RLJ Ratio Legis Journal
ISSN 2830-4624
published by
Master of Law, Faculty of Law
Universitas Islam Sultan Agung

Legal Protection of Customer Personal Data in Digital Financial Transactions at Bank Rakyat Indonesia (BRI)

Titania Vera Modesty

Faculty of Law, Universitas Islam Sultan Agung (UNISSULA) Semarang, Indonesia,
E-mail: titaniaveramodesty.std@unissula.ac.id

Abstract. *The digital transformation of banking through mobile banking services like BRImo facilitates customer transactions but increases vulnerability to personal data misuse and social engineering-based digital fraud. This situation creates a risk of both financial and non-financial losses for customers as data subjects. This study aims to analyze the adoption of Personal Data Protection (PDP) principles in BRI's digital transactions and to examine forms of repressive legal protection, reporting procedures, and the effectiveness of loss recovery mechanisms for customers who fall victim to digital security incidents. This research employs a socio-legal (empirical-juridical) approach with a descriptive-analytical specification. Data sources include primary data obtained through limited interviews with PT Bank Rakyat Indonesia (Persero) Tbk and BRImo customers, as well as secondary data consisting of primary, secondary, and tertiary legal materials. Data were collected through literature reviews and structured interviews, then analyzed using a qualitative descriptive method involving data reduction, data presentation, and systematic conclusion drawing. The research findings indicate that BRI has implemented multi-layered (end-to-end) data governance and security, appointed a data protection function, and provided a Privacy Notice in accordance with Law No. 27 of 2022 and OJK regulations. However, the implementation of consent has not yet fully adopted a granular approach. Regarding repressive protection, the effectiveness of loss recovery is heavily determined by reporting timeframes and the ability to prove the source of the error. BRI provides service recovery in the event of system failures but may refuse refunds if the loss is caused by customer negligence. The availability of escalation channels such as the OJK, LAPS SJK, and the Indonesia Anti-Scam Center (IASC) serves as a crucial means to optimize fund tracing and law enforcement.*

Keywords: *Bank Rakyat Indonesia (BRI); Customers; Digital Financial Transactions; Legal Protection; Personal Data.*

1. Introduction

The development of information and communication technology has brought significant changes to the provision of banking services in Indonesia. Banking services, previously primarily conducted through face-to-face interactions at branch offices, are gradually transforming into digital technology-based services. This development allows customers to conduct various banking activities independently through electronic devices, without being limited by space and time. One form of this transformation is the development of mobile banking services, which provide convenience, speed, and efficiency in conducting financial transactions. This change in service patterns not only impacts how banks interact with customers but also increases the dependence of banking activities on information technology systems and the processing of customers' personal data.[1]

The development of digital banking transactions has had a direct impact on the increasingly intensive processing of customer personal data. When using mobile banking services, personal data is processed from registration and service opening, through identity verification, authentication, transaction execution, account activity monitoring, and customer complaint handling. The data processed includes not only basic identity information but also phone numbers, email addresses, account information, transaction data, and data and information used to authenticate and maintain transaction security.[2]This condition makes personal data an inseparable part of the provision of digital banking services.

In digital financial transactions, personal data plays a strategic role because it is used to identify and verify customers while also supporting transaction security. The registration and activation process for mobile banking services requires identity and contact information, while transaction authentication can involve various credentials and security information. Banks also process transaction data and customer activity patterns for risk management, fraud prevention, compliance with legal obligations, and service quality improvement. The more extensive this processing, the greater the need to ensure that customer personal data is processed legally, in a limited, transparent, and secure manner.[3]

Vulnerability to personal data misuse is increasing with the proliferation of internet-based banking transactions. The integration of various information

[1] Ria Tifanny Tambunan and Muhammad Irwan Padli Nasution, "Challenges and Strategies of Banking in Facing the Development of Digitalization Transformation in the 4.0 Era," Sci-Tech Journal 2, no. 2 (2022): 148–56, https://doi.org/10.56709/stj.v2i2.75.

