

DOI: 10.46924/jihk.v8i1.437

Limitations on the Use of Emergency Contact Data in Fintech Lending under the Personal Data Protection Act

Mochammad Zainuril Huda[1*], Krista Yitawati[2], & Meirza Aulia Chairani[3]

[1,2,3]Universitas Merdeka Madiun, Indonesia

Correspondence

Mochammad Zainuril Huda, Universitas Merdeka Madiun, Indonesia Jl. Serayu No.79, Pandean, Kec. Taman, Kota Madiun, Jawa Timur 63133, *e*-mail: nurilh45@gmail.com

How to cite

Huda, Mochammad Zainuril., Yitawati, Krista., & Chairani, Meirza Aulia. 2026. Limitations on the Use of Emergency Contact Data in Fintech Lending under the Personal Data Protection Act. *Jurnal Ilmu Hukum Kyadiren* 8(1), 141-157. https://doi.org/10.46924/jihk.v8i1.437

Original Article

Abstract

This study is motivated by the increasing misuse of emergency contact data in the debt collection practices of fintech lending services, which may infringe upon personal data protection rights. Although Law Number 27 of 2022 on Personal Data Protection (PDP Law) provides a legal framework for the management and protection of personal data, its implementation in the fintech sector continues to face several challenges. This study aims to analyze the legal provisions governing the use and limitation of access to emergency contact data and to identify the challenges associated with enforcing laws against such misuse. The research employs a normative legal research method with statutory and conceptual approaches, relying on the analysis of legislation, academic literature, and relevant legal documents. The findings indicate that the PDP Law establishes key principles, including consent, purpose limitation in data processing, and the responsibilities of data controllers. However, instances of misuse persist due to weak regulatory oversight, limited institutional coordination, and low levels of public legal awareness. Therefore, strengthening supervisory mechanisms and enhancing the integration of law enforcement institutions are essential to improving personal data protection within the fintech lending ecosystem.

Keywords: *Personal Data Protection, Fintech Lending, Emergency Contacts, Law Enforcement*

Abstrak

Penelitian ini dilatarbelakangi oleh meningkatnya penyalahgunaan data kontak darurat dalam proses penagihan pinjaman pada layanan fintech lending yang berpotensi melanggar hak perlindungan data pribadi. Meskipun Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) telah memberikan kerangka hukum bagi pengelolaan dan perlindungan data pribadi, implementasinya dalam sektor fintech masih menghadapi berbagai tantangan. Penelitian ini bertujuan menganalisis pengaturan hukum terkait penggunaan dan pembatasan akses terhadap data kontak darurat serta mengidentifikasi tantangan dalam penegakan hukum terhadap penyalahgunaannya. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan dan konseptual melalui analisis terhadap regulasi, literatur ilmiah, serta dokumen terkait. Hasil penelitian menunjukkan bahwa UU PDP telah mengatur prinsip persetujuan, pembatasan tujuan pemrosesan data, dan tanggung jawab pengendali data, namun penyalahgunaan masih terjadi akibat lemahnya pengawasan, koordinasi kelembagaan, dan rendahnya kesadaran hukum masyarakat. Oleh karena itu, penguatan pengawasan dan integrasi penegakan hukum menjadi penting untuk meningkatkan perlindungan data pribadi dalam ekosistem fintech lending.

Kata kunci: *Perlindungan Data Pribadi, Fintech Lending, Kontak Darurat, Penegakan Hukum*

1. INTRODUCTION

The rapid development of digital technology has significantly transformed various sectors, including the financial services industry. One of the most notable innovations in recent years is financial technology (fintech), particularly fintech lending or peer-to-peer (P2P) lending services. Fintech lending refers to information technology–based financial services that connect lenders and borrowers through digital platforms without directly involving conventional financial institutions. This service model offers several advantages, including faster loan application processes, broader access to financing, and relatively simple procedures. Consequently, fintech lending has been widely recognized as a mechanism for improving financial inclusion, particularly among communities that remain underserved by formal banking institutions.

In Indonesia, the growth of fintech lending has been remarkably rapid, driven by increasing internet penetration and the widespread use of digital devices. Online lending services have become an alternative source of financing for many individuals seeking to meet both consumptive and productive needs. In response to this development, the government, through the Financial Services Authority, has introduced regulatory and supervisory frameworks to ensure that fintech lending activities operate in accordance with the principles of prudence, transparency, and consumer protection. These efforts are reflected in various regulatory instruments governing the implementation of information technology–based lending services.

Despite the convenience and accessibility offered by fintech lending, its expansion has also generated a number of complex legal issues. One of the most prominent concerns relates to the misuse of personal data belonging to users of online lending services. In practice, fintech lending providers commonly request access to a wide range of personal data as part of the verification and creditworthiness assessment process. The data collected typically includes not only basic identity information but also additional data such as contact lists, location data, photographs, and other forms of digital activity.

The extensive collection of such data raises significant concerns regarding the security and confidentiality of users' personal information. In many instances, data obtained by fintech platforms is not solely used for verification purposes but may also be exploited during the debt collection process. One of the most frequently reported practices involves the misuse of emergency contact information by debt collectors in online loan collection activities. In principle, emergency contact information constitutes third-party data provided by borrowers solely for communication purposes under specific circumstances, such as when the borrower cannot be reached. However, in practice, this information is often used as a means of exerting pressure during the debt collection process.

