Legal Protection of Bank Rakyat Indonesia Customers Against Personal Data Breaches under Law No. 27 of 2022 and Law No. 1 of 2024

Azzahrah Munirah Kesuma*, Muhammad Ilman Abidin

Study Program of Law, Faculty of Law, Bandung Islamic University, Indonesia.

azzahrahkesuma@gmail.com, muhammadilmanabidin@unisba.ac.id

Abstract. The banking sector holds a strategic position as a financial intermediary supporting national economic development. The rapid growth of digital banking services driven by information technology aims to enhance convenience and efficiency for customers. In providing such services, banks are legally obligated to protect customers by safeguarding the confidentiality of personal data in accordance with the confidentiality principle stipulated in Article 40 of Law Number 10 of 1998 on Banking. Personal data protection is further strengthened under Law Number 27 of 2022 on Personal Data Protection and Article 15 paragraph (2) of Law Number 1 of 2024 on Electronic Information and Transactions, which imposes responsibility on Electronic System Operators. In practice, personal data breaches involving customers of Bank Rakyat Indonesia (Bank BRI) have resulted in financial losses. This article examines the legal protection afforded to Bank BRI customers whose personal data have been compromised and analyzes the bank's liability for such incidents. This study employs a normative juridical research method based on library research. The findings show that customer protection is implemented through preventive and repressive legal measures, while Bank BRI's liability arises from its obligations as a Personal Data Controller and an Electronic System Operator.

Keywords: *legal protection, personal data protection, banking customers*.

*azzahrahkesuma@gmail.com

A. Introduction

Banking is one of the financial institutions that has a strategic role in supporting the economy and national development (Usanti et al., 2017). The bank works based on public trust and functions as a financial intermediary, between parties who have a surplus of funds and parties who lack funds. In the Indonesian context, banks also carry out their functions as agents of development which aim to support the implementation of national development to realize equity, economic growth, and national stability, as stated by Heru Soepraptomo that banks are expected to be able to increase national savings, grow business activities, and optimize the allocation of economic resources.

Sri Redjeki Hartono in his inauguration speech as Professor of Commercial Law at the Faculty of Law, Diponegoro University in 1995, said that "There have been changes and shifts in people's patterns of life and behavior over the past two decades, which have shifted from the old pattern to the new pattern. These changes are triggered by a variety of factors, including economic globalization, advances in communication and information, and market needs.

Financial Services Authority Regulation Number 12/POJK.03/2018 defines digital banking services as banking services through electronic media that utilize customer data to provide convenience, speed, and efficiency in obtaining information, communicating, and conducting banking transactions, which in its implementation must still ensure the security of funds and customer trust as stipulated in Article 37B paragraph (1) of Law Number 10 of 1998 concerning Banking Requires every bank to guarantee the public funds that are deposited, considering that third-party funds collected from the community reach around 60-70% of the total funds managed by the bank.

The large proportion of public funds shows that banks are highly dependent on public trust in order to carry out their operations optimally. From the data, it appears that public funds have a very large role in bank operations and national development. Therefore, if people's trust in banks decreases to the point that they are reluctant to save their funds, it will have a serious impact on the sustainability of banking activities

In the context of the legal relationship formed between the two, the bank and the customer have a contractual and non-contractual relationship. The contractual relationship is based on an agreement made between the bank as a creditor and the customer as a debtor. Meanwhile, the non-contractual relationship reflects the mandate carried out by the bank for the benefit of its customers. When viewed from a historical perspective, the main function of a bank basically begins as a trustee of the customer who deposits the funds (Fuady, 1999).

But in reality, there are still often various cases related to the decline in customer trust in the bank. This is due to the implementation of personal data protection by digital banks which still have a number of weaknesses. This condition shows that data protection efforts have not been running optimally, causing concern in the community and potentially reducing the level of public trust in the digital banking system that continues to develop.

