensation for violations of the processing of Personal Data concerning them in accordance with statutory provisions (Article 12 Paragraph (1)).

*Administrative Sanctions*, Violation of the provisions of Article 20 Paragraph (l), Article 21, Article 24, Article 25 Paragraph (2), Article 26 Paragraph (3), Article 27, Article 28, Article 29, Article 30, Article 31, Article 32 Paragraph (1), Article 33, Article 34 Paragraph (1), Article 35, Article 36, Article 37, Article 38, Article 39 Paragraph (1), Article 40 Paragraph (1), Article 41 Paragraph (1) and Paragraph (3), Article 42 Paragraph (1), Article 43 Paragraph (1), Article 44 Paragraph (1), Article 45, Article 46 Paragraph (1) and Paragraph (3), Article 47, Article 48 Paragraph (l), Article 49, Article 51 Paragraph (1) and Paragraph (5), Article 52, Article 53 Paragraph (l), Article 55 Paragraph (21) and Article 56 Paragraphs (2) to (4) are subject to administrative

---

<sup>19</sup> Vu Minh Chau, "Protecting Vulnerable Groups through Administrative Law: Strengthening the Right to Good Administration for Social Justice and Inclusion," *International Journal of Law, Justice and Jurisprudence* 5, no. 1 (January 1, 2025): 430–41, <https://www.doi.org/10.22271/2790-0673.2025.v5.i1e.207>.

sanctions (Article 57 Paragraph (1)). The administrative sanctions referred to in Paragraph (1) include: (a) written warning; (b) temporary suspension of Personal Data processing activities; (c) deletion or destruction of Personal Data; and/or (d) administrative fines (Article 57 Paragraph (2)).

Based on the legal protection analysis above, in point 1 of the internal legal protection of Digital Banking in the "Terms and Conditions" and "Privacy Policy" has included legal protection for consumers who use its services, as well as external legal protection contained in the Personal Data Protection Law in Indonesia. Consumer protection plays an important role in the discussion of law and technology, in line with the convergence of telematics that all users of technology systems are consumers of electronic systems. Observing this statement, it means that someone who uses the services of a digital banking platform is a consumer of the banking customer itself, so every user of the service (end-use) based on Article 4 of Law Number 8 of 1999 concerning Consumer Protection also has inherent consumer rights, as follows:

1. The right to comfort, security, and safety when consuming goods and/or services; In this regard, electronic system operators, as digital service providers, must protect consumers using their services from potential dangers, ensuring that consumers are comfortable, safe, and secure when using their services.
2. The right to choose goods and/or services and to receive them in accordance with the exchange rate, conditions, and guarantees promised; Every consumer has the right to make their own decisions without coercion from external parties when using and operating a digital banking service, including providing consent to the privacy policy form.
3. The right to correct, clear, and honest information regarding the conditions and guarantees of goods and/or services; Digital banking service providers are required to protect consumers by providing correct, clear, and honest information, which must be outlined in a privacy policy regarding the use and processing of personal data, particularly regarding the use of cookies.
4. The right to have their opinions and complaints regarding the goods and/or services used heard; Consumers have the right to express opinions and submit complaints regarding the digital banking services they use, and digital banking service providers are obliged to provide a special feature within their services for

consumers to consult and report directly to the digital banking service providers regarding their use of the services.

5. The right to receive advocacy, protection, and appropriate consumer protection dispute resolution; If a dispute or problem arises between a consumer and a service provider arising from the use of an online marketplace and resulting in a loss, the digital banking service provider is obliged to provide consumer protection and dispute resolution efforts. The government also plays a role in providing these protection efforts.
6. The right to receive consumer guidance and education; Because the position of consumers and business actors is sometimes unequal, consumers have the right to receive guidance and education, particularly regarding digital banking operations, so that consumers can understand their rights and how to defend them.
7. The right to be treated or served fairly, honestly, and without discrimination; Consumers have the right to be treated equally when using digital banking services. In this regard, digital banking service providers must provide services correctly, honestly, and equitably.
8. The right to receive compensation, damages, and/or replacement if the goods and/or services received do not comply with the agreement or are not as expected. If a consumer, while using an online marketplace service, later suffers a loss due to a non-compliance with the agreement or an inappropriate performance, in this case the "privacy policy," the consumer is entitled to compensation.
9. Rights regulated in other laws and regulations

Consumer rights are not limited to the Consumer Protection Law alone; consumers may have rights that are additional to other laws and regulations. Based on this, in the context of the use of cookies as an instrument for targeted advertising practices in online marketplaces, reference can be made to laws and regulations governing personal data protection.