[2]Maisah, Maisah, et al. "Legal analysis of customer personal data protection in digital banking services in Indonesia." Aufklarung: Journal of Education, Social and Humanities 3.3 (2023): 285-290.

[3] Maisah Maisah et al., "Legal Analysis of Customer Personal Data Protection in Digital Banking Services in Indonesia," Aufklarung: Journal of Education, Social and Humanities 3, no. 3 (2023): 285–90.

technology systems, the use of customers' personal devices, and the involvement of third parties in the provision of digital services can expand the scope for unauthorized data access. In addition to system factors, user behavior is also a factor that can be exploited by criminals through various forms of social engineering, phishing, malware, and other fraudulent methods. Customers under certain circumstances may have difficulty distinguishing between legitimate communications and those created by criminals, leading to the unknowing disclosure of banking data or credentials.[4]

These issues demonstrate that protecting customers' personal data cannot be viewed solely as a technical issue of system security. Personal data relates to customers' legal interests as both data subjects and consumers of financial services. Misuse of personal data can lead to financial losses in the form of unauthorized transactions or loss of funds, as well as non-financial losses in the form of a loss of security, impaired trust in the bank, identity theft, and the possibility of repeated fraud. Therefore, banks, as providers of digital financial services, have a responsibility to ensure that personal data processing is carried out with due regard for security, confidentiality, legal certainty, and protection of customer interests.[5]

Protection of personal data is fundamentally constitutionally based. Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia guarantees the protection of personal self, family, honor, dignity, and property under one's control, as well as the right to a sense of security and protection from the threat of fear to do or not do something that is a basic human right. In the context of digital banking transactions, this personal protection is relevant to the protection of customer personal data processed through the bank's electronic system. This constitutional basis is then realized through various laws and regulations governing the confidentiality of customer information, consumer protection, information technology security, and personal data protection.

Before the existence of specific regulations regarding the protection of personal data, protection of personal information in electronic systems was recognized, among other things, through Law Number 11 of 2008 concerning Electronic Information and Transactions as amended. Article 26 paragraph (1) stipulates that the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned, unless otherwise stipulated by statutory regulations. This provision demonstrates the recognition of the individual's interest in their personal data in electronic

[4] Dewi Fatmala Putri et al., "Analysis of BSI Customer Protection Against Data Leaks in Using Digital Banking," Scientific Journal of Economics and Management 1, no. 4 (2023): 173–81, https://doi.org/https://doi.org/10.61722/jiem.v1i4.331.

[5] Vicky Katiandagho, Diana Darmayanti Putong, and Isye Junita Melo, "Personal Data Protection Law Strengthens Banking Law in Maintaining Customer Data Confidentiality and Protecting Personal Data of Indonesian Citizens," To-Ra Law Journal: Law to Regulate and Protect Society 9, no. 1 (2023): 106–14, https://doi.org/https://doi.org/10.55809/tora.v9i1.212.

activities. However, technological developments and the increasing complexity of data processing have given rise to the need for more comprehensive regulations.[6]

This need was then addressed through Law Number 27 of 2022 concerning Personal Data Protection. This law provides a more comprehensive legal framework regarding the principles of personal data protection, types of personal data, data subject rights, personal data processing, obligations of personal data controllers and processors, data security, dispute resolution, and sanctions for personal data protection violations. Personal financial data is also included in the specific category of personal data. Therefore, data relating to customer financial activities has legal standing and receives special protection under the personal data protection regime.[7]

2. Research Methods

This research uses an empirical juridical approach method, namely an approach that examines law not only as a norm contained in statutory regulations, but also looks at the application of law in practice.[8]This approach is used to analyze the implementation of customer personal data protection in the provision of digital banking services, particularly mobile banking, by linking relevant legal provisions, such as Law Number 27 of 2022 concerning Personal Data Protection, Financial Services Authority regulations, and other provisions with facts found in the field.