One example of a case of personal data breach case involving a Bank Rakyat Indonesia customer (hereinafter abbreviated as Bank BRI), the case was revealed in the Singaraja District Court Decision Number 635/Pdt.G/2023/PN.Sgr dated September 19, 2024, the victim was named Nyoman Werdiasa. Nyoman started opening a BRI Simpedes account and started saving at Bank BRI since October 4, 2016. Nyoman lost his savings of IDR 248 million which was stored in the BRI Simpedes account. The loss began on the night of Saturday, August 19, 2023 at 21.14 WITA, he received a notification from the BRImo application regarding a series of outgoing transactions. In a short time, the funds in his account were lost without his permission or knowledge with a total loss of Rp248,012,500 (two hundred and forty-eight million twelve thousand five hundred rupiah).

In the trial process, the Defendant (PT Bank Rakyat Indonesia Tbk.) filed an exception on the grounds that the losses suffered by the Plaintiff were not caused by errors or negligence in the BRI Bank system, but due to the negligence of the Plaintiff himself who allegedly accessed the fake link (phishing) so that his personal data was misused by third parties. Departing from this case, it appears that there is still a gap in the application of the principle of customer confidentiality at Bank BRI, where banks tend to place responsibility for the loss of funds to customers due to personal negligence.

After outlining the damages and filing a claim for damages against the Defendants, the ssPlaintiff then faced the exception filed by the Defendant. In its exception, the Defendant stated that the loss of balance in the Plaintiff's account was not caused by a system error, but was the Plaintiff's own negligence. According to the Defendant, the Plaintiff's account is registered on the BRImo

service with a mobile phone number 081353008449 so that every transaction or device transfer can only be done by sending an OTP code, SMS link, or password to the number. Thus, the Defendant argues that the transaction that occurs is a legitimate transaction because it can only be done if the Plaintiff himself enters or submits the security code.

The loss of customer balance occurs after an action from a certain party on behalf of or acting as if it were a party to Bank BRI. This action causes the customer to provide certain data and/or access which then leads to the transfer of funds from the customer's account without the consent of the customer concerned. For this incident, the customer took legal action by filing a lawsuit with the court. However, based on the trial process that has taken place, the Panel of Judges in its decision stated that the Plaintiff's lawsuit is unacceptable (*Niet Ontvankelijke Verklaard*) and sentenced the Plaintiff to pay the costs of the case.

The protection of personal data in Law Number 1 of 2024 concerning Information and Electronic Transactions (UU ITE) is not strictly regulated, but its substance is reflected in the provisions of its articles. Article 26 of the ITE Law emphasizes that any use of information through electronic media related to a person's personal data must obtain consent from the party concerned. If personal data is used without permission, the aggrieved individual has the right to file a lawsuit for the violation and loss experienced.

According to Article 4 of Law Number 27 of 2022 concerning Personal Data Protection, information such as full name, email address, residential address, and telephone number is included in the category of Personal Data that is general. A telephone number that can be accessed by a third party can be considered personal data that, when combined with other information, is capable of identifying a person. Meanwhile, information related to personal financial data known by third parties, such as customer active transaction data through the BRImo application, is included in the category of Personal Data that is specific.

The breach of personal data of Bank BRI customers, including phone numbers, customer names, and personal financial information that can be accessed or contacted by third parties, raises concerns about the security of personal data stored by Bank BRI. It calls into question whether customers' personal data is adequately protected within the Bank BRI system or remains vulnerable to unauthorized access or hacking.

Based on the background described above, the research problems to be examined in this study are as follows: **"**How is the legal protection of customers of Bank Rakyat Indonesia (Bank BRI) against personal data breaches regulated under Law Number 27 of 2022 on Personal Data Protection and Law Number 1 of 2024 on Electronic Information and Transactions?" and "What is the liability of Bank Rakyat Indonesia (Bank BRI) for its customers' personal data breaches under Law Number 27 of 2022 on Personal Data Protection and Law Number 1 of 2024 on Electronic Information and Transactions?.