Various reports indicate that debt collectors sometimes contact third parties listed as emergency contacts—such as family members, friends, or coworkers—to inform them about the borrower's outstanding debt obligations. In certain cases, these communications are accompanied by intimidation, threats, or the dissemination of the borrower's personal information to other parties. Such practices not only violate ethical standards in debt collection but may also infringe upon individual privacy rights and the fundamental principles of personal data protection.

These developments indicate that personal data management practices within fintech lending services continue to face significant regulatory and compliance challenges. The misuse of emergency contact data reflects a gap between existing practices and the principles of personal data protection that digital service providers are expected to uphold. From a legal perspective, the processing and use of personal data must be based on valid consent from the data subject and must be limited to the purposes for which the data were originally collected. The use of personal data beyond these purposes without explicit consent may constitute a violation of the data subject's right to privacy.

In order to strengthen legal protection for citizens' personal data, the Indonesian government enacted Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). This legislation represents a significant milestone in Indonesia's legal framework, as it provides, for the first time, a comprehensive regulatory regime governing the processing of personal data. The Personal Data Protection Law establishes several fundamental principles for personal data governance, including the principles of consent, purpose limitation, data accuracy, data security, and accountability of data controllers.

Platform providers essentially function as personal data controllers and are therefore legally obligated to ensure that all processes involving the collection, storage, and use of personal data are carried out lawfully, transparently, and responsibly. Emergency contact information provided by borrowers may only be used for specific purposes that have been previously agreed upon and must not be employed as a tool of pressure or intimidation in the debt collection process. Consequently, the use of such data beyond the original purpose of its collection may constitute a violation of the principle of purpose limitation as stipulated in the Personal Data Protection Law.

Nevertheless, despite the strengthening of the regulatory framework on personal data protection through the enactment of the Personal Data Protection Law, various cases of personal data misuse in the fintech sector continue to occur. One notable case occurred in 2023 when the Jakarta Metropolitan Police arrested two suspects involved in the distribution of personal data belonging to online loan customers. The perpetrators threatened victims by disseminating personal information, including identity photographs and personal images obtained from social media platforms. For

these actions, the suspects were charged under several provisions of the Electronic Information and Transactions Law and the Trade Law, both of which provide for significant criminal penalties.

This case illustrates that the problem of personal data misuse in fintech lending services is not merely a matter of regulatory adequacy but also relates to the effectiveness of oversight and law enforcement. In many instances, personal data breaches occur due to weak compliance by service providers with established data protection principles and the limited supervisory capacity of relevant institutions. Furthermore, the complexity of the fintech ecosystem, which involves multiple actors—such as platform operators, debt collection agencies, and other third parties—further complicates the enforcement of legal accountability.

The development of financial technology lending (fintech lending) in Indonesia has significantly transformed the digital financial services landscape. Technology-based lending platforms facilitate fast and efficient financing processes between lenders and borrowers without requiring face-to-face interaction. This accessibility has contributed to increasing financial inclusion, particularly for individuals who previously faced difficulties obtaining credit from conventional financial institutions. However, alongside these benefits, a number of legal challenges have emerged, particularly concerning the protection of personal data belonging to fintech lending service users.

Several previous studies have identified that the primary issues in online lending services relate to the collection, processing, and dissemination of personal data by platform providers and third parties acting as debt collectors. Research conducted by Novinna examined the legal status of debt collectors in fintech lending and the legal consequences of unlawful collection practices. The findings indicate that debt collectors frequently employ coercive collection methods, including the disclosure of consumers' personal data to third parties as a means of pressuring debtors to fulfill their repayment obligations. Such practices are considered inconsistent with the principles of consumer protection and may give rise to legal liability for fintech service providers.[1]

Similarly, research conducted by Johan highlighted debt collection practices undertaken by fintech companies through the dissemination of debtors' personal information to contacts stored on users' mobile devices. The study concluded that the collection and dissemination of personal data without valid consent constitute violations of individuals' privacy rights and the personal domain of data subjects. Accordingly, the study emphasizes the necessity of establishing specific regulatory

[1] Veronica Novinna, "Perlindungan Konsumen Dari Penyebarluasan Data Pribadi Oleh Pihak Ketiga: Kasus Fintech Peer To Peer Lending," *Jurnal Magister Hukum Udayana* 9, no. 1 (2020): 92–110, https://doi.org/10.24843/JMHU.2020.v09.i01.p07.

frameworks governing personal data protection in electronic transactions, particularly within the context of online lending services.[2]

Subsequent studies on personal data protection in the fintech sector have continued to evolve in parallel with the development of new regulatory frameworks in Indonesia. Research conducted by Noptabi et al. analyzed the legal protection of fintech lending consumers' personal data based on the Consumer Protection Law and regulations issued by the Financial Services Authority. The study found that legal protection for personal data had been regulated through various sectoral instruments, including regulations issued by the Financial Services Authority and the Ministry of Communication and Informatics. However, at the time the study was conducted, Indonesia did not yet have a comprehensive law specifically governing personal data protection. As a result, law enforcement mechanisms were largely limited to administrative sanctions.[3]

Following the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), a growing body of research has begun to examine the implications of this regulation for personal data protection within the fintech ecosystem. Research conducted by Pane and Kansil affirms that personal data protection constitutes an integral part of the right to privacy guaranteed by the constitution. The study further indicates that many cases involving online loan collection practices include threats to disclose debtors' personal data, thereby highlighting the urgent need for effective dispute resolution mechanisms to ensure legal protection for victims of personal data breaches.[4]

Furthermore, research by Angeline and Dwijayanthi analyzes the protection of personal data belonging to fintech lending consumers within the framework of Indonesian positive law. The study confirms that fintech providers function as personal data controllers and are therefore required to obtain consent from data subjects prior to processing their personal data. In addition, service providers are obligated to ensure the security and confidentiality of consumers' personal information. In cases of data breaches, data subjects are entitled to pursue legal remedies through administrative, civil, and criminal mechanisms.[5]

---

2 Suwinto Johan, "Financial Technology Company's Debt Collection Method: A Legal Aspect," *Unnes Law Journal* 8, no. 1 (2022): 1–20, https://doi.org/10.15294/ulj.v7i1.52173.