3. Results and Discussion

3.1. Legal Regulation of Personal Data in Digital Transactions at BRI (BRImo) and Adoption of Personal Data Protection Principles (PDP) Based on Law No. 27 of 2022 and POJK

Advances in information and communication technology have transformed the delivery of banking services in Indonesia. Previously primarily conducted through in-person interactions at bank branches, banking services have evolved into digital technology-based services that allow customers to conduct various banking activities without having to visit a branch. These changes have not only altered the relationship between banks and customers but have also led to an increasing reliance on electronic data processing.

In the BRImo mobile banking service provided by PT Bank Rakyat Indonesia (Persero) Tbk, the processing of customer personal data takes place from the registration stage, identity verification, service activation, authentication, transaction execution, monitoring transaction activity, to storing transaction

[6]Ibid.
[7]Ibid.
[8] Sugiyono, Quantitative, Qualitative, and R&D Research Methods (Bandung: Alfabeta, 2017), p. 43.

history.[9]Thus, personal data is an inherent part of the provision of digital banking services because it is used to confirm customer identity, carry out transaction instructions, maintain system security, and manage the relationship between the bank and customers.

BRI's position in processing BRImo customers' personal data can be seen based on the provisions of Article 1 number 4 of Law Number 27 of 2022 concerning Personal Data Protection (hereinafter referred to as the PDP Law). This provision stipulates that a Personal Data Controller is any person, public body, and international organization acting individually or jointly in determining the purpose and exercising control over the processing of Personal Data. Meanwhile, Article 1 number 6 of the PDP Law stipulates that a Personal Data Subject is an individual to whom Personal Data is attached.

In this relationship, the customer is the Personal Data Subject, while BRI is the Personal Data Controller because BRI determines the processing purposes and controls the data processing required in the provision of digital banking services. BRI can also involve other parties in data processing based on certain cooperative relationships, so that in such conditions the party can be positioned as a Personal Data Processor as referred to in Article 1 number 5 of the PDP Law.[10]

This position creates a legal obligation for BRI to process personal data in accordance with the principles of personal data protection. Article 3 of the PDP Law stipulates that personal data protection is based on protection, legal certainty, public interest, benefit, prudence, balance, accountability, and confidentiality. These principles form the basis for all personal data processing activities, including digital banking activities. This regulation demonstrates that personal data processing relates not only to the technical aspects of system security but also to the legality of the processing, the intended use of the data, the interests of the Personal Data Subject, transparency, confidentiality, and the accountability of the Personal Data Controller.

An interview with Mariya Ulfah, Assistant Operations Manager of PT Bank Rakyat Indonesia (Persero) Tbk, showed that BRI has implemented governance related to information security and personal data protection in the implementation of BRImo. BRI stated that this governance refers to the PDP Law, the provisions of the Financial Services Authority, and cybersecurity standards. In its implementation, BRI has an information security function, which is realized, among others, through the existence of a Chief Information Security Officer

[9] Muhammad Alfan Ikhwanus Sholeh and Muzayyin, "The Role and Optimization of Customer File Uploading at BRI Unit Arjasa Jember," Writing: Jurnal Penelitian Nusantara 1, no. 3 (2025): 831–38, https://doi.org/https://doi.org/10.59435/menulis.v1i3.200.

[10] Tiara Ayu Lestari and Dian Yulviani, "Legal Perspective on Banks' Obligations to Protect the Confidentiality of Borrower Customer Data (Debtors)," Al-Zayn: Journal of Social Sciences & Law 4, no. 1 (2026): 5489–97, https://doi.org/https://doi.org/10.61104/alz.v4i1.3973.

(CISO), while the personal data protection function is placed within a governance structure that coordinates with the risk management and compliance functions.[11]BRI also stated that its internal policy regarding data confidentiality applies to employees and third parties who collaborate with the bank.

Regulations regarding officials or officers who carry out personal data protection functions are contained in Article 53 of the PDP Law. This provision requires Personal Data Controllers and Personal Data Processors to appoint officials or officers who carry out personal data protection functions under certain conditions. These conditions include when processing is carried out for public services, the core activities of the Personal Data Controller or Personal Data Processor require regular and systematic monitoring on a large scale, or the core activities consist of large-scale processing of Personal Data of a specific nature and/or Personal Data related to criminal acts.[12]Article 54 of the PDP Law further regulates the duties of the official or officer, including providing information and advice to the Controller or Processor regarding compliance with the PDP Law, monitoring compliance, providing advice regarding the assessment of the impact of personal data protection, and acting as a contact person regarding the processing of Personal Data.