This study aims to examine the legal protection afforded to Bank Rakyat Indonesia (Bank BRI) customers against personal data breaches and to analyze the bank's liability under Law Number 27 of 2022 on Personal Data Protection and Law Number 1 of 2024 on Electronic Information and Transactions.

B. Method

This study employs a normative juridical research method by examining secondary data in the form of applicable laws and regulations relevant to the research topic. The research is descriptive-analytical in nature, aiming to systematically describe legal facts and issues related to customer protection and subsequently analyze them by referring to statutory provisions, legal theories, and their application in practice. Data collection is conducted through library research using three types of legal materials, namely primary, secondary, and tertiary legal materials, in order to obtain accurate and comprehensive data that provide a thorough understanding of legal protection for banking customers.

C. Result and Discussion

Legal protection of Customer of Bank Rakyat Indonesia (Bank BRI) against Personal Data Breaches Regulated Under Law No. 27 of 2022 on Personal Data Protection and Law No. 1 of 2024 on Electronic information and Transactions

The protection of customers' personal data constitutes a constitutional right as guaranteed under Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which affirms the right to personal security, privacy, and protection of property. This constitutional mandate is further elaborated through statutory regulations, particularly Law Number 27 of 2022 on Personal Data Protection and Law Number 1 of 2024 on Electronic Information and Transactions, which require the state and relevant actors to ensure effective legal protection mechanisms in the processing of personal data. In the context of digital banking, legal protection encompasses both preventive measures aimed at preventing data breaches and repressive measures providing remedies when violations occur. Therefore, an assessment of customer legal protection must begin with determining the legal position of the bank in managing customers' personal data.

1. Bank BRI's Position as a Personal Data Controller and Electronic System Operator

In providing digital banking services, Bank BRI plays a central and dominant role in collecting, storing, processing, and securing customers' personal data through electronic systems. Customers, as users of banking services, do not possess control over the technical infrastructure, security mechanisms, or data processing systems operated by the bank. This condition places Bank BRI in a strategic legal position that must be clearly defined to assess its obligations toward customers' personal data protection.

Based on Article 1 point 4 of Law Number 27 of 2022 on Personal Data Protection, Bank BRI qualifies as a Personal Data Controller because it independently determines the purposes and exercises control over the processing of customers' personal data. This includes determining what data are collected, how they are processed, and for what purposes they are used in digital banking services. Consequently, Bank BRI bears direct legal responsibility for ensuring that such processing is conducted lawfully, fairly, transparently, and in accordance with the principles of personal data protection.

Simultaneously, under Government Regulation Number 71 of 2019 and Law Number 1 of 2024 on Information and Electronic Transactions, Bank BRI also acts as an Electronic System Operator responsible for the provision, management, and operation of electronic banking systems. As an Electronic System Operator, the bank is legally obliged to operate electronic systems in a reliable, secure, and accountable manner, including ensuring the protection of electronic data and information from unauthorized access, misuse, or system failure.

This dual position places significant legal obligations on Bank BRI, both substantively and technically. The PDP Law functions as lex specialis governing the protection of personal data, while the ITE Law operates as lex generalis reinforcing the bank's technical obligations in maintaining electronic system security and reliability. Accordingly, Bank BRI's legal status as both a Personal Data Controller and an Electronic System Operator forms the normative foundation for customer legal protection against personal data breaches in digital banking services.

2. Preventive and Repressive Legal Protection

Legal protection for banking customers is implemented through preventive and repressive mechanisms, which must operate in an integrated manner to ensure effective protection of customers' rights. Preventive legal protection is primarily aimed at preventing personal data breaches before they occur, while repressive legal protection focuses on providing remedies and accountability when violations have already taken place.