3 Iim Saputra Noptabi, Serlika Aprita, and Mona Wulandari, "Legal Protection of Personal Data Financial Technology Based Online Loans from The Consumer Protection Act," *Walisongo Law Review* 4, no. 1 (2022): 121–134, https://doi.org/10.21580/walrev.2022.4.1.11135.

4 Ian Dharsono Wijaya Pane and Christine S.T. Kansil, "Penyelesaian Sengketa Terhadap Dugaan Penyalahgunaan Data Pribadi Dalam Layanan Fintech," *Syntax Literate: Jurnal Ilmiah Indonesia* 7, no. 11 (2011): 17174–87, https://doi.org/10.36418/syntax-literate.v7i11.12021.

5 Priskila Angeline and Putri Triari Dwijayanthi, "Perlindungan Data Pribadi Bagi Penerima Dana Fintech Lending Dalam Perspektif Hukum Positif Indonesia," *Kertha Semaya: Journal Ilmu Hukum* 11, no. 12 (2023): 2996–3007, https://doi.org/10.24843/KS.2023.v11.i12.p19.

Another study conducted by Rahmawati et al. identified various forms of personal data misuse committed by fintech lending operators. These violations include unauthorized data processing, unlawful disclosure of personal data, and the use of malicious software to access users' personal information. The study concludes that such violations may be subject to criminal sanctions under the Personal Data Protection Law; however, the effectiveness of enforcement remains highly dependent on the strength of supervisory mechanisms.[6]

An evaluation of regulatory effectiveness was also undertaken by Rifa and Hidayati, who assessed the effectiveness of penal policies in protecting the personal data of fintech lending customers. The findings indicate that although regulatory instruments—such as the Personal Data Protection Law, the Electronic Information and Transactions Law, and regulations issued by the Financial Services Authority (OJK)—provide a relatively comprehensive legal framework, their implementation continues to face significant challenges, particularly in relation to oversight mechanisms and the enforcement of sanctions for personal data violations.[7]

In addition, research conducted by Andayani highlights the role of the Financial Services Authority (OJK) in supervising fintech lending operators. The study finds that although regulatory frameworks impose obligations related to personal data protection, the implementation of supervisory mechanisms over fintech platforms remains suboptimal. This condition is attributed to several factors, including limited institutional resources, the large number of illegal fintech platforms, and low levels of public digital literacy regarding the risks associated with personal data misuse.[8]

From a broader perspective, research by Darnela and Rusdiana introduces a normative–empirical approach by examining the level of public legal awareness regarding personal data protection. The study identifies the existence of a privacy paradox, a condition in which individuals are aware of the risks associated with personal data misuse but nevertheless continue to grant data access to digital applications. This finding suggests that effective personal data protection depends not only on regulatory frameworks but also on the level of public legal awareness and digital literacy.[9]

Meanwhile, research by Lasmana et al. investigates personal data protection within the billing process of PayLater services, which form part of the broader fintech lending

---

6 Elvia Rahmawati, Miftakhul Huda, and Ian Firstian Aldhi, "Personal Data Misuse in Fintech Lending Providers from Perspective Indonesian Cyberlaw," *Airlangga Development Journal* 8, no. 1 (2024): 8–20, https://doi.org/10.20473/adj.v8i1.56398.

7 Fauzi Rifa and Maslihati Nur Hidayati, "Kebijakan Penal Dalam Perlindungan Data Pribadi Nasabah Fintech Lending Di Indonesia," *Binamulia Hukum* 13, no. 2 (2024): 461–481, https://doi.org/10.37893/jbh.v13i2.964.

8 Komang Dian Andayani, "Analisis Yuridis Terhadap Pengaturan Perlindungan Data Pribadi Dalam Layanan Fintech Peer-To-Peer Lending," *Aliansi: Jurnal Hukum, Pendidikan Dan Sosial Humaniora* 2, no. 5 (2025): 110–121, https://doi.org/10.62383/aliansi.v2i5.1208.

9 Lindra Darnela and Erma Rusdiana, "Public Legal Awareness and the Effectiveness of Indonesia's Personal Data Protection Law: Bridging Normative Framework and Privacy Paradox," *Supremasi Hukum: Jurnal Kajian Ilmu Hukum* 14, no. 1 (2025): 1–28, https://doi.org/10.14421/2gg2rp29.

ecosystem. The study confirms that billing procedures are regulated through Financial Services Authority (OJK) regulations that emphasize ethical collection practices. However, in practice, instances of unprofessional billing behavior continue to occur, including the misuse of personal data as a means of intimidating service users.[10]

Additionally, Syahputra and Fibrianti examine personal data protection in the context of illegal fintech lending operations. Their research indicates that although various regulations governing personal data protection have been established, the current supervisory framework remains fragmented and sectoral, lacking effective institutional integration. Consequently, the study recommends the establishment of an independent personal data protection supervisory authority with clearly defined powers and responsibilities.[11]

Previous studies have generally focused on the regulatory framework governing personal data protection, the role of supervisory institutions, and various forms of data misuse within fintech lending services. However, research specifically examining the misuse of emergency contact data in debt collection practices conducted by debt collectors, as well as the implementation of the purpose limitation principle under the Personal Data Protection Law, remains relatively limited. Accordingly, this study offers a novel contribution by analyzing the legal framework and law enforcement challenges associated with the use and restriction of access to emergency contact data within the fintech lending ecosystem. Based on this background, this study aims to:

1) analyze the legal framework governing the use and limitation of access to emergency contact data in fintech lending services based on the provisions of Law Number 27 of 2022 concerning Personal Data Protection and other relevant regulations in the financial services sector; and
2) identify the challenges in law enforcement related to the misuse of emergency contact data in online loan collection practices, including regulatory aspects, oversight by relevant authorities, and the effectiveness of sanction mechanisms.

