RECHTENSTUDENT JOURNAL
Volume 5 Number (3) December 2024, pp. 198-210
DOI: https://doi.org/10.35719/rch.v5i3.356
Published by the UIN KHAS Jember, Indonesia
ISSN: 2723-0406 | E-ISSN: 2775-5304 Available online 30 December 2024

Legal Protection for Financial Technology Peer to Peer Lending Debtors Against Doxing Actions by Creditors

Muhammad Fatoni Kurniawan*
University of Jember, Indonesia
Fendi Setyawan
University of Jember, Indonesia
Dyah Ochtorina Susanti
University of Jember, Indonesia
****Corresponding Author's Email:*** muhammadfatonik@gmail.com

Article

How to cite:
Muhammad Fatoni Kurniawan, et al, **'Legal Protection for Financial Technology Peer to Peer Lending Debtors Against Doxing Actions by Creditors'** (2024) Vol. 5 No. 3 Rechtenstudent Journal, Sharia Faculty of KH Achmad Siddiq Jember State Islamic University.

DOI:
10.35719/rch.v5i3.356

Article History:
Submitted: 30/10/2024
Reviewed: 05/11/2024
Revised: 21/11/2024
Accepted: 29/11/2024

ISSN:
2723-0406 (printed)
E-ISSN:
2775-5304 (online)

Abstract

Technological advancements have increased financial access through financial technology (fintech) services, particularly peer-to-peer (P2P) lending, yet these developments also present significant risks. Illegal online lenders (*pinjol*) often misuse personal data and employ intimidating debt collection practices, while large-scale data breaches, such as those involving BPJS Kesehatan, Tokopedia, and Kredit Plus where 890,000 customer records were allegedly leaked and sold highlight the urgent need for effective debtor protection. This research employs a normative juridical method using statutory, conceptual, and historical approaches to examine the legal framework for debtor protection against doxing practices. The findings show that legal protection is crucial to maintaining stability, security, and user trust in fintech services. Protection mechanisms are divided into internal measures, which regulate transparency, fair treatment, confidentiality, and risk management, and external measures provided by authorities through law enforcement, administrative sanctions, and dispute resolution. Despite the existence of the Personal Data Protection Law (PDP Law), the Information and Electronic Transactions Law (ITE Law), and Financial Services Authority (OJK) regulations, regulatory disharmony, weak supervision, and low public awareness hinder effective protection. Strengthening PDP Law enforcement and explicitly prohibiting doxing practices in OJK regulations are recommended.
Keywords: *Fintech, Doxing, Legal Protection.*

Abstrak

Perkembangan teknologi mempermudah akses keuangan melalui layanan fintech seperti *peer to peer* (P2P) lending. Namun, kemudahan ini disertai risiko, terutama dari pinjaman online (pinjol) ilegal yang kerap menyalahgunakan data pribadi dan melakukan penagihan secara intimidatif. Lemahnya perlindungan hukum memperparah situasi, ditambah maraknya kebocoran data seperti pada BPJS Kesehatan, Tokopedia, dan Kredit Plus. Salah satu kasus serius adalah bocornya sekitar 890.000 data nasabah Kredit Plus yang diduga dijual bebas di internet. Jenis penelitian yang digunakan dalam ini adalah tipe penelitian yuridis normatif, menggunakan tiga pendekatan yakni pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan sejarah (history). Penelitian ini menunjukkan perlindungan hukum dalam industri fintech sangat penting untuk menjaga stabilitas, keamanan, dan kepercayaan pengguna. Perlindungan ini terbagi menjadi dua bentuk, yaitu perlindungan internal yang

