5th CoNeScINTech
Conference on Business, Social Sciences and Technology

Volume 5 No 1 (2025)

Received : June 13, 2025
Accepted : September 17, 2025
Published : September 18, 2025

Conference on Business, Social Sciences and Technology
https://journal.uib.ac.id/index.php/conescintech

The Legal Responsibility of Bank Central Asia for the Protection of Customer's Personal Data in Cases of Misuse by Third Parties

Fernando[1], Agustianto[2]
2351046.fernando@uib.edu
[1,2]Faculty of Law, Universitas Internasional Batam, Batam, Indonesia

Abstract

The advancement of technology in the digital era has significantly impacted various sectors, including banking, particularly in the management and protection of customers' personal data. Banks are legally and ethically responsible for safeguarding the personal information entrusted to them. This study aims to analyze the legal protection and liability of Bank Central Asia (BCA) in cases involving the misuse of customer personal data by third parties.

The research is grounded in an empirical legal approach, supported by statutory analysis. It examines key regulations in Indonesia, including Law No. 27 of 2022 on Personal Data Protection, OJK Regulation No. 44 of 2024 on Bank Secrecy, Law No. 1 of 2024 in conjunction with Law No. 11 of 2008 on Electronic Information and Transactions, among others. The study explores the extent of bank obligations, customers' legal remedies in the event of data breaches, and institutional accountability. Field data were collected through interviews and case analysis involving banking practices and third-party collaborations. The findings indicate that while the regulatory framework provides a solid foundation, gaps remain in enforcement and monitoring mechanisms, especially in third-party partnerships. The study emphasizes the need for stricter regulatory implementation, enhanced legal literacy among customers regarding their data privacy rights, and improved institutional oversight to ensure more effective protection of personal data in the digital banking landscape.

Keywords:
Personal Data Protection, Legal Liability, Third-Party Misuse, Banking Regulation, Digital Privacy

Introduction

In the current era of rapid digitalization, advancements in information technology have profoundly impacted various facets of human life. The influence of digital transformation extends beyond communication, education, and commerce, reaching into the financial services sector, including the banking industry. Banking plays a critical role in economic development. As technological advancements accelerate, they have driven banks toward continual innovation, enabling the provision of faster, more efficient, and more accessible services as part of this digital transformation. However, alongside the convenience and efficiency brought by these advancements, new challenges have emerged, particularly regarding the protection of customers' personal data. Personal data refers to any information about an identifiable individual, either directly or indirectly, through electronic or non-electronic systems, as defined in Article 1(1) of Law No. 27 of 2022 on Personal Data Protection ("PDP Law").

Such personal data is highly vulnerable to misuse if not managed with utmost care and responsibility. In this context, banks serve not only as financial service providers but also as data controllers, bearing both legal and ethical obligations to safeguard the confidentiality and integrity of customer data. This responsibility is underscored by regulatory provisions, including Article 1(11) of OJK Regulation No. 44 of 2024 concerning Bank Secrecy ("Bank

Secrecy Regulation"), which defines bank secrecy as information related to depositors and their deposits, as well as investors and their investments. Further, Article 2 of the regulation mandates that banks and affiliated parties must maintain the confidentiality of depositor and investor information. These provisions clearly establish the duty of banks and affiliated entities to uphold the confidentiality of customer data, making legal accountability a central issue when personal data breaches occur, especially as public trust in financial institutions is increasingly at stake. Negligent or irresponsible handling of personal data heightens the risk of exploitation by malicious actors. This vulnerability is reflected in the growing number of cases involving digital fraud, account breaches, and the illicit use of personal data for unlawful activities. Such incidents result in significant financial and non-financial losses for affected individuals and diminish customer trust in the banking system. Despite advancements in data security technologies, weaknesses in data protection systems—along with potential involvement from both internal and external parties—continue to present serious risks. These vulnerabilities often culminate in legal action against banks, which are held accountable as data controllers.