2. RESEARCH METHODOLOGY

This study employs a normative legal research method to analyze legal norms related to personal data protection in financial technology lending (fintech) services, particularly concerning the use and limitation of access to emergency contact data by platform operators and debt collectors during the online loan collection process. Normative legal research conceptualizes law as a system of norms that includes legal principles,

[10] Josephine Aprilia Lasmana et al., "Perlindungan Hukum Terhadap Data Pribadi Pengguna Dalam Proses Penagihan Oleh Penyelenggara Peer-to-Peer Lending Berbasis PayLater," *Begawan Abioso* 16, no. 2 (2025): 63–73, https://doi.org/10.37893/abioso.v16i2.1237.

[11] Bearlly Deo Syahputra and Nurul Fibrianti, "Independent Authority on Personal Data Protection in Illegal Financial Technology: Capturing Peer-to-Peer (P2P) Lending Issues," *Journal of Private and Commercial Law Section* 8, no. 1 (2024): 114–35, https://doi.org/10.15294/jpcl.v8i1.3967.

doctrines, and rules governing social behavior. Accordingly, this study focuses on examining positive legal provisions regulating personal data protection and assessing their relevance to debt collection practices in online lending services.

The research adopts several analytical approaches, namely the statutory approach, conceptual approach, and case study approach. The statutory approach is applied to examine various regulatory instruments related to personal data protection, particularly Law Number 27 of 2022 concerning Personal Data Protection, as well as other relevant regulations, including the Electronic Information and Transactions Law (ITE Law) and regulations issued by the Financial Services Authority (OJK) governing information technology–based lending services. The conceptual approach is used to analyze legal doctrines and theoretical concepts related to the right to privacy, principles of personal data protection, and the legal responsibilities of fintech operators as personal data controllers. Meanwhile, the case study approach is utilized to examine instances of personal data misuse in online lending services in order to evaluate the effectiveness of legal implementation in protecting data subjects.

3. RESEARCH RESULT AND DISCUSSION

3.1. Legal Regulations Governing the Use and Restriction of Access to Emergency Contact Data in Fintech Lending Services

This study aims to analyze the legal framework governing the use and limitations on access to emergency contact data in fintech lending services based on the provisions of Law Number 27 of 2022 concerning Personal Data Protection and other relevant regulations within the financial services sector. The analysis is conducted through a normative review of statutory regulations, legal doctrines, and secondary data, including consumer complaint reports and official documentation from supervisory institutions in the financial services sector. The primary focus of this study is to evaluate how the existing regulatory framework governs the processing of emergency contact data while also examining the extent to which applicable legal norms align with practices observed in online loan collection activities conducted by fintech lending providers.

The provisions of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) affirm that the use and processing of personal data, including emergency contact information, must adhere to the fundamental principles of personal data protection. Emergency contact information provided by borrowers during the loan application process on fintech platforms essentially constitutes personal data belonging to third parties who do not have a direct legal relationship with the loan agreement between the fintech provider and the borrower. Therefore, the processing of such data cannot be carried out arbitrarily by platform providers and must comply with the legal requirements stipulated under the Personal Data Protection Law.

The PDP Law explicitly provides that any processing of personal data must be based on the valid consent of the data subject and carried out for specific, explicit, and legitimate purposes. This provision reflects the principle of purpose limitation, which stipulates that personal data may only be processed for purposes that have been previously approved by the data subject. Within the context of fintech lending services, emergency contact information should generally be used solely for verification or communication purposes under particular circumstances, such as when the borrower cannot be contacted directly. The use of such data for other purposes—such as contacting third parties to pressure borrowers during debt collection—lacks a legal basis in the absence of explicit consent from the data subject.

In addition to regulating the principles governing data processing, the PDP Law also provides legal protection by recognizing the rights of personal data subjects. These rights include the right to obtain information regarding the processing of personal data, the right to correct inaccurate personal data, the right to withdraw consent for data processing, and the right to request the deletion of personal data. In the context of the use of emergency contact information in fintech lending services, these provisions imply that individuals whose information is listed as emergency contacts possess the legal right to know how their personal data were obtained, the purposes for which the data are used, and the right to object to such processing if it deviates from the original purpose of data collection.

Furthermore, the Personal Data Protection Law imposes obligations on data controllers and data processors to ensure the security and confidentiality of the personal data under their control. Fintech lending providers, as personal data controllers, are therefore required to ensure that personal data collected from service users—including emergency contact information—are adequately protected from unauthorized access, data breaches, or misuse by third parties. These obligations are reinforced through the imposition of administrative and criminal sanctions for parties who intentionally misuse personal data.

Article 20 paragraph (2) of the Personal Data Protection Law emphasizes that the processing of personal data must be based on the explicit and documented consent of the data subject. Moreover, Articles 67 and 68 of the PDP Law provide criminal sanctions for individuals or entities that unlawfully disclose or misuse personal data. These provisions establish a strong legal basis for prosecuting perpetrators of personal data misuse within fintech lending services, including cases in which platform operators or debt collectors unlawfully utilize emergency contact information during debt collection activities.