berfokus pada pengaturan operasional dan hubungan antara pihak-pihak yang terlibat dalam layanan fintech melalui regulasi yang mengatur transparansi, perlakuan adil, kerahasiaan data, serta manajemen risiko. Sementara itu, perlindungan eksternal diberikan oleh otoritas melalui penegakan hukum, sanksi administratif, dan mekanisme penyelesaian sengketa guna melindungi konsumen sebagai pihak yang lebih rentan. Meskipun Indonesia telah memiliki sejumlah regulasi seperti UU Perlindungan Data Pribadi (UU PDP), UU ITE, dan berbagai Peraturan OJK terkait fintech, perlindungan hukum terhadap debitur, khususnya dari tindakan doxing oleh penyelenggara pinjaman online, masih menghadapi tantangan besar dalam implementasi. Ketidakharmonisan antar peraturan, lemahnya kapasitas lembaga pengawas, serta rendahnya kesadaran masyarakat dan pelaku usaha menjadi kendala utama. Oleh karena itu, diperlukan pembaruan hukum yang mencakup penguatan implementasi UU PDP, pengaturan khusus dalam POJK yang melarang secara tegas praktik *doxing*.
Kata Kunci *Teknologi Finansial, Doxing, Perlindungan Hukum.*

Introduction

Technological advancements have transformed every aspect of life. In today's world, people's activities in every sector have also undergone significant changes. Collecting and distributing another person's personal data is now considered a violation. Any data containing another person's personal information can have economic value. The issue of protecting each person's personal data has long been a concern.[1]

Data such as Population Identification Number (NIK), Electronic Population Identification Card (E-KTP), Family Card (KK), is a classification of information that must be protected.[2] Violations of personal data can include wiretapping, selling, and other actions without the owner's permission. In the context of a criminal act, data can be misused for unlawful purposes, such as money laundering, scamming, and so on. This is why it's urgent to protect personal data.[3]

Fintech is the combination of financial services and technology, ultimately transforming business models from conventional to technology-based. Previously, debtors had to meet face-to-face and carry cash to make payments. Now, debtors can conduct remote transactions, making payments in seconds. [4] Fintech P2P lending provides borrowers with easy access to loans quickly and without going through traditional financial institutions.[5] This can also expose them to potential risks, such as falling into the trap of high interest rates. Furthermore, intimidating loan collection practices are currently causing concern among those seeking quick funding.

Many wealthy or financially successful individuals can also fall prey to online loans, known as "pinjol," even though they may have numerous assets or high incomes. Pinjol is

[1] Gatot Supramono, Perjanjian Pinjam Meminjam, (Jakarta : Prenadamedia Kencana, 2013), 29.
[2] Windy Sonya Novita, Aspek Hukum Peer To Peer Lending dalam Identifikasi Permasalahan Hukum dan Mekanisme Penyelesaian, *Jurnal Yustisia Privat Law Sebelas Maret University*, Volume 8, No. 1 Tahun 2020, 156.
[3] i*bid*
[4] Lukmaul Hakim, et.all. Pengaruh Pinjaman Online Terhadap Perkembangan Usaha Koperasi Syariah Bmt Investa Mubarokah Cianjur, *Jurnal Keuangan dan Perbankan Syariah*, Vol. 02, No. 02 September, 2022, 179
[5] Abdul Karim, et.al, Fintech P2P Lending in Increasing People's Purchasing Power in South Sulawesi Province, *Journal the Winners,* Vol. 5 No. 2, 2024, 116.

often an option for low-income individuals because it offers quick access through simple requirements. However, these loans are highly vulnerable to predatory lenders, particularly illegal lenders that are unregistered and unlicensed by the Financial Services Authority (OJK).[6]

When borrowers enter the online lending market, they will consistently receive offers via text message with links to download illegal loan apps. They will also be constantly presented with attractive special offers to use online loans as a quick way to resolve their financial problems. Once enticed by these offers, consumers' finances are subtly exploited by illegal lenders, who offer fast funds that can be disbursed instantly within hours with simple requirements.Consequently, these illegal lending providers charge exorbitant interest rates and service fees, burdening borrowers. While the loan process is easy and withdrawals are quick, transaction security can be problematic, particularly with frequent doxing by lenders.[7]