## B. Legal Actions That Can Be Taken in the Misuse of Personal Data in Banking Institutions in the Digital Era

Indonesia has provided regulations regarding legal protection of personal data and privacy rights, specifically in Law Number 27 of 2022 concerning Personal Data Protection. However, it has not explicitly addressed the complex threats that may arise in the future, particularly regarding cookies and their use for targeted advertising practices.<sup>20</sup>

Several laws and regulations in Indonesia state that any storage, processing, distribution, and use of personal data and information of service users is permitted with consent. However, the main issue is the processing and use of this personal information for banking purposes. In this case, digital banking uses cookie technology to monitor personal data and all activities and behaviors of consumers using its services (end-use). This illustrates that digital banking collects personal data and information of its consumers for free, distributes personal data to external parties, and exploits it for profit. To understand the need for legal protection in laws and regulations that accommodate and regulate in detail, especially regarding the recording, distribution, and use of personal information of consumers using electronic systems using technology.

In the context of personal data in banking institutions in the digital age, there are several legal actions that both victims and the state can take as a form of protection and law enforcement. Generally, these actions include civil, criminal, and administrative/regulatory channels. In civil law, injured customers can file a lawsuit for damages against the bank or third party that misused their personal data. This is based on the principle of legal responsibility for unlawful acts (*Perbuatan Melawan Hukum*), especially in cases of negligence in maintaining data security.<sup>21</sup> This protection is crucial because data breaches can result in both financial and non-financial losses for customers. Furthermore, through criminal channels, perpetrators of

---

<sup>20</sup> Risky Budiman, "The Development of Personal Data Protection Law in Indonesia: Challenges and Prospects for the Implementation of Law No. 27 of 2022," *Jurnal Smart Hukum (JSH)* 2, no. 1 (September 30, 2023): 24–36, <https://doi.org/10.55299/jsh.v2i1.1352>.

<sup>21</sup> Nabilla Farah Quraisyta and Ilham Dwi Rafiqi, "Legal Protection for Persons with Disabilities Due to Work Accidents After the Job Creation Law," *Hang Tuah Law Journal*, December 15, 2023, 189–205, <https://doi.org/10.30649/htlj.v7i2.162>.

personal data misuse can be subject to criminal sanctions as stipulated in the Personal Data Protection Law (Law No. 27 of 2022), as mentioned in the previous section. These sanctions include imprisonment and/or fines as a deterrent to perpetrators of digital crimes, including cases of data misuse for fictitious credit or illegal online loans. This criminal approach is important given the rise in cybercrime in the banking sector, which exploits weaknesses in data security systems.

This legal remedy is initiated after a legal violation has occurred with the aim of restoring or remediating the situation. In implementing this legal protection, the OJK's repressive role focuses on two targets: legal fintech lending and illegal fintech lending. The repressive legal protection for legal fintech lending, based on the author's interviews with the Directorate of Financial Technology Regulation, Licensing, and Supervision, follows the following procedures:

1. Consumer/Public Complaints to the OJK. The public can file complaints about legal Fintech Lending business activities that violate the law by submitting the following complete documents:
  - (a) A written application containing a description of the complaint, a chronology of the problem, and the amount of the loss;
  - (b) Valid proof of identity. If authorized, please provide a Power of Attorney along with proof of identity of the grantor and grantee;
  - (c) A letter of resolution/response to the complaint and/or receipt of the complaint issued by the Financial Services Provider (PUJK) and/or proof of submission of the complaint to the PUJK;
  - (d) A statement signed on a stamped paper stating that the dispute is not currently in process or has previously been decided by an arbitration institution, court, or other mediation institution, and has not previously been facilitated by the OJK.The complete documents can then be submitted by letter to: Member of the Board of Commissioners for Consumer Education and Protection, Financial Services Authority (OJK), at the Consumer Service Directorate, Menara Radius Prawiro, 2nd Floor, Bank Indonesia Office Complex, JL MH Thamrin No. 2, Central Jakarta 10350, or by email to [konsumen@ojk.go.id](mailto:konsumen@ojk.go.id).
2. Receipt and Filing of Reports. After the OJK receives the complaint, the report and all supporting documents will be reviewed and analyzed by a team of Members of the Board of

Commissioners for Consumer Education and Protection, Financial Services Authority (OJK), to determine whether the report contains elements that indicate a dispute and material loss. If indications of a dispute and material loss are found, the OJK will refer the case to the Financial Services Authority (PUJK) for confirmation and investigation.