Regulations concerning personal data protection in the fintech sector are not limited to the Personal Data Protection Law (PDP Law) but are also reinforced by various sectoral regulations within the financial services industry. The Financial Services

Authority (OJK), as the primary supervisory body for the financial services sector, possesses the authority to regulate and oversee the operation of fintech lending services. In principle, regulations issued by OJK prohibit fintech providers from arbitrarily using the personal data of consumers or other parties and require the application of prudential principles in the management and protection of personal data.

However, an examination of consumer complaint reports and official documentation issued by OJK indicates that, in practice, violations of personal data protection principles continue to occur. Consumer complaint data suggest that the misuse of personal data—particularly the use of emergency contact information in debt collection practices—remains one of the most frequently reported violations within the fintech lending sector. In several cases, debt collectors have contacted individuals listed as emergency contacts through telephone calls, text messages, or instant messaging applications without the consent of the data subject.

Moreover, such collection practices often involve the disclosure of personal information regarding the borrower's debt status to third parties. These actions not only violate the principles of personal data protection but also potentially harm individuals who are not directly involved in the loan agreement. This situation illustrates a gap between the legal norms established in statutory regulations and their implementation in practice.

The findings of this study are consistent with previous research indicating that debt collection practices in fintech lending services frequently disregard the rights of personal data subjects. Several studies have demonstrated that debt collectors operating within fintech platforms often utilize contact data stored on users' devices as a means of exerting pressure on borrowers to repay their debts.[12] These practices indicate that personal data governance within the fintech ecosystem continues to face significant challenges, particularly regarding the level of compliance among service providers with personal data protection principles.

Compared with previous studies, this research confirms that although Indonesia's regulatory framework for personal data protection has undergone significant development following the enactment of the Personal Data Protection Law, its implementation within the fintech lending sector remains limited in effectiveness. Prior research has largely focused on regulatory aspects or the general normative framework for personal data protection.[13] In contrast, this study specifically examines the use of

---

[12] Andayani, "Analisis Yuridis Terhadap Pengaturan Perlindungan Data Pribadi Dalam Layanan Fintech Peer-To-Peer Lending"; Johan, "Financial Technology Company's Debt Collection Method: A Legal Aspect"; Lasmana et al., "Perlindungan Hukum Terhadap Data Pribadi Pengguna Dalam Proses Penagihan Oleh Penyelenggara Peer-to-Peer Lending Berbasis PayLater"; Novinna, "Perlindungan Konsumen Dari Penyebarluasan Data Pribadi Oleh Pihak Ketiga: Kasus Fintech Peer To Peer Lending"; Pane and Kansil, "Penyelesaian Sengketa Terhadap Dugaan Penyalahgunaan Data Pribadi Dalam Layanan Fintech."

[13] Angeline and Dwijayanthi, "Perlindungan Data Pribadi Bagi Penerima Dana Fintech Lending Dalam Perspektif Hukum Positif Indonesia"; Putu Eva Ditayani Antari and Ni Gusti Agung Ayu Mas Triwulandari, "Legal Protection of Consumer Personal Data Peer to Peer Lending Through Financial Technology in Indonesia: An

emergency contact data in online loan collection practices and analyzes its legal implications under the Personal Data Protection Law.

The misuse of emergency contact information is not solely related to regulatory shortcomings but is also influenced by several other factors, including low levels of compliance among fintech operators, weak supervisory mechanisms, and limited public legal awareness.[14] Many individuals whose information is listed as emergency contacts are unaware that their personal data are legally protected and that they possess the right to refuse or object to unauthorized data processing. Consequently, numerous cases of personal data misuse remain unreported or are not pursued through legal channels.

Furthermore, the effectiveness of law enforcement in addressing personal data violations is also influenced by institutional factors. Although the Personal Data Protection Law establishes various forms of sanctions for personal data breaches, its effective implementation requires the support of a strong supervisory authority as well as effective coordination among relevant institutions, including the Financial Services Authority (OJK), the Ministry of Communication and Informatics, and law enforcement agencies.

This study confirms that the Personal Data Protection Law (PDP Law) provides a strong legal foundation for regulating the use and restricting access to emergency contact data in fintech lending services. However, the effectiveness of this legal protection remains highly dependent on its implementation in practice, particularly with regard to the level of compliance among fintech service providers with personal data protection principles and the effectiveness of oversight conducted by relevant institutions.

Strengthening supervisory mechanisms, enhancing public legal awareness, and enforcing strict sanctions for personal data violations are therefore essential factors in ensuring that personal data protection in fintech lending services is effectively implemented. These measures are crucial to providing comprehensive legal protection

---

Approached of Comparative Study," *Jurnal Komunikasi Hukum* 10, no. 2 (2024): 93–115, https://doi.org/10.23887/jkh.v10i2.83167; Darnela and Rusdiana, "Public Legal Awareness and the Effectiveness of Indonesia's Personal Data Protection Law: Bridging Normative Framework and Privacy Paradox"; Noptabi, Aprita, and Wulandari, "Legal Protection of Personal Data Financial Technology Based Online Loans from The Consumer Protection Act"; Pane and Kansil, "Penyelesaian Sengketa Terhadap Dugaan Penyalahgunaan Data Pribadi Dalam Layanan Fintech"; Rifa and Hidayati, "Kebijakan Penal Dalam Perlindungan Data Pribadi Nasabah Fintech Lending Di Indonesia"; Syahputra and Fibrianti, "Independent Authority on Personal Data Protection in Illegal Financial Technology: Capturing Peer-to-Peer (P2P) Lending Issues."