Throughout 2020 and 2022, there have been cases of personal data leaks. Some of the major cases include the data leak of consumers of the "Social Security Administration (BPJS) Health" which reached 260 million leaked users, then the e-commerce data leak Cermati and e-commerce Lazada data leak and sale of customer data KreditPlus, a fintech that has long been involved in providing P2P world industry services, then the data leak of Tokopedia e-commerce service users, in May 2020.[8]

Based on the many existing case examples, legally based on the 1945 Constitution of the Republic of Indonesia, the protection of personal data is the right of every citizen guaranteed by the constitution based on Article 28G paragraph (1) "Everyone has the right to protection of themselves, their families, their honor, their dignity, and their property under their control, and has the right to a sense of security and protection from the threat of fear to do or not do something that is a basic human right."[9]

Based on the data collected on cases of misuse of personal data in the fintech industry based on peer to peer lending, there are many examples of cases that can be used as study material, one example of a case of personal data leakage is the leak of personal data belonging to customers using online loan services (pinjol) from Indonesia, namely fintech Kreditplus, which is suspected of being leaked and sold freely on the internet.[10]

Calculations and investigations by fintech service providers, including PT. Kredit Plus Indonesia, indicate that approximately 890,000 Kredit Plus customers' data were allegedly leaked. This is undoubtedly detrimental to consumers of the fintech service. Indications of criminal activity resulting from personal data leaks, which then lead to unauthorized misuse of personal data, are highly vulnerable and frequently occur in Indonesia's cyber world.[11]

---

[6] Risma Dewi Hermawan, et.al, Upaya Polri Memberikan PerlindunganHukumbagi Konsumen dalamPerjanjian Pinjaman Online Ilegal di Surakarta, *Rechtenstudent Journal,* Vol. 4 No. 1, 2023, 52.

[7] Nanang Shonhadji, Fraud Analysis on Illegal Online Lending Using Haberma's Theory of the Public Sphere, *Jiab,* Vol. 17 No. 1, 2022, 34.

[8] Caesar Akbar, "6 Kasus Kebocoran Data Pribadi Di Indonesia ," accessed July 23, 2025, https://nasional.tempo.co/read/1501790/6-kasus-kebocoran-data-pribadi-di-Indonesia.

[9] Denny Suwondo, The Legal Protection of Personal Data in Perspective of Human Rights, *Law Development Journal,* Vol. 5 No. 4, 2023, 420.

[10] Fika Nurul Ulya and Sakina Rakhma Diah Setiawan, "Data Nasabah KreditPlus Bocor Ini Kata OJK," accessed July 23, 2025, https://money.kompas.com/read/2020/08/04/170900526/data-nasabah-kreditplus-bocor-ini-kataojk.

[11] ibid

The misuse of personal data in online lending applications constitutes a violation of privacy and human dignity, and violates a two-party agreement between the creditor and the debtor. The data misuse by PT. Kredit Plus Indonesia results in significant losses for users of the industry's services.[12]

Personal data leaks not only impact customers or users but also other impacts, such as the privacy of their families, the circulation of personal data, which can lead to cybercrimes such as savings account breaches, credit card hacking, social media account hacking, and many other detrimental issues. Given the numerous cases of personal data leaks by P2P providers, as described above, the urgent need for the creation of organic legislation is crucial to harmonize laws protecting privacy and personal data in cyberspace in the digital age and to fill the gap. Based on the background of the problem above, it is interesting to study the state's obligation to protect Financial Technology Peer to Peer Lending Debtors regarding doxing actions by Creditors and to find out how the law is updated for Financial Technology Peer to Peer Lending Debtors regarding doxing actions in a thesis research entitled "Legal Protection for Financial Technology Peer to Peer Lending Debtors Against Doxing Actions by Creditors."

Research Method

The type of research used is normative juridical, this research is focused on examining the application of rules or norms in applicable positive law.[13] Normative legal research is also known as doctrinal research. Doctrinal legal research aims to provide a systematic exposition (detailed explanation) of the legal rules governing a particular legal field, analyzing the relationships between these legal rules. The goal is to provide a systematic exposition that regulates legal protection for debtors in financial technology peer-to-peer lending against doxing by creditors.[14]

This study uses three legal research approaches: the statute approach, the conceptual approach, and the historical approach. The statute approach is conducted by examining all laws and regulations related to the legal issue being discussed.