3. Submission of Evidence of Complaints. The PUJK will provide a receipt for Complaint registration as proof of receipt of the Complaint and can be used to track the progress of the Complaint Handling process. (a) Notification of receipt of a Complaint to the Consumer shall include at least the following information: Complaint registration number and The date of receipt of the Complaint shall correspond to the date on which the PUJK received the Complaint from the Consumer. (b) The PUJK shall provide proof of receipt of the Consumer Complaint through the following media Telephone, Short Message Services (SMS), Letter/e-mail, Face-to-face.
4. Complaint Classification. Complaints received by the PUJK shall be classified according to the level of resolution, the Complaint information medium, the location of the Complaint, the complexity of the Complaint material, and other matters deemed necessary for classification, for example, using the following parameters: (a) Consumer Complaints submitted to the Complaint Service work unit or function that can be resolved within the next few days; (b) Complaints submitted through the Financial Services Authority; (c) Complaints submitted through print or electronic media; (d) Complaints submitted through Legal Aid Institutions, Non-Governmental Organizations, and/or similar institutions; (e) Complaints submitted through relevant State Institutions, such as the Ombudsman of the Republic of Indonesia, the National Commission on Human Rights, and the State Secretariat.
5. Complaint Analysis and Follow-up. The PUJK conducts verification and analysis to determine the next steps in Complaint Handling. The Complaint Handling work unit and/or function can coordinate with relevant work units. If necessary, the PUJK conducts an investigation to confirm the validity of the Complaint filed by the Consumer. The level of inquiry/investigation is adjusted according to the severity of the Complaint, including the frequency of the incident and the

resulting impact. The PUJK conducts investigations by: (a) Conducting an internal examination of the Complaint competently, correctly, and objectively; (b) Conducting an analysis to confirm the validity of the Complaint. After the PUJK has conducted verification and investigation, the Complaint resolution process is as follows: (a) Complaints that are believed to be untrue: Expressing empathy and clarification to the Consumer. (b) Complaints that are believed to be valid Apology (Redress) / A letter of apology may be issued by the PUJK to the Consumer. Complaint Settlement Offer, Compensation is not provided for potential lost profits and costs incurred by the Consumer in processing the Complaint, including but not limited to consultation fees, costs for processing supporting documents for the Complaint, and accommodation.

6. Mediation between the Disputing Parties. The OJK will bring the two parties together by summoning the PUJK and the consumer to assist the disputing parties in reaching an agreement. At this stage, the OJK only acts as a facilitator between the two parties involved.
7. Coordination with the OJK. The OJK will verify and clarify the status of the complaint with the consumer.

Banks, as financial institutions, are obligated to implement the principle of prudence, ensure the security of electronic systems, and provide complaint and dispute resolution mechanisms for customers. Therefore, legal protection of personal data is not solely the responsibility of the state but also inherent in the institutional obligations of banks as financial services providers.

First, the government needs to continue strengthening the policies and regulations derived from the Personal Data Protection Law to ensure effective implementation, particularly in the high-risk digital banking sector. More technical implementing regulations are needed regarding system security standards, data governance, audit mechanisms, and coordination between institutions, including the Financial Services Authority (OJK) and the Ministry of Communication and Information Technology (Kominfo), to prevent overlapping authority. Second, the Financial Services Authority (OJK) is expected to enhance its oversight and law enforcement function regarding digital banks, not only in institutional and product aspects, but also in protecting customer personal data. The Financial Services

Authority (OJK) needs to ensure that every digital bank truly implements the principle of prudence, has a reliable cybersecurity system, and procedures for handling data breach incidents that are transparent and responsive to customer losses. Third, banking institutions are required to prioritize personal data protection as a core part of good corporate governance. Banks are not only required to comply with regulations but also to proactively increase investment in information technology security, conduct regular training for human resources, and develop privacy policies that are easy to understand and do not harm customers. Fourth, the public, as users of digital banking services, needs to improve their digital literacy and legal awareness regarding personal data protection. Customers must be more critical in providing data, understand their rights, and be willing to use complaint mechanisms in the event of suspected violations. Synergy between the government, supervisory authorities, banking institutions, and the public is key to realizing a digital banking ecosystem that is safe, trustworthy, and guarantees legal certainty in the digital era.