14 Fitika Andraini et al., "Pendekatan Sosio-Yuridis Terhadap Bahaya Pinjaman Online Ilegal: Analisa Proram Edukasi Interaktif Untuk Mahasiswa," *Jurnal Ilmiah Galuh Justisi* 14, no. 1 (2026): 146–64, http://dx.doi.org/10.25157/justisi.v14i1.21961; Muhammad Irfan Maulana et al., "Kepastian Hukum Dan Perlindungan Konsumen FinTech Pada Layanan Pinjaman Online Di Indonesia: Studi Putusan No 1206 K/PDT/2024," *Al-Zayn: Jurnal Ilmu Sosial & Hukum* 4, no. 1 (2026): 707–720, https://doi.org/10.61104/alz.v4i1.3117; Elza Syarief, "Teknologi Dan Perlindungan Hak Asasi Manusia Dalam Keadaan Darurat Di Indonesia," *Global Review of Law and Human Rights* 1, no. 1 (2025): 49–64, https://idereach.com/Journal/index.php/grlhr/article/view/120.

for all data subjects, including third parties whose information is listed as emergency contact data.

3.2. Challenges in Law Enforcement Against the Misuse of Emergency Contact Data in Online Loan Collection Practices

This study aims to identify various challenges in law enforcement related to the misuse of emergency contact data in online loan collection practices, particularly within the financial technology lending (fintech lending) ecosystem. The analysis focuses on three main aspects: challenges arising from the regulatory framework, the effectiveness of oversight by relevant institutions, and the mechanisms for imposing sanctions on violations involving the misuse of personal data. Using a normative legal research approach supported by an examination of consumer complaint reports and legal literature, this study seeks to assess the extent to which the implementation of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) is capable of providing effective legal protection against the misuse of emergency contact data in online loan collection practices.

From a normative perspective, the PDP Law provides a relatively strong legal foundation for regulating the processing of personal data, including emergency contact information used in fintech lending services. The law emphasizes that any processing of personal data must be based on the valid consent of the data subject, carried out for a specific purpose, and limited to the objectives stated at the time of data collection. These provisions reflect the implementation of key personal data protection principles, including the principles of lawfulness of processing, consent, and purpose limitation.

Emergency contact information essentially constitutes supplementary information provided by borrowers to facilitate communication under specific circumstances, such as when the debtor cannot be contacted directly. Accordingly, the use of such data should be limited to emergency communication or identity verification purposes. However, in practice, several studies indicate that emergency contact information is frequently used as an alternative tool by debt collectors during the debt collection process. This practice typically involves contacting third parties listed as emergency contacts in order to exert pressure on the debtor to promptly fulfill their repayment obligations.

The use of emergency contact information in such collection practices has the potential to violate the principle of purpose limitation as stipulated in the PDP Law. Data initially collected for emergency communication purposes are instead used for purposes that differ from the original objective of data collection. From the perspective of personal data protection law, such conduct may be classified as unlawful processing of personal data because it is carried out without the valid consent of the data subject and exceeds the scope of the previously agreed purposes of data processing.

Furthermore, legal responsibility for such violations ultimately rests with the fintech lending provider as the controller of personal data. The Personal Data Protection Law explicitly emphasizes that data controllers remain responsible for all personal data processing activities, including those carried out by third parties such as debt collection agencies or individual collectors. Consequently, the delegation of debt collection activities to third parties does not absolve fintech operators of their legal responsibility for any misuse of personal data occurring during the collection process.

Although the legal framework clearly regulates these responsibilities, this study finds that law enforcement against the misuse of emergency contact data continues to face several challenges. One of the primary challenges arises from institutional factors and the lack of effective coordination among supervisory authorities. In practice, supervision of fintech lending operators falls under the authority of the Financial Services Authority (OJK). However, enforcement mechanisms for personal data protection violations committed by fintech operators still largely rely on administrative sanctions, such as written warnings, restrictions on business activities, or the revocation of business licenses.

At the same time, the Personal Data Protection Law provides the possibility of imposing criminal and civil sanctions for unlawful personal data violations. Nevertheless, the integration between the sectoral supervisory mechanisms administered by OJK and the broader law enforcement regime established under the PDP Law has not yet been fully implemented. As a result, the enforcement of legal provisions against the misuse of personal data in the fintech sector continues to encounter challenges related to institutional coordination and the effectiveness of enforcement mechanisms.

The findings of this study are consistent with several previous studies indicating that one of the primary weaknesses in personal data protection in Indonesia lies in its implementation and supervisory mechanisms. A number of studies have shown that although the regulatory framework for personal data protection has developed significantly, the effectiveness of law enforcement remains highly dependent on the institutional capacity of supervisory authorities and the level of coordination among relevant agencies.[15] Other studies have also found that personal data violations in the fintech sector frequently remain unprosecuted because most cases are resolved through administrative mechanisms rather than through formal legal proceedings.[16]

---

[15] Andayani, "Analisis Yuridis Terhadap Pengaturan Perlindungan Data Pribadi Dalam Layanan Fintech Peer-To-Peer Lending"; Antari and Triwulandari, "Legal Protection of Consumer Personal Data Peer to Peer Lending Through Financial Technology in Indonesia: An Approached of Comparative Study"; Rahmawati, Huda, and Aldhi, "Personal Data Misuse in Fintech Lending Providers from Perspective Indonesian Cyberlaw"; Rifa and Hidayati, "Kebijakan Penal Dalam Perlindungan Data Pribadi Nasabah Fintech Lending Di Indonesia"; Syahputra and Fibrianti, "Independent Authority on Personal Data Protection in Illegal Financial Technology: Capturing Peer-to-Peer (P2P) Lending Issues."