Results and Discussion

Creditors' Responsibilities When They Are Known to Have Carried Out Doxing Actions

Indonesia is one of the countries with a high number of internet users. According to data from Internetworldstats, as of March 2021, internet penetration in Indonesia reached 76.8% of the country's population, with 212.35 million users. The majority of users use the internet for communication via social media and search engines for various purposes.[15]

The internet's existence in Indonesia is inextricably linked to the use of social media platforms such as Facebook, Instagram, LINE, Twitter, WhatsApp, YouTube, and others. It

[12] Muhammad Labib & Rumawi, Legal Protection for Financial Technology Users Against Fraud and Illegal Acts, *Rehctenstudent Journal,* Vol 4 No. 3, 2023, 216.

[13] Mukti Fajar and Yulianto Achmad, *Dualisme Penelitian Hukum Normatif Dan Empiri*s (Pustaka Pelajar, 2017). 33

[14] Dyah Ochtorina Susanti and A'an Efendi, *Penelitian Hukum (Legal Research)* (Sinar Grafika, 2018). 11

[15] Agnes z Yonatan, "Indonesia Peringkat 4," accessed July 23, 2025, , https://data.goodstats.id/statistic/indonesia-peringkat-4-ini-dia-7-negara-pengguna-internet-terbesar-di-dunia-FLw6V.

seems that not only has positive impacts, but it also creates the potential for new problems, namely cybercrime.[16]

One form of personal data crime on social media is doxing/doxxing, or dropping boxes. The data of approximately 890,000 Kredit Plus customers was allegedly leaked. This is undoubtedly very detrimental to consumers of this fintech service. Indications of criminal acts resulting from personal data leaks, which then lead to misuse of personal data without the data owner's consent, are highly vulnerable and frequently occur in Indonesia's cyber world.[17]

Legal protection theory according to Moch. Isnaeni, legal protection theory according to Mochammad Isnaeni is a theory of civil legal protection. Legal protection is a legal effort given to legal subjects to protect their rights through legal mechanisms. Internal legal protection is legal protection created through an agreement made by each party. External legal protection is legal protection created by the authorities through the formation of regulations aimed at the interests of the weaker party.[18]

Fintech is a technology-based money lending service in Indonesia. Financial Services Authority Regulation No. 77/POJK.01/2016, Article 1 Number 3, states that "Technology-Based Money Lending Services (fintech) are the provision of financial services to bring together lenders and borrowers to enter into loan agreements in rupiah directly through an electronic system using the internet."[19]

The creditor's liability to the debtor in cases of doxing, which is the unauthorized dissemination of a debtor's personal information that could compromise the debtor's privacy or security, depends on various factors, including the applicable laws in the country or region where the transaction takes place. In general, doxing by a creditor or a party related to the creditor can involve several legal violations, and the creditor may be subject to sanctions or certain responsibilities. The concept of legal protection is divided into two categories:

a. Internal Legal Protection

Internal legal protection is legal protection created through an agreement between each party. Internal legal protection is preventative in nature, thus, it is implemented before a dispute arises. Legal protection for Fintech service users before a dispute arises can be achieved through efforts by the Fintech service provider.

The provider's efforts before the aforementioned dispute arise include implementing the basic principles of legal protection for Fintech service users. These principles are stated in Article 29 of POJK No. 77/POJK.01/2016 concerning Information Technology-Based Money Lending Services, which states, "The principles of transparency, fair treatment, reliability, data confidentiality and security, and simple, fast, and affordable resolution of user disputes." .

b. External Legal Protection

---

[16] Wina Puspita Sari & Asep Soegiarto, Indonesia Government Public Relations in Using Social Media, *ICHELSS,* 2021, 495-496.