## Conclusion

Based on the discussion on Legal Accountability for Personal Data Misuse in Banking Institutions in the Digital Era, it can be concluded that the transformation of banking towards digital services has had a significant impact on financial services patterns in Indonesia. Banking digitalization provides convenience, speed, and efficiency for the public, but also opens up wider opportunities for potential legal violations, particularly in the form of misuse of customer personal data. Personal data in digital banking services is highly sensitive and valuable information, and therefore must be maximally protected by banks as electronic system operators. Protection of customer personal data is essentially a manifestation of citizens' constitutional rights as guaranteed by the 1945 Constitution. Prior to the enactment of Law Number 27 of 2022 concerning Personal Data Protection, regulations regarding personal data were scattered across various sectoral regulations, including those in the banking and consumer protection sectors, thus creating weaknesses in terms of legal certainty. With the enactment of the Personal Data Protection Law, the state provides a firmer legal basis regarding the rights of data subjects, the obligations of data controllers, and legal accountability mechanisms in the event of violations. Legal liability for

misuse of personal data in digital banking can take various forms, ranging from civil liability in the form of compensation, administrative sanctions by the competent authorities, to criminal sanctions if the elements of a crime are met.

## References

- Aziz, Arya Salman, and Muhammad Abyan Zaidan. "Perlindungan Hukum Nasabah Terhadap Penyalahgunaan Data Pribadi Oleh Pihak Ketiga Dalam Kerja Sama Perbankan Digital." *Ekopedia: Jurnal Ilmiah Ekonomi* 1, no. 2 (April 2025): 120-29. <https://doi.org/10.63822/qwcqac23>.
- Budiman, Risky. "The Development of Personal Data Protection Law in Indonesia: Challenges and Prospects for the Implementation of Law No. 27 of 2022." *Jurnal Smart Hukum (JSH)* 2, no. 1 (September 30, 2023): 24-36. <https://doi.org/10.55299/jsh.v2i1.1352>.
- CH Himabindu, Bandaru Srinivasa Rao. "A Study on Digital Transformation: How Fintech Is Revolutionizing the Banking Landscape." *Journal of Informatics Education and Research* 5, no. 1 (January 31, 2025). <https://doi.org/10.52783/jier.v5i1.2109>.
- Chau, Vu Minh. "Protecting Vulnerable Groups through Administrative Law: Strengthening the Right to Good Administration for Social Justice and Inclusion." *International Journal of Law, Justice and Jurisprudence* 5, no. 1 (January 1, 2025): 430-41. <https://www.doi.org/10.22271/2790-0673.2025.v5.i1e.207>.
- Cvijovic, Jelena, Milica Kostic-Stankovic, and Marija Reljic. "Customer Relationship Management in Banking Industry: Modern Approach." *Industrija* 45, no. 3 (2017): 151-65. <https://doi.org/10.5937/industrija45-15975>.
- Fauzi, Wetria. "The Authority of the Financial Services Authority (OJK) in Publishing Insurance Regulation in the Perspective of Insurance Law in Indonesia." *Jurnal Hukum & Pembangunan* 47, no. 2 (July 2, 2017): 211. [10.21143/jhp.vol47.no2.1452](https://doi.org/10.21143/jhp.vol47.no2.1452).
- Mariyam, Siti, Adhi Putra Satria, Hariyanto Hariyanto, and Ahmad Masum. "Safeguarding Personal Data in Indonesian E-Commerce from a Constitutional Rights Perspective." *Jambe Law Journal* 8, no. 2 (December 31, 2025): 683-711. <https://doi.org/10.22437/x5q9y093>.