[16] Andayani, "Analisis Yuridis Terhadap Pengaturan Perlindungan Data Pribadi Dalam Layanan Fintech Peer-To-Peer Lending"; Lasmana et al., "Perlindungan Hukum Terhadap Data Pribadi Pengguna Dalam Proses

Compared with previous research, the findings of this study reinforce the argument that the problem of personal data misuse in the fintech sector is not merely related to the existence of regulatory frameworks but also to the effectiveness of existing oversight and law enforcement mechanisms. This study contributes additional insight by specifically highlighting the misuse of emergency contact data in online loan collection practices, which represents one of the most common forms of personal data violations in fintech lending services.

In addition to regulatory and institutional factors, this study also finds that low levels of public legal awareness constitute a critical factor affecting the effectiveness of law enforcement against personal data violations. Many individuals listed as emergency contacts are unaware that their personal data are protected under the Personal Data Protection Law and that they possess the legal right to object to data processing that is inconsistent with the original purpose of data collection. As a result, numerous cases of personal data misuse remain unreported to supervisory authorities or law enforcement institutions.

The limited public understanding of rights as personal data subjects also leads to the underutilization of available complaint mechanisms. In many instances, individuals listed as emergency contacts simply endure the consequences of intimidating debt collection practices without realizing that such conduct may constitute a violation of the law. This situation demonstrates that effective personal data protection depends not only on the existence of robust regulatory frameworks but also on the development of a supportive legal culture and adequate levels of public digital literacy.

The challenges associated with law enforcement against the misuse of emergency contact data in fintech lending services are therefore multidimensional.[17] These challenges are not limited to the normative aspects of regulation but also involve institutional capacity, coordination among supervisory institutions, and the level of legal awareness among members of the public as data subjects. Consequently, efforts to strengthen personal data protection in the fintech sector must be undertaken comprehensively and involve multiple stakeholders. Strengthening coordination between supervisory authorities in the financial services sector and institutions responsible for personal data protection is essential. In addition, supervision of third-party actors—such as debt collection agencies—must also be reinforced to ensure that

Penagihan Oleh Penyelenggara Peer-to-Peer Lending Berbasis PayLater"; Noptabi, Aprita, and Wulandari, "Legal Protection of Personal Data Financial Technology Based Online Loans from The Consumer Protection Act"; Novinna, "Perlindungan Konsumen Dari Penyebarluasan Data Pribadi Oleh Pihak Ketiga: Kasus Fintech Peer To Peer Lending"; Rifa and Hidayati, "Kebijakan Penal Dalam Perlindungan Data Pribadi Nasabah Fintech Lending Di Indonesia."

17 Rahmawati, Huda, and Aldhi, "Personal Data Misuse in Fintech Lending Providers from Perspective Indonesian Cyberlaw."

all personal data processing activities are conducted in accordance with applicable legal provisions.[18]

This study confirms that the primary challenges in law enforcement against the misuse of emergency contact data in fintech lending services lie in the implementation of regulatory provisions, the effectiveness of institutional oversight, and the relatively low level of public legal awareness. Although the Personal Data Protection Law provides a strong legal framework for safeguarding personal data, the effectiveness of this protection largely depends on the commitment of fintech operators to comply with personal data protection principles and the capacity of supervisory institutions to consistently enforce the law.

Strengthening the synergy between personal data protection regulations and sector-specific regulations in the fintech sector, enhancing oversight of third-party activities involved in online loan collection processes, and improving public legal education regarding the rights of personal data subjects are therefore essential. These efforts are expected to contribute to the development of a more effective and comprehensive personal data protection system.

4. CONCLUSION

This study aims to analyze the legal provisions governing the use and limitations on access to emergency contact data in fintech lending services based on Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) and relevant sectoral regulations within the financial services sector. In addition, the study seeks to identify various challenges in law enforcement related to the misuse of such data in online loan collection practices.

The results indicate that, from a normative perspective, the PDP Law provides a strong legal framework through the principles of consent, purpose limitation in personal data processing, and the obligation of data controllers to ensure the security and confidentiality of personal data. However, in practice, cases of misuse of emergency contact information continue to occur, particularly when debt collectors use such data as a means of pressuring third parties who have no direct legal relationship with the loan agreement. The findings of this study confirm that the primary challenges in law enforcement arise from weak supervisory mechanisms, the lack of optimal integration between administrative, civil, and criminal sanction mechanisms, and the relatively low level of public legal awareness regarding the right to personal data protection.

The findings of this research contribute to strengthening the development of personal data protection policies within the fintech ecosystem. However, this study is limited by its reliance on a normative legal approach without empirical data support. Therefore, future research is recommended to employ empirical methods in order to

[18] Shinta Dewi, *Cyber Law: Perlindungan Privasi Atas Informasi Pribadi Dalam Ecommerce Menurut Hukum Internasional* (Bandung: Widya Padjadjaran, 2020).

evaluate the effectiveness of the implementation of the PDP Law and to develop a more effective monitoring model for debt collection practices in fintech lending services.