[17] Teguh Cahya Yudiana, et.al, The Urgency of Doxing on Social Media Regulation and the Implementation of Right to Be Forgitten on Related Content for the Optimization of Data Privacy Protection in Indonesia, PJIH, Vol. 9 No. 1, 2022, 26.

[18] Moch. Isnaeni, *Pengantar Hukum Jaminan Kebendaan* (Revka Petra Media , 2016). 39-42

[19] I Putu Raditya Sudwika Utama & Anak Agung Gede Agung Indra Prathama, Pengawasan Bank Indonesia dan Otoritas Jasa Keuangan terkait Penerapan Financial Technology, *Yusttia,* Vol. 16 No. 2, 2022, 172.

External legal protection is legal protection created by authorities through the establishment of regulations aimed at the benefit of the vulnerable party. This protection can only be implemented after a dispute arises. Disputes within fintech providers can occur between providers and users, or between users themselves. If a dispute has arisen, there are specific methods for resolving the issue. Anyone who feels they have been harmed can file a complaint so that the problem can be resolved promptly.

When a fintech provider receives a complaint from a service user who feels aggrieved, the fintech provider must immediately follow up, as stipulated in Article 38 of POJK No. 1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector, which states, "Financial service providers, in this case Fintech service providers, are required to conduct: a. Internal investigations of complaints competently, correctly, and objectively; b. Analysis to ensure the validity of the complaint; c. Issue an apology and offer compensation (redress/remedy) or product and/or service improvements, if the consumer's complaint is justified."

According to Mochammad Isnaeni, in the context of doxing, there are internal and external legal protections. This can be analyzed to see how the legal system can protect victims of doxing and impose sanctions on perpetrators. Internal legal protection, according to Mochammad Isnaeni, focuses on efforts to prevent legal violations before they occur. In relation to doxing, this internal protection is crucial for reducing the likelihood of crimes or violations of a person's right to privacy.

External legal protection, according to Moch. Isnaeni, functions to respond to or address legal violations that have already occurred, as well as provide sanctions or redress for victims after the violation occurs. In the case of doxing, this external approach is crucial to ensure that perpetrators of doxing are prosecuted and victims receive justice.[20]

External protections in relation to doxing: Prosecution of the Doxing Perpetrator. After doxing occurs, authorities can investigate and prosecute the perpetrator for any violation of the law, whether related to defamation, unauthorized disclosure of personal data, or even threats to the victim's safety. In many legal systems, doxing can be considered a crime that threatens someone's privacy, and therefore, the perpetrator can face criminal prosecution.

External protections also include measures taken to protect the victim after doxing occurs. This can include compensation for the harm suffered by the victim, both material (e.g., financial loss) and immaterial (e.g., reputational and emotional harm). Additionally, victims can obtain a court order to remove the information disseminated or prohibit the perpetrator from taking further action against them.

Legal Reforms to Protect Debtors from Doxing by Creditors

Despite the existence of regulations such as the Personal Data Protection Law (PDP Law), the Electronic Information and Transactions Law (ITE Law), and the Financial Services Authority Regulation (POJK), the implementation and enforcement of personal data protection laws in Indonesia still face significant challenges. These challenges include: Disharmony between various regulations leads to inconsistent interpretation and application

[20] ibid

of the law, law enforcement is often hampered by the lack of capacity of supervisory institutions and inadequate legal procedures, and the low level of public and business understanding of the rights and obligations related to personal data protection, which hinders comprehensive protection efforts.

Legal Updates to Protect Debtors from Doxing by Creditors in the Indonesian Fintech Context. Doxing (the unauthorized distribution of a person's personal information with the intent to harm or embarrass them) by creditors or fintech providers against debtors is an increasingly relevant issue in the development of the fintech industry in Indonesia. This is especially true with the rise of online lending practices, where debtors' personal data is highly vulnerable to misuse. Therefore, there is an urgent need for clearer and more effective legal updates to protect debtors from potential misuse of personal data, including detrimental doxing.