In the context of providing digital banking services, these regulations are relevant because banks process large amounts of customer data continuously. This data also includes data that, under the Personal Data Protection Law, has a higher level of protection.[13]Therefore, BRI's governance structure encompasses not only information technology security but also oversight of personal data processing. According to sources, these functions include oversight of privacy notice and consent policies, data security, access control, and information security risk management in digital services.

3.2. Forms of Repressive Legal Protection, Victim Procedures, and the Effectiveness of Dispute Resolution Mechanisms and Loss Recovery

Repressive legal protection in digital financial transactions is a mechanism that operates after an event that causes harm or after the discovery of an alleged violation of customer rights. In the BRImo service, the types of events that may require repressive protection include transactions not carried out by the customer, account takeover, misuse of personal data, phishing, smishing, social engineering, the use of unauthorized applications, and other forms of fraud that

[11] Mariya Ulfah, "Interview with Mariya Ulfa as Assistant Manager of Operations at BRI Bank" (Semarang, nd).

[12] Hikmawan Ajiraga, "The Role and Responsibilities of Data Protection Officers in the Implementation of Personal Data Protection," Asas Wa Tandhim: Journal of Law, Education and Social Religion 5, no. 1 (2026): 261–290, https://doi.org/https://doi.org/10.47200/awtjhpsa.v5i1.3209.

[13] Alieffa Nanda Ervian, Hamzah, and Sepriyadi Adhan S, "Legal Protection for Customers Against Personal Data Leaks in Digital Banking Services in Indonesia," Al-Zayn: Journal of Social Sciences & Law 3, no. 6 (2025): 8785–93, https://doi.org/https://doi.org/10.61104/alz.v3i6.2783.

result in reduced funds in the customer's account. The nature of digital transactions means that handling these incidents cannot be done simply by examining the customer's transaction evidence, but requires tracing the series of electronic activities that occur before, during, and after the transaction.

Normatively, one of the main bases for repressive protection for Personal Data Subjects is contained in Article 12 paragraph (1) of Law Number 27 of 2022 concerning Personal Data Protection. This provision states that "Personal Data Subjects have the right to sue and receive compensation for violations of the processing of Personal Data about them in accordance with the provisions of laws and regulations." This provision positions customers as Personal Data Subjects who have the right to obtain redress if there are violations in the processing of their personal data.[14]This right differs from the right to a refund for any unrecognized transaction. Compensation under Article 12 relates to violations of Personal Data processing, so it must first be determined whether there was any legally justifiable act or failure in data processing.

In digital banking transactions, the relationship between personal data breaches and financial losses can take different forms. Personal data can be misused by the perpetrator to gain account access, while financial losses arise after the perpetrator has completed the transaction. In other circumstances, the perpetrator can obtain customer credentials through phishing or social engineering without a breach of the bank's systems. These differences in the source of the incident influence the determination of who can be held accountable.[15]If a security leak or failure originates from a system under the bank's control, the issue relates to BRI's obligations as the Personal Data Controller and as a Financial Services Provider (PUJK). If the data is obtained through fraudulent actions against customers, the issue of accountability also involves the perpetrator as the party who obtained or used the data unlawfully.

Article 46 paragraph (1) of the PDP Law stipulates that in the event of a failure in Personal Data Protection, the Personal Data Controller is required to provide written notification within 3 x 24 hours to the Personal Data Subject and the institution. The notification must at least contain the Personal Data that was disclosed, when and how the Personal Data was disclosed, and efforts to handle and recover from the disclosure of Personal Data.[16]This provision becomes

[14] Jovita Najova and Rachmadi Usman, "Digital Financial Sector; Fintech; Legal Harmonization; Consumer Protection; Financial Regulation: Preventive and Repressive Efforts to Protect Fintech Service Users," Al-Zayn: Journal of Social Sciences & Law 4, no. 4 (2026): 11100–114, https://doi.org/https://doi.org/10.61104/alz.v4i4.9641.