Preventive legal protection is reflected in the obligation of banks to apply the prudential principle and to ensure the security of personal data, as stipulated in Article 39 of the PDP Law and Article 15 of the ITE Law. These provisions require banks, as Personal Data Controllers and Electronic System Operators, to implement appropriate technical and organizational measures to protect personal data. Such measures include obtaining valid consent for data processing, implementing secure and multi-layered authentication systems, and preventing unauthorized access, disclosure, or misuse of customers' personal data.

These preventive obligations are further reinforced by Government Regulation Number 71 of 2019, which requires Electronic System Operators to apply personal data protection principles throughout the entire data processing lifecycle. In addition, Article 26 paragraph (1) of the ITE Law recognizes personal data protection as an integral part of privacy rights in the use of information

technology. In the context of digital banking, this provision also implies the protection of customers' anonymity and confidentiality in electronic transactions, ensuring that customers' identities and transaction activities are not improperly accessed or exploited by unauthorized parties.

Repressive legal protection applies when a personal data breach has occurred and is aimed at restoring customers' rights while ensuring legal accountability for violations. Article 65 of the PDP Law explicitly grants personal data subjects the right to seek legal remedies and compensation for losses suffered as a result of personal data breaches. In addition, Article 57 of the PDP Law provides for administrative sanctions against Personal Data Controllers who fail to fulfill their legal obligations, including written warnings, suspension of data processing activities, and administrative fines.

These repressive mechanisms are consistent with the Consumer Protection Law and Financial Services Authority regulations, which obligate financial service providers to compensate consumers for losses arising from negligence or unlawful conduct. Accordingly, repressive legal protection serves not only as a recovery mechanism for aggrieved customers but also as a deterrent aimed at encouraging banks to strengthen their data protection systems and comply with applicable legal standards.

3. Judicial Considerations in the Singaraja District Court Decision Number 635/Pdt.G/2023/PN.Sgr

In the Singaraja District Court Decision Number 635/Pdt.G/2023/PN.Sgr, the panel of judges emphasized customer negligence resulting from phishing and granted the exception submitted by Bank BRI. The court's consideration focused primarily on the assumption that the loss of customer funds occurred due to the customer's own actions, without conducting an in-depth examination of the bank's obligations and responsibilities as a Personal Data Controller and Electronic System Operator.

From the perspective of customer legal protection, this approach raises significant juridical concerns. Customers are structurally in a weaker position in legal relations with banks, as they have no control over the bank's electronic systems, security infrastructure, or internal data protection mechanisms. An approach that places primary responsibility on customers risks undermining the essence of legal protection, which is intended to safeguard parties who are vulnerable in asymmetric legal relationships.

Furthermore, the decision did not sufficiently assess Bank BRI's fiduciary duty and its obligation to ensure system reliability and personal data security. Given the technical complexity of phishing cases and the bank's superior capacity to explain system security mechanisms, placing the burden of proof predominantly on customers may result in substantive injustice. Therefore, the bank's conduct in the a quo case may be juridically qualified as an unlawful act under Article 1365 of the Civil Code, as it contradicts statutory obligations and results in financial losses for customers.

Singaraja District Court Decision Number 635/Pdt.G/2023/PN.Sgr, the panel of judges emphasized customer negligence due to phishing and granted the exception submitted by Bank BRI, without conducting an in-depth examination of the bank's obligations as a Personal Data Controller. From the perspective of customer legal protection, this approach raises concerns, as customers are structurally in a weaker position and have no control over the bank's electronic systems and security mechanisms.

Bank Rakyat Indonesia's (Bank BRI) Liability for Its Customers' Personal Data Breaches under Law No. 27 of 2022 on Personal Data Protection and Law No. 1 of 2024 on Information and Electronic Transactions.

Legal liability arises when a legal subject fails to fulfill statutory obligations, resulting in losses to other parties. In the banking sector, liability is closely linked to the bank's position as a financial services business actor that manages customers' funds and personal data through digital banking systems. Consequently, in cases of personal data breaches leading to financial losses, the legal issue extends beyond the occurrence of loss to determining which party must bear responsibility under applicable laws.