First, Strengthening Personal Data Protection (PDP Law). One of the key steps in legal reform to protect debtors from doxing is to strengthen and clarify the implementation of the PDP Law, which was enacted in 2022. The PDP Law provides a clearer legal basis for the management and protection of personal data in Indonesia and strictly regulates the obligations of data managers to maintain the confidentiality of consumers' (in this case, debtors') personal data.

Lawful and transparent processing of personal data: Every fintech provider must obtain explicit consent from debtors to collect, store, and use their personal data. Misuse of personal data, including for doxing, may result in administrative and criminal sanctions.

a. Right to deletion of personal data: Debtors have the right to request deletion of their personal data from fintech platforms after repaying their loans, to reduce the risk of misuse or the dissemination of detrimental information.
b. Strict sanctions against misuse of personal data: The PDP Law must ensure that there are stricter sanctions against misuse of debtors' personal data, both by fintech companies themselves and third parties who access the data for unauthorized purposes.

While the Personal Data Protection Law provides a strong legal framework, its effectiveness remains to be tested in the implementation phase. One major challenge is the establishment and operationalization of a personal data protection supervisory body, which would oversee compliance with the Personal Data Protection Law and handle complaints related to personal data breaches. Delays in establishing this body could undermine the effectiveness of the protections promised by the Personal Data Protection Law. This is a major concern because the supervisory body plays a crucial role in ensuring the consistent implementation of data protection principles.[21]

From the perspective of Satjipto Rahardjo's legal certainty theory, the Personal Data Protection Law provides a clearer and more comprehensive legal framework than previous regulations. This law explicitly defines what is meant by personal data, the rights of data subjects, and the obligations of data controllers and processors. This clarity is expected to

[21] Yolanda, E., dan Hutabarat. Urgensi Lembaga Pelindungan Data Pribadi di Indonesia Berdasarkan Asas Hukum Responsif. Syntax Literate: Jurnal Ilmiah Indonesia, volume 8, nomor 6) 2023, 6

increase legal certainty for all parties involved in the processing of personal data, while also encouraging compliance with applicable regulations.[22]

Although the Personal Data Protection Law has provided a clearer legal framework, several areas still require clarification to increase legal certainty. One such area is the consent mechanism considered valid in the digital context, which currently requires more detailed guidance. Furthermore, the criteria for determining "legitimate interests" as the legal basis for processing personal data also need to be elaborated in greater detail to avoid overly broad interpretations and potential abuse.

Second, Special Provisions in the OJK Regulation on Fintech. The OJK Regulation on online lending and fintech should include specific provisions regarding the prohibition of doxing practices by fintech operators. Several areas that could be the focus of the update include::

a. Prohibition on the dissemination of personal information without the debtor's consent: Provisions are needed that explicitly prohibit fintech providers from disseminating debtors' personal information without the debtor's written or explicit consent. This includes, for example, disclosing debtors' personal information in any form (name, address, telephone number, place of employment, etc.) to third parties without consent.
b. Handling violations by fintech providers: The Financial Services Authority (OJK) can establish stricter regulations to ensure that fintech providers have effective internal mechanisms to handle violations related to the dissemination of debtors' personal information. Fintech providers found to have committed doxing acts should be subject to severe administrative sanctions, including revocation of their operating licenses.
c. Educational obligations for fintech providers: Fintech providers should also be required to provide education to debtors regarding their rights regarding personal data and how to protect that information. This is important to prevent debtors from becoming victims of doxing acts that could occur.

Financial Services Authority Regulation (POJK) Number 77/POJK.01/2016 and POJK Number 10/POJK.05/2022 provide a more specific regulatory framework regarding personal data protection in the context of fintech lending. From a legal protection theory perspective, these two POJKs provide internal protection through the obligation of fintech lending providers to maintain the confidentiality of customer personal data and obtain customer consent before using personal data for specific purposes.