In the legal context, a distinction exists between *das sollen* (what ought to be) and *das sein* (what is). Normatively, the protection of personal data is regulated by the Personal Data Protection Law (PDP Law), and, in line with this study, the protection of customer data is also governed by the provisions of Law No. 10 of 1998 on the Amendment to Law No. 7 of 1992 concerning Banking ("Banking Law"). The PDP Law serves as the legal foundation for personal data protection in Indonesia, aiming to safeguard citizens' personal data and to ensure lawful, ethical, and principle-based data processing. However, its implementation and effectiveness, particularly in the context of financial service providers and third parties, remain a significant challenge. In practice, discrepancies persist between the normative provisions and their application. This is evident in the widespread misuse of personal data by irresponsible actors, revealing a substantial gap between the legal obligation to protect personal data and the existing reality. Frequently, banks deny liability by asserting that data breaches occur outside their systems—even when such data originate from within the bank or are leaked by bank employees.

Previous studies provide relevant insights. Sudjana (Faculty of Law, Universitas Padjadjaran), in his article titled "The Disclosure of Banking Secrets as a Violation of Customer Privacy and Electronic Personal Data Rights," examined bank liability in a data breach case based on Decision No. 57/PDT/2012/PT.Sby. His analysis incorporates strict liability, vicarious liability, and presumption of liability, concluding that internal perpetrators still render the bank liable. However, the study is limited by insufficient regulatory references—particularly the exclusion of the PDP Law—and lacks empirical depth. Further, Ferdinan Tambing et al., in "Customer Data Security in Banks and the Protection Role of the Financial Services Authority (OJK)" (Jurnal Sultra Research of Law, 2023), emphasize the importance of OJK's supervisory role and banks' compliance. Nonetheless, the study is predominantly normative-descriptive and lacks detailed analysis of specific legal liabilities or civil remedies. Another study by Vicky Katiandagho, Diana D. Putong, and Isye Junita Melo, titled "The Personal Data Protection Law Strengthens the Banking Law in Protecting Customer Confidentiality" (Jurnal Hukum To-ra, 2023), discusses the illicit trade of personal data by bank insiders and weak regulatory enforcement. However, this work is largely narrative and lacks structured analysis of institutional or civil bank liability.

The frequent misuse of personal data by third parties in the financial services sector—particularly by commercial banks—has become a major public concern. Although legal frameworks for personal data protection exist, enforcement remains inadequate, compounded by low public awareness regarding the importance of data privacy. When third parties, with access to banking systems, commit data violations, critical questions arise regarding the bank's liability for data protection negligence and the legal remedies available to affected customers. In light of Indonesia's positive law and the enactment of the PDP Law, which affirms data subjects' rights and controllers' obligations, these issues gain further relevance. This article seeks to offer a novel contribution by focusing specifically on Indonesia's largest private bank, Bank Central Asia (BCA). It examines BCA's legal liability when customer data is misused by third parties, and outlines the legal avenues available to affected individuals. The study centers on two research questions: (1) what recourse is available to customers whose data has been misused by third parties, and (2) what is BCA's legal responsibility in such cases. The aim is to analyze these issues while

contributing to the broader discourse on personal data protection, banking law, and digital financial regulation. The research is geographically focused on Batam City, Riau Islands, Indonesia, particularly based on data from BCA in Jodoh, Batam.