[15] Emmi Rahmiwita Nasution and Zuwairiah Harmika, "Legal Protection for Bank Customers Experiencing Personal Data Leaks Reviewed from Law Number 27 of 2022," Innovative: Journal Of Social Science Research 5, no. 4 (2025): 11373–84, https://doi.org/https://doi.org/10.31004/innovative.v5i4.20892.

[16] Musrika Yanti, "Analysis of Civil Liability in Data Leaks: Synchronization of the Personal Data Protection Law and the Civil Code," Journal of Social Sciences and Humanities 1, no. 4 (2025): 1539–49, https://doi.org/https://doi.org/10.63822/n9bwps44.

relevant if the incident experienced by the customer is related to a failure to protect data under BRI's control. In these conditions, handling is not only related to transactions that have occurred, but also to the obligations of the Personal Data Controller in handling and remediating the consequences of data protection failures.

Article 12 of the PDP Law also needs to be read in conjunction with Article 57, which regulates administrative sanctions. Article 57 paragraph (2) stipulates that administrative sanctions can take the form of written warnings, temporary suspension of Personal Data processing activities, deletion or destruction of Personal Data, and/or administrative fines. Article 57 paragraph (3) stipulates that the maximum administrative fine is 2% of annual revenue or annual receipts for the violation variable. These administrative sanctions are an enforcement instrument against Personal Data Controllers or Personal Data Processors who commit violations, while the customer's right to sue and obtain compensation is a different recovery mechanism.[17]This separation is important so that administrative sanctions are not equated with the compensation that customers must receive.

In the banking sector, repressive mechanisms are also based on OJK Regulation No. 22 of 2023 concerning Consumer and Public Protection in the Financial Services Sector. This regulation outlines PUJK's obligations to protect consumer assets, privacy, and data and provides a mechanism for handling complaints and resolving disputes. This regulation positions customer complaints as part of PUJK's obligations, not merely an additional service provided based on internal bank policies.[18]

Based on an interview with Mariya Ulfah, Assistant Operations Manager at PT Bank Rakyat Indonesia (Persero) Tbk, when customers encounter unknown transactions or indications of account misuse, they are directed to immediately report the matter through official BRI channels. The channels mentioned in the interview include the Help Center menu in the BRImo app, Contact BRI 1500017, and the official Sabrina WhatsApp account. Once the report is received, the internal system issues a complaint ticket number, which is used to monitor the progress of the handling.[19]In the initial stage, the report is followed by security measures in the form of temporarily blocking the account or accounts that are suspected of being misused.

[17] Al Satria Diah and Sidi Ahyar Wiraguna, "Legal Responsibility of E-Commerce Platforms for Personal Data Leaks in the Perspective of Law No. 27 of 2022," Journal of Law and Public Policy Studies 2, no. 2 (2025): 1089–96, https://doi.org/https://doi.org/10.62379/3w415f14.
[18] Fuad Fuad, Rio Rama Baskara, and Anas Urbaningrum, "Legal Protection Design for Consumers and Personal Data for Business Activities Using Fintech in Indonesia," Jurnal Rectum 7, no. 1 (2025): 176–87, https://doi.org/http://dx.doi.org/10.46930/jurnalrectum.v7i1.5360.
[19] Ulfah, "Interview with Mariya Ulfa as Assistant Manager of Operations at BRI Bank."

4. Conclusion

1. Legal Regulation of Personal Data in Digital Transactions at BRI (BRImo) and Adoption of Personal Data Protection Principles (PDP) Based on Law No. 27 of 2022 and POJK, BRI has been realized as a Personal Data Controller through the implementation of end-to-end security governance (encryption, DLP, TPRM), the appointment of PDP supervisory functions, and the provision of Privacy Notices throughout the customer data processing cycle. 2. Repressive Legal Protection, Victim Procedures, and the Effectiveness of Dispute Resolution and Loss Recovery Mechanisms provide a framework for handling incidents for customers through BRI's official complaint channels, account blocking, digital log investigations, and escalation to the Financial Services Authority (OJK), the Financial Services Authority (SJK) LAPS, the Police, and the Indonesia Anti-Scam Center (IASC). Customers' initial steps in responding to incidents (especially within the first 12 hours) and securing electronic evidence are crucial for the chances of recovering funds, but the effectiveness of financial loss recovery is still hampered by information asymmetry.