- Marzuki, Peter Mahmud. *Penelitian Hukum*. Ke-5. Jakarta: Kencana Prenada Media Group, 2009.
- Matwar, Habib, and Mustapa Khamal Rokan. "The Financial Services Authority (OJK) in Supervising the Bank Payment System and Protecting Customers Against Criminal Acts." *International Journal of Economics, Business and Accounting Research (IJEBAR)* 8, no. 1 (January 12, 2024). <https://doi.org/10.29040/ijebar.v8i1.12193>.
- Nandang Sutrisno, and Nur Gemilang Mahardhika. "Liberalisation of Banking Services Under the Framework of Asean Economic Community: An Indonesian Perspective." *Hang Tuah Law Journal*, August 26, 2022, 33-45. <https://doi.org/10.30649/htlj.v6i1.65>.
- Nastiti, Nur Dyah, and Rahmatina Awaliah Kasri. "The Role of Banking Regulation in the Development of Islamic Banking Financing in Indonesia." *International Journal of Islamic and Middle Eastern Finance and Management* 12, no. 5 (November 11, 2019): 643-62. <https://doi.org/10.1108/IMEFM-10-2018-0365>.
- Permana, Sukarelawati. "Pengaturan Perlindungan Data Pribadi Konsumen Jasa Keuangan Dalam Penggunaan Uang Elektronik Berbasis Server." *Veritas et Justitia* 8, no. 2 (December 26, 2022): 386-414. <https://doi.org/10.25123/vej.v8i2.5213>.
- Putera, Andika Persada. "The Prudential Principle as the Basis in Implementing Banking Transaction." *Hang Tuah Law Journal*, January 15, 2021, 52-60. <https://doi.org/10.30649/htlj.v4i2.16>.
- Quraisyta, Nabilla Farah, and Ilham Dwi Rafiqi. "Legal Protection for Persons with Disabilities Due to Work Accidents After the Job Creation Law." *Hang Tuah Law Journal*, December 15, 2023, 189-205. <https://doi.org/10.30649/htlj.v7i2.162>.
- Rahardjo, Satjipto. *Ilmu Hukum*. Cetakan Ke. Bandung: Citra Aditya Bhakti, 2012.
- Rosadi, Sinta Dewi. "Prinsip-Prinsip Perlindungan Data Pribadi Nasabah Kartu Kredit Dikaitkan Dengan Undang-Undang No 11 Tahun 2008 Tentang ITE Dan Peraturan Bank Indonesia NO 7/6/PBI/2005." *Sosiohumaniora* 19, no. 3 (November 8, 2017). <https://doi.org/10.24198/sosiohumaniora.v19i3.11380>.
- Sriono, Risdalina, Kusno, Indra Kumalasari M, and Hengki Syahyunan. "Legal Protection for Digital Bank Customers in Indonesia: Analysis of Data Confidentiality Regulations and

- Bank Responsibility.” *LITIGASI* 25, no. 2 (October 31, 2024): 301–30. <https://doi.org/10.23969/litigasi.v25i2.18538>.
- Syazali, Emir Adzan, Johni Najwan, and Muskibah Muskibah. “Legal Reform and Strengthening of The Financial Services Authority (OJK): Protecting Investors From Insider Trading in Indonesia.” *As-Siyasi: Journal of Constitutional Law* 4, no. 2 (December 25, 2024): 184–209. <https://doi.org/10.24042/as-siyasi.v4i2.25513>.
- Wahyu, Ruly, and Men Wih Widiatno. “Tanggung Jawab Hukum Pidana Penyelenggara Elektronik Perbankan Terhadap Perlindungan Data Pribadi Nasabah.” *Arus Jurnal Sosial Dan Humaniora* 5, no. 2 (August 29, 2025): 3190–99. <https://doi.org/10.57250/ajsh.v5i2.1620>.
- Yuspın, Wardah, Anindhita Nurfaatin Sukirman, Arief Budiono, Jompon Pitaksantayothin, and Ata Fauzie. “Legal Reconstruction of Indonesian Banking Laws: Challenges and Opportunities for Digital Bank Regulation.” *Varia Justicia* 19, no. 1 (April 29, 2023): 52–69. <https://doi.org/10.31603/variajusticia.v19i1.8019>.

### **Conflicting Interest Statement**

There is no conflict of interest in the publication of this article.

### **Publishing Ethical and Originality Statement**

All authors declared that this work is original and has never been published in any form and in any media, nor is it under consideration for publication in any journal, and all sources cited in this work refer to the basic standards of scientific citation.