Under Law Number 10 of 1998 on Banking, Bank BRI is legally obligated to safeguard the confidentiality of customers' personal and financial data. This obligation is reinforced by Article 15 paragraph (2) of Law Number 1 of 2024 on Electronic Information and Transactions, which holds

Electronic System Operators responsible for the operation and security of their systems. Furthermore, Law Number 27 of 2022 on Personal Data Protection positions Bank BRI as a Personal Data Controller with duties to ensure lawful processing, confidentiality, and security of customers' personal data. These obligations arise within a contractual relationship between banks and customers, formed through agreements and consent to digital banking services, requiring banks to maintain reliable and secure systems.

1. Classification of Customers' Personal Data and Its Implications for Bank BRI's Liability

The PDP Law defines personal data broadly to include any data that can identify an individual, either directly or indirectly. In digital banking services, personal data plays a crucial role in customer identification, verification, and transaction security. The PDP Law classifies personal data into general personal data and specific personal data.

General personal data includes information such as telephone numbers and IP addresses, which, in digital banking, function not only as communication tools but also as instruments of customer identification and verification. In the a quo case, Bank BRI used the customer's registered phone number to transmit OTP codes and device-change links, indicating active processing of general personal data. Any failure to secure such data may therefore constitute a breach of general personal data protection obligations.

Specific personal data under the PDP Law includes sensitive data, particularly personal financial data. Although OTPs and device-change links are not expressly categorized, the PDP Law adopts a functional approach, assessing data based on its role and impact. Since OTPs and device-change links function as authentication tools granting access to customers' financial data, they are functionally attached to personal financial data and possess a high level of sensitivity. Their misuse may therefore result in significant harm, reinforcing the bank's obligation to ensure heightened protection.

2. One-Time Passwords (OTPs) as Authentication Instruments in Electronic Systems

The use of OTPs as authentication instruments has a normative basis in Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions. Authentication mechanisms may combine factors such as something possessed, known, or inherent to an individual. OTPs sent to registered phone numbers form part of a multi-layered authentication system commonly used in digital banking.

Article 71 of the PP PSTE emphasizes that the reliability of authentication mechanisms is the responsibility of the Electronic System Operator. Accordingly, banks bear responsibility not only for the success of transactions but also for ensuring that authentication processes are secure and resistant to misuse. In the a quo case, Bank BRI argued that transactions were conducted using correct credentials; however, no detailed technical evidence was presented to demonstrate that authentication was consciously and legitimately performed by the customer. This absence of proof is relevant, given that authentication mechanisms are integral to personal data management and system security under the bank's control.

3. Bank BRI's Liability in the Singaraja District Court Decision Number 635/Pdt.G/2023/PN.Sgr Based on the Principle of Presumption of Liability

In digital banking, banks exercise full control over electronic systems, security mechanisms, and personal data processing, while customers lack technical access to these systems. This imbalance, coupled with the fiduciary nature of the bank–customer relationship, supports the application of the principle of presumption of liability. Under this principle, business actors are deemed responsible for consumer losses unless they can prove the absence of fault or negligence.

Applying this principle to personal data breaches, Bank BRI should, in principle, bear responsibility for customer losses arising from transactions conducted through systems under its exclusive control. Shifting the burden entirely to customers, as occurred in the Singaraja District Court Decision Number 635/Pdt.G/2023/PN.Sgr, places customers in an unfair position, requiring them to prove technical failures beyond their capacity. The court's emphasis on customer negligence without a substantive examination of system reliability reflects a gap between the normative construction of liability under personal data protection law and its application in judicial practice. This condition risks

weakening legal protection for digital banking customers and undermines the objective of ensuring accountability for personal data controllers.