Research Methods

This study employs an empirical legal research approach to assess the legal responsibility of BCA in protecting customer personal data in cases of misuse by third parties. The research combines primary and secondary data with legal materials to provide a comprehensive analysis. Primary data are collected through interviews with Bank BCA's legal officers, data protection specialists, and compliance staff, as well as surveys from customers who have experienced data misuse. These data offer firsthand insights into how the bank handles data protection and addresses third-party misuse. Secondary data are obtained from a review of academic literature, including journal articles, books, and previous research on data protection laws and banking regulations. These sources contextualize the study within broader legal and regulatory frameworks. For legal analysis, primary legal materials such as Law No. 27 of 2022 on Personal Data Protection, OJK Regulation No. 44/POJK.03/2015 on Bank Secrecy, and Law No. 11/2008 on Electronic Information and Transactions are examined. Secondary legal materials include scholarly analyses and case law related to data misuse and bank liability. Tertiary legal materials, such as legal dictionaries and encyclopedias, provide clarification of legal terms. The research uses descriptive analysis to understand the implementation of data protection laws and identify gaps between regulatory frameworks and actual practices. This approach aims to evaluate Bank BCA's responsibility and effectiveness in safeguarding customer data and preventing third-party misuse.

Results and Discussion

The Legal Responsibility of Bank Central Asia Regarding Customer Personal Data Protection in Batam City

In today's digital era, the protection of customers' personal data has become a critical concern within the banking industry. The misuse of personal data by third parties can result in significant financial losses for customers and inflict severe reputational damage on banks. As institutions that manage and store sensitive customer information, banks bear a substantial responsibility and legal obligation to ensure that personal data remains secure and protected from threats and unauthorized access. Safeguarding this information is essential not only for maintaining operational integrity but also for preserving customer trust and the institution's credibility. Unfortunately, these ideals are increasingly contradicted by the rising incidence of data breaches and personal data misuse involving third parties.

Indonesia has established a regulatory framework for personal data protection, including the Personal Data Protection Law (UU PDP), along with other relevant legislation such as Law No. 1 of 2024 in conjunction with Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), and the Financial Services Authority Regulation on Bank Secrecy (POJK Rahasia Bank). These regulations provide a legal foundation for banks to safeguard customer data and delineate their responsibilities in upholding data privacy. In particular, commercial banks such as BCA are legally obligated to maintain the confidentiality of customer data as stipulated in Article 40 of the Banking Law. This duty is a core principle of banking operations, requiring banks to protect any information received from customers and to prevent unauthorized disclosures.

Data misuse by third parties frequently occurs through tactics such as phishing, carding, and data theft. These actors may exploit system vulnerabilities or take advantage of customer negligence. Such incidents have become increasingly prevalent, posing a tangible threat to customers and severely undermining the credibility of financial institutions. The escalation of these cases can be attributed to both weaknesses in banks' cybersecurity systems and the growing sophistication of fraud techniques in line with technological advancements. This troubling trend highlights a significant gap in data protection frameworks and underscores the urgent need to enhance data security systems and cyber defense mechanisms across the banking sector.

In cases of personal data misuse by third parties, the bank, as the data controller, must bear legal responsibility. It is incumbent upon the bank to identify the root causes of the data breach and to undertake remediation efforts for affected customers. This process includes an audit of the bank's information technology systems, which serves to evaluate and verify whether the system operates effectively, securely, and in accordance with prevailing regulations. Furthermore, a comprehensive review of the bank's collaboration protocols with third-party service providers is essential. Legal accountability may encompass compensation for affected customers as well as necessary revisions to existing data protection policies. Additionally, the bank is obliged to report any incidents of data breaches to the relevant regulatory authorities, namely the Financial Services Authority (OJK) and the Ministry of Communication and Informatics (Kominfo), as stipulated by applicable law.

Bank Central Asia (BCA) has implemented various measures to prevent the misuse of personal data, including deploying multi-layered security systems, conducting regular security audits, and educating customers about the importance of safeguarding personal information. The bank also cooperates with trusted third parties and operates a robust monitoring system to minimize the risk of data breaches. However, in evaluating the adequacy of the bank's protective efforts, it is relevant to apply the Legal Protection Theory proposed by Philipus M. Hadjon. According to Hadjon, legal protection comprises legal instruments and mechanisms designed to recognize and uphold the rights of the public. He posits that legal protection pertains to the respect for human dignity and the recognition of human rights as legal subjects under statutory law. Legal protection can be classified into two types: preventive and repressive.