5. References

Journals:

Albariq, Achmad Zahid Zhafif. "Kebijakan Hukum Pidana Terhadap Penggunaan Data Pribadi Dalam Kejahatan Digital." Al-Zayn: Jurnal Ilmu Sosial & Hukum 4, no. 4 (2026): 12410–15. https://doi.org/10.61104/alz.v4i4.11281.

Daffa, Muh. Faraz, Sufirman Rahman, dan Abdul Qahar. "Kekuatan Pembuktian Tanda Tangan Elektronik Sebagai Alat Bukti Dalam Perkara Perdata." Journal of Lex Philosophy (JLP) 4, no. 1 (2023): 205–21. https://doi.org/10.52103/jlp.v4i1.1499.

Diah, Al Satria, dan Sidi Ahyar Wiraguna. "Tanggung Jawab Hukum Platform E-Commerce Atas Kebocoran Data Pribadi Dalam Perspektif UU No. 27 Tahun 2022." Jurnal Kajian Hukum Dan Kebijakan Publik 2, no. 2 (2025): 1089–96. https://doi.org/10.62379/3w415f14.

Ervian, Alieffa Nanda, Hamzah, dan Sepriyadi Adhan S. "Perlindungan Hukum Terhadap Nasabah Atas Kebocoran Data Pribadi Dalam Layanan Perbankan Digital Di Indonesia." Al-Zayn: Jurnal Ilmu Sosial & Hukum 3, no. 6 (2025): 8785–93. https://doi.org/10.61104/alz.v3i6.2783.

Books:

Ali, Zainuddin. Metode Penelitian Hukum. Jakarta: Sinar Grafika, 2016.

Badrulzaman, Mariam Darus. Klausula Baku Dalam Perjanjian Standar Dan Perlindungan Konsumen. Bandung: Citra Aditya Bakti, 2001.

Barkatullah, Abdul Halim. Hukum Transaksi Elektronik Di Indonesia: Sebagai Panduan Dalam Menghadapi Era Perdagangan Bebas Digital. Bandung: Nusa Media, 2017.

Budhijanto, Danrivanto. Cyber Law Dan Revolusi Industri 4.0. Bandung: Logoz Publishing, 2019.

Fuady, Munir. Perbuatan Melawan Hukum. Bandung: Citra Aditya Bhakti, 2002.

Hadjon, Philipus M. Perlindungan Hukum Bagi Rakyat Di Indonesia. Surabaya: Bina Ilmu, 1987.

Hermansyah. Hukum Perbankan Nasional Indonesia. Ed. 3. Jakarta: Prenadamedia Group, 2020.

Kasmir. Bank Dan Lembaga Keuangan Lainnya. Ed. revisi. Jakarta: Rajawali Pers, 2014.

Kelsen, Hans. Hukum Dan Negara: Seri Teori Hukum Murni. Diterjemahkan oleh Raisul Muttaqien. Yogyakarta: Nusamedia, 2021.

Makarim, Edmon. Pengantar Hukum Telematika: Suatu Kompilasi Kajian. Jakarta: RajaGrafindo Persada, 2005.

Regulations:

Financial Services Authority of the Republic of Indonesia. Financial Services Authority Regulation Number 1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector.

Financial Services Authority of the Republic of Indonesia. Financial Services Authority Regulation Number 18/POJK.07/2018 concerning Consumer Complaints Services in the Financial Services Sector.

Financial Services Authority of the Republic of Indonesia. Financial Services Authority Regulation Number 38/POJK.03/2016 concerning the Implementation of Risk Management in the Use of Information Technology by Commercial Banks.