D. Conclusion

Legal protection for Bank Rakyat Indonesia (Bank BRI) customers against personal data breaches is normatively supported by the 1945 Constitution, Law Number 27 of 2022 on Personal Data Protection, and Law Number 1 of 2024 on Electronic Information and Transactions. Bank BRI is legally positioned as a Personal Data Controller and an Electronic System Operator, bearing obligations to ensure the security of customers' personal data and the reliability of digital banking systems through preventive and repressive measures. However, judicial practice, as reflected in the Singaraja District Court Decision Number 635/Pdt.G/2023/PN.Sgr, shows that such protection has not been substantively implemented, as the court emphasized customer negligence due to phishing without a thorough examination of the bank's obligations and system reliability. This indicates a gap between normative legal protection and its application in practice.

Bank BRI is therefore recommended to strengthen the implementation of personal data protection and the security of digital banking systems, particularly in relation to authentication mechanisms and risk management. In addition, the application of the presumption of liability principle should be consistently upheld in handling personal data breach cases, considering the technical nature of electronic systems that are difficult for customers to assess. Enhancing customer awareness and education regarding cybercrime risks, especially phishing, is also essential to improve the safe use of digital banking services.

Acknowledgement

With the highest respect, the author would also like to express gratitude and prayers to the following individuals, hoping that Allah SWT grants them the best rewards:

1. Prof. Ir. A. Harits Nu'man, M.T., Ph.D., IPU., Rector of Universitas Islam Bandung;
2. Prof. Dr. Efik Yusdiansyah, S.H., M.Hum., Dean of the Faculty of Law, Universitas Islam Bandung;
3. Dr. Ade Mahmud, S.H., M.H., Head of the Undergraduate Law Study Program, Faculty of Law, Universitas Islam Bandung;
4. Prof. Dr. Lina Jamilah, S.H., M.H., Academic Advisor;
5. Muhammad Ilman Abidin, S.H., M.H., Thesis Supervisor.

References

Efrianto, L. B. P., & Diana Wiyanti. (2022). Tanggung Jawab Bank Terhadap Nasabah yang Dananya Terbukti Digunakan oleh Karyawan Bank. *Jurnal Riset Ilmu Hukum*, 107–112. https://doi.org/10.29313/jrih.v2i2.1457

Fadilla, M. F., & Nurcahyono, A. (2023). *Kajian Kriminologi terhadap Penyebaran Data Pribadi yang Dilakukan oleh Peretas (Hacker) Dihubungkan dengan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi*. https://journal.sbpublisher.com/index.php/lol

Ririn Puspita Dewi, & Diana Wiyanti. (2024). Perlindungan Hukum Nasabah atas Peretasan Data Pribadi ditinjau dari Undang Undang. *Jurnal Riset Ilmu Hukum*, 95–100. https://doi.org/10.29313/jrih.v4i2.5193

Djumhana, M. Banking Law in Indonesia. Citra Aditya Bakti, Bandung, 2006.

Fuady, Munir. Banking Law. Citra Aditya Bakti, Bandung, 1999.

Hadjon, Philipus M. Introduction to Indonesian Administrative Law. Gadjah Mada University Press, Yogyakarta, 2011.

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

Law Number 8 of 1999 concerning Consumer Protection.

Law Number 10 of 1998 concerning Banking.

Law Number 11 of 2008 concerning Information and Electronic Transactions.

Law Number 27 of 2022 concerning Personal Data Protection.

Marlina, A., & Bimo, W. A. “Bank Digitalization to Improve Service and Customer Satisfaction.” Innovator, Vol. 7, No. 1, 2018, pp. 14–34.

Soekanto, Soerjono. Normative Law Research: A Brief Overview. PT Raja Grafindo Persada, Jakarta, 2009.

The 1945 Constitution of the Republic of Indonesia.

Usanti, Trisadini P., & Somad, Abd. Banking Law. Kencana, Surabaya, 2017.