REFERENCES

Journals

Andayani, Komang Dian. "Analisis Yuridis Terhadap Pengaturan Perlindungan Data Pribadi Dalam Layanan Fintech Peer-To-Peer Lending." *Aliansi: Jurnal Hukum, Pendidikan Dan Sosial Humaniora* 2, no. 5 (2025): 110–121. https://doi.org/10.62383/aliansi.v2i5.1208.

Andraini, Fitika, Adi Suliantoro, Safik Faozi, Wenny Megawati, and Infijarun Ni'am. "Pendekatan Sosio-Yuridis Terhadap Bahaya Pinjaman Online Ilegal: Analisa Proram Edukasi Interaktif Untuk Mahasiswa." *Jurnal Ilmiah Galuh Justisi* 14, no. 1 (2026): 146–64. http://dx.doi.org/10.25157/justisi.v14i1.21961.

Angeline, Priskila, and Putri Triari Dwijayanthi. "Perlindungan Data Pribadi Bagi Penerima Dana Fintech Lending Dalam Perspektif Hukum Positif Indonesia." *Kertha Semaya: Journal Ilmu Hukum* 11, no. 12 (2023): 2996–3007. https://doi.org/10.24843/KS.2023.v11.i12.p19.

Antari, Putu Eva Ditayani, and Ni Gusti Agung Ayu Mas Triwulandari. "Legal Protection of Consumer Personal Data Peer to Peer Lending Through Financial Technology in Indonesia: An Approached of Comparative Study." *Jurnal Komunikasi Hukum* 10, no. 2 (2024): 93–115. https://doi.org/10.23887/jkh.v10i2.83167.

Darnela, Lindra, and Erma Rusdiana. "Public Legal Awareness and the Effectiveness of Indonesia's Personal Data Protection Law: Bridging Normative Framework and Privacy Paradox." *Supremasi Hukum: Jurnal Kajian Ilmu Hukum* 14, no. 1 (2025): 1–28. https://doi.org/10.14421/2gg2rp29.

Johan, Suwinto. "Financial Technology Company's Debt Collection Method: A Legal Aspect." *Unnes Law Journal* 8, no. 1 (2022): 1–20. https://doi.org/10.15294/ulj.v7i1.52173.

Lasmana, Josephine Aprilia, Ivan Imam Efendi, Indah Rahma Mareta, and Farahiyah Dini Khoirun Nafida. "Perlindungan Hukum Terhadap Data Pribadi Pengguna Dalam Proses Penagihan Oleh Penyelenggara Peer-to-Peer Lending Berbasis PayLater." *Begawan Abioso* 16, no. 2 (2025): 63–73. https://doi.org/10.37893/abioso.v16i2.1237.

Maulana, Muhammad Irfan, Muhamad Hiroshi Ikhsan, Muhammad Bintang Firdaus, and Dwi Desi Yayi Tarina. "Kepastian Hukum Dan Perlindungan Konsumen FinTech Pada Layanan Pinjaman Online Di Indonesia: Studi

Putusan No 1206 K/PDT/2024." *Al-Zayn: Jurnal Ilmu Sosial & Hukum* 4, no. 1 (2026): 707–720. https://doi.org/10.61104/alz.v4i1.3117.

Noptabi, Iim Saputra, Serlika Aprita, and Mona Wulandari. "Legal Protection of Personal Data Financial Technology Based Online Loans from The Consumer Protection Act." *Walisongo Law Review* 4, no. 1 (2022): 121–134. https://doi.org/10.21580/walrev.2022.4.1.11135.

Novinna, Veronica. "Perlindungan Konsumen Dari Penyebarluasan Data Pribadi Oleh Pihak Ketiga: Kasus Fintech Peer To Peer Lending." *Jurnal Magister Hukum Udayana* 9, no. 1 (2020): 92–110. https://doi.org/10.24843/JMHU.2020.v09.i01.p07.

Pane, Ian Dharsono Wijaya, and Christine S.T. Kansil. "Penyelesaian Sengketa Terhadap Dugaan Penyalahgunaan Data Pribadi Dalam Layanan Fintech." *Syntax Literate: Jurnal Ilmiah Indonesia* 7, no. 11 (2011): 17174–87. https://doi.org/10.36418/syntax-literate.v7i11.12021.

Rahmawati, Elvia, Miftakhul Huda, and Ian Firstian Aldhi. "Personal Data Misuse in Fintech Lending Providers from Perspective Indonesian Cyberlaw." *Airlangga Development Journal* 8, no. 1 (2024): 8–20. https://doi.org/10.20473/adj.v8i1.56398.

Rifa, Fauzi, and Maslihati Nur Hidayati. "Kebijakan Penal Dalam Perlindungan Data Pribadi Nasabah Fintech Lending Di Indonesia." *Binamulia Hukum* 13, no. 2 (2024): 461–481. https://doi.org/10.37893/jbh.v13i2.964.

Syahputra, Bearlly Deo, and Nurul Fibrianti. "Independent Authority on Personal Data Protection in Illegal Financial Technology: Capturing Peer-to-Peer (P2P) Lending Issues." *Journal of Private and Commercial Law Section* 8, no. 1 (2024): 114–35. https://doi.org/10.15294/jpcl.v8i1.3967.

Syarief, Elza. "Teknologi Dan Perlindungan Hak Asasi Manusia Dalam Keadaan Darurat Di Indonesia." *Global Review of Law and Human Rights* 1, no. 1 (2025): 49–64. https://idereach.com/Journal/index.php/grlhr/article/view/120.

Books

Dewi, Shinta. *Cyber Law: Perlindungan Privasi Atas Informasi Pribadi Dalam Ecommerce Menurut Hukum Internasional.* Bandung: Widya Padjadjaran, 2020.