Preventive legal protection refers to measures aimed at preventing disputes and problems before they arise. In the context of banking, this includes the obligation to implement data leakage prevention policies and to conduct regular audits to avert data breaches, thereby reducing the risk of significant harm to both customers and the bank's reputation. Conversely, repressive legal protection is designed to resolve disputes that have already occurred. This includes the recovery of compromised data, ensuring justice for affected customers, and resolving disputes through litigation, whether criminal or civil.

While BCA has made commendable efforts to safeguard personal data, there remains room for improvement. Enhancing data security policies, strengthening oversight mechanisms over third-party partners, and increasing legal awareness among customers are necessary steps forward. Moreover, more stringent enforcement against third-party data misuse is essential to fostering a safer banking environment and protecting customers' privacy rights. In this regard, banks must not only employ preventive legal protection but also offer repressive remedies for customers who fall victim to third-party data misuse. These efforts are vital not only for bolstering public trust in the banking system but also as a concrete expression of the bank's legal responsibility to society.

Availability Legal Remedies to Customers Victimized by Third-Party Data Misuse

The misuse of personal data by third parties has become an increasingly prevalent issue, particularly in the current digital era. Within the banking sector, customers who fall victim to such misuse—such as identity theft, fraud, and unauthorized transactions—can suffer significant financial and psychological harm. These incidents often stem from data breaches caused either by the negligence of banking institutions or by customers' own lapses in safeguarding their personal and privacy-related data. Such data, when exploited by irresponsible third parties, may be used for unauthorized and self-serving purposes. Accordingly, it is crucial to understand the legal remedies available to affected individuals to ensure they receive adequate and equitable legal protection in accordance with prevailing regulations.

In Indonesia, the protection of personal data is governed by various legal instruments, most notably the Personal Data Protection Act (UU PDP). This law outlines the rights of individuals over their personal data and the obligations of legal entities, including banks, to safeguard such data. When misuse occurs, customers are entitled to seek accountability and report such incidents to the relevant authorities, as stipulated in Article 12 of the PDP Act. Moreover, Articles 36 and 37 of the PDP Act explicitly mandate banks to protect, supervise, and maintain the confidentiality of their customers' data. The obligation of banks to uphold data confidentiality is further reinforced in

the Financial Services Authority Regulation (POJK) on Bank Secrecy, particularly Article 1(11) and Article 2, which emphasize the duty of banks to preserve the confidentiality of all customer data and personal information.

Customers affected by third-party data misuse have several legal avenues available. The initial step is to report the incident to their bank, requesting clarification and remedial measures. Subsequently, the matter may be escalated to the relevant authorities, such as the police or the Financial Services Authority (OJK), for further investigation. In certain circumstances, customers may also pursue civil litigation against the responsible third parties for damages incurred. For instance, Bank Central Asia (BCA) affirms that in cases of third-party data misuse, affected customers may lodge complaints through the Halo BCA service or submit written complaints at the nearest branch office. Should the complaint be substantiated, civil lawsuits seeking compensation for both material and immaterial damages are permitted.

As institutions entrusted with storing clients' personal data, banks bear a substantial responsibility to ensure the confidentiality and security of such information. Based on an interview with representatives from Bank Central Asia (BCA), the bank has implemented a comprehensive set of policies and procedures to protect customers' personal data from unauthorized access or misuse by third parties. These measures include a strict privacy policy prohibiting the disclosure of customer data without written consent, access management systems limiting data access to authorized personnel, authentication and encryption technologies to detect potential abuses, and supervisory protocols that require any third-party partnership to be governed by a binding agreement. These contracts explicitly forbid the duplication of personal data without authorization and impose obligations on the third party to uphold data privacy standards.

In the event of data misuse, the bank is obligated to promptly initiate an investigation, support affected customers, and enhance any potentially vulnerable security systems. Banks are also required to provide complaint mechanisms and restitution procedures for customers who suffer financial harm due to data breaches. If third-party data misuse constitutes a criminal act, such as identity theft or fraud, affected individuals have the right to report the incident to law enforcement for criminal prosecution. Indonesia's Electronic Information and Transactions Law (UU ITE), as amended by Law No. 19 of 2016, provides the legal framework for prosecuting electronic data misuse. In addition to pursuing criminal charges, customers may file civil lawsuits against the third parties involved, or against the bank itself if negligence in safeguarding personal data can be established.

BCA, in this context, offers indirect legal support by taking responsibility for investigating, resolving, and providing redress for incidents that fall within its operational domain—particularly those involving third-party partners acting on its behalf. The legal system empowers customers to seek financial compensation for damages resulting from data breaches, and banks may be held accountable if they fail to meet their data protection obligations. To mitigate the risks of personal data misuse, it is essential for customers to exercise caution when sharing personal information and to prioritize secure digital transaction practices. Additionally, public awareness regarding legal rights over personal data must be strengthened.

Collaborative efforts between the public, financial institutions, and government authorities are crucial for reinforcing data protection regulations and oversight mechanisms. Only through such cooperation can a secure and accountable data protection environment be achieved. With appropriate legal measures in place, customers can assert their rights and seek justice in the face of personal data misuse.

Conclusions

With the advancement of technology, the protection of customers' personal data has become a crucial obligation for banks, which act as data controllers. This necessity arises due to the ease with which personal data can now be accessed by third parties through technological means, often resulting in criminal misuse. In Indonesia, personal data protection is regulated by several legal instruments, including the Personal Data Protection Law (UU PDP), the Banking Law, the Financial Services Authority Regulation on Bank Secrecy (POJK Rahasia Bank), and the Electronic Information and Transactions Law (UU ITE). These laws provide a legal foundation for banks to safeguard customer data and stipulate their obligations in this regard. Despite existing regulations, cases of personal

data misuse remain prevalent. Consequently, banks, as data controllers, are legally responsible for fulfilling their obligations to protect customer data. Based on findings from interviews with Bank Central Asia (BCA) as the research object, the bank has implemented both preventive and repressive legal protection measures. However, significant vulnerabilities remain, especially regarding third-party involvement, which could lead to data breaches or misuse.

To address this, BCA must strengthen its preventive legal safeguards by reinforcing policies concerning data breaches, conducting regular information system audits, monitoring third-party activities, and providing digital literacy education to customers. On the other hand, when a violation occurs, BCA is also obliged to implement repressive legal measures aimed at remedying customer losses and ensuring fair dispute resolution. Customers affected by third-party misuse of their personal data may suffer financial and psychological harm. They are entitled to hold the bank accountable and seek legal remedies, whether through criminal or civil litigation. As a data controller, BCA is responsible for investigating, resolving, and providing redress for incidents occurring within its scope of responsibility—especially those involving third-party partners acting on its behalf. Failure to fulfill these duties may result in BCA being held legally liable. Therefore, a collaborative effort among the government, banks, and the public is essential to reduce the risk of personal data misuse. Additionally, stronger legal regulations and rigorous enforcement are imperative to ensure that personal data protection aligns with the prevailing legal standards and effectively safeguards customer rights.

References

Rahmawati, I. N., Rahmadani, N., Heni, D. R., & Kevin, S. (2023). Pertanggung jawaban Pihak Bank terhadap Kebocoran Data Diri Nasabah. *Aufklarung: Jurnal Pendidikan, Sosial Dan Humaniora*, *3*(2), 208-215.

Hukumonline. (2019, Juni 17). *Bolehkah bank memberikan informasi data nasabah kepada asuransi?* Hukumonline.com.

Djafar, W., & Santoso, M. J. (2019). Perlindungan Data Pribadi. *Konsep, Instrumen, dan Prinsipnya, Lembaga Studi dan Advokasi Masyarakat (ELSAM), Jakarta*.

Yuniarti, S. (2019). Perlindungan hukum data pribadi di Indonesia. *Business Economic, Communication, and Social Sciences Journal (BECOSS)*, *1*(1), 147-154.

Sudjana, S. (2022). Pembocoran Rahasia Bank Sebagai Pelanggaran Hak Privasi Dan Data Pribadi Elektronik Nasabah Bank. *Refleksi Hukum: Jurnal Ilmu Hukum*, *6*(2), 247-266.

Ferdinan Tambing, M. Yusuf, Agus, Muhammad Fitriadi, & Muh. Nadzirin Anshari Nur. (2023). Keamanan Data Nasabah di Bank dan Perlindungan Otoritas Jasa Keuangan . *Sultra Research of Law*, *5*(1), 32-42.

Katiandagho, V., Putong, D. D., & Melo, I. J. (2023). Undang–Undang Perlindungan Data Pribadi Memperkuat Undang–Undang Perbankan Dalam Menjaga Rahasia Data Nasabah Dan Untuk Melindungi Data Pribadi Masyarakat Indonesia. Jurnal Hukum to-ra: Hukum Untuk Mengatur dan Melindungi Masyarakat, 9(1), 106-114.

Telkom University. (n.d.). Audit sistem informasi: Pengertian dan proses pelaksanaannya.

Marpaung, J. E. (n.d.). *Tinjauan Yuridis Terhadap Perlindungan Hukum Bagi Nasabah Bank dalam Menjaga Kerahasiaan Data Pribadi Nasabah*. Universitas Medan Area.

Bediona, K., Herliansyah, M. R. F., Nurjaman, R. H., & Syarifuddin, D. (2024). Analisis Teori Perlindungan Hukum Menurut Philipus M Hadjon Dalam Kaitannya Dengan Pemberian Hukuman Kebiri Terhadap Pelaku Kejahatan Seksual. *Das Sollen: Jurnal Kajian Kontemporer Hukum Dan Masyarakat*, *2*(01).

Fakultas Hukum Universitas Pattimura. (n.d.). *Bab II Tinjauan Pustaka: A. Tinjauan tentang perlindungan hukum*. OPAC Fakultas Hukum Universitas Pattimura.

Zennia, A., & Imanullah, D. M. N. (2021). Perlindungan Hukum Preventif Dan Represif Bagi Pengguna Uang Elektronik Dalam Melakukan Transaksi Tol Nontunai. *Privat Law*, *9*, 218-226.

Tanumulia, R., Astutik, S., & Widodo, E. (2024). PERLINDUNGAN HUKUM TERHADAP KERAHASIAN DATA PRIBADI NASABAH DI ERA DIGITALISASI PERBANKAN. *Jurnal Penelitian Multidisiplin Terpadu*, *8*(11).

Maramis, A. V. (2025). TINJAUAN YURIDIS TERHADAP PERLINDUNGAN DATA PRIBADI DALAM MENGATASI CYBERCRIME PADA KASUS PHISHING. *LEX PRIVATUM*, *14*(5).

Sutrisna, C. (2021). Aspek Hukum Perlindungan Data Pribadi dan Kondisi Darurat Kebocoran atas Data Pribadi di Indonesia. *Wacana Paramarta: Jurnal Ilmu Hukum*, *20*(5), 1-10.

mardiana Parihin, N. (2023). Urgensi Perlindungan Data Pribadi Dalam Perpektif Hak Asasi Manusia. *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia*, *5*(1), 16-23.

Kitab Undang Undang Hukum Perdata;

POJK No. 44 Tahun 2024 Tentang Rahasia Bank;

UU No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi;

UU No. 10 Tahun 1998 Tentang Perubahan Atas Undang Undang No. 7 Tahun 1992 tentang Perbankan;

Naskah Akademik UU PDP;

Undang-Undang No. 1 Tahun 2024 jo. Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.