External protection in the Financial Services Authority Regulation (POJK) is evident in the administrative sanctions for violations of personal data protection provisions. However, these sanctions are limited to the Personal Data Protection Law (PDP) and the Electronic Information and Transactions (ITE) Law. The absence of criminal sanctions in the POJKs may reduce the deterrent effect for perpetrators of serious violations of customer personal data.[23]

From a legal certainty perspective, the POJK provides a fairly clear regulatory framework for personal data protection in the context of fintech lending. However, several

[22] Julyano, M., dan Sulistyawan, A. Y. Pemahaman Terhadap Asas Kepastian Hukum Melalui Konstruksi Penalaran Positivisme Hukum. Jurnal Crepido, volume 1 nomor 1 2019, 14

[23] Nurul Insi Syahrudidin & Eva Achjani Zulfa, Personal Data Protection Violations by Fintect Lending in Indonesia, *JLPH,* Vol. 4 No. 4, 2024, 1000.

areas require further clarification. One such issue is the mechanism for valid consent in a digital context, which currently lacks adequate technical guidance. Furthermore, procedures for handling personal data breaches require more detailed regulations to ensure fairness for all parties involved.

Third, the Revision and Strengthening of the Electronic Information and Transactions (ITE) Law. The crime of doxing can also be considered a violation of the ITE Law (Law Number 11 of 2008 concerning Electronic Information and Transactions), which regulates the misuse of electronic information, including defamation, blackmail, and the unauthorized dissemination of personal data.

Misuse of personal information as a crime: The ITE Law could be updated by adding an article specifically criminalizing doxing, or the unauthorized dissemination of personal data intended to harm or defame. This needs to be part of a broader effort to eradicate data misuse in the digital space. Increased criminal sanctions: In the context of doxing by creditors or fintech providers, criminal sanctions could be increased, including imprisonment and higher fines. This is expected to have a deterrent effect and reduce data misuse practices.

The Electronic Information and Transactions Law (ITE Law) also plays an important role in personal data protection in Indonesia. From a legal protection theory perspective, the ITE Law provides internal protection by requiring electronic system providers to maintain the confidentiality of users' personal data. External protection is realized through criminal sanctions for parties who violate personal data protection provisions. However, from a legal certainty theory perspective, the ITE Law provides a fairly clear legal framework for electronic transactions in general but lacks certainty in the context of personal data protection. Compared with the PDP Law, the ITE Law is more general in nature and therefore requires harmonization.

Fourth, Strengthening the Role of Supervisory Institutions and Complaint Services. To make it easier for debtors to access legal protection related to doxing, supervisory institutions such as the Financial Services Authority (OJK) and the Ministry of Communication and Information Technology (Kominfo) need to strengthen complaint mechanisms and resolve disputes quickly and effectively.[24]

a. More accessible complaint services: Debtors should be able to easily file complaints regarding misuse of personal data or doxing by fintech providers, either through the OJK platform or other services integrated with the personal data complaint system.
b. Fast and fair dispute resolution processes: Courts or arbitration institutions dealing with fintech disputes can introduce special procedures to handle disputes involving violations of personal data rights or doxing. Prompt dispute resolution will reduce the losses incurred by debtors due to the misuse of their personal information..

Fifth, Legal Education and Awareness for Debtors In addition to regulatory updates, it is also important to provide legal education to the public, especially debtors, regarding their rights regarding personal data and the legal protection available.

[24] Ambar Alimatur Rosyidah, et.al, Cyber Crime Against Women's Personal Data on Online Platforms and The Role of PDP Laws, *Jurnal Komunikasi Indonesia,* Vol. 13 No. 2, 2024, 265.

a. Education on personal data rights: Debtors need to be given a better understanding of their rights in the context of fintech transactions, including the right to control their personal information and the right to protection from data misuse.
b. Counseling on how to report doxing: Debtors should also be provided with information on how to report doxing, either through the Financial Services Authority (OJK), the Ministry of Communication and Information Technology (Kominfo), or other complaint platforms. This counseling is important so that debtors can immediately take legal action when facing data misuse.

The fintech lending industry has unique characteristics that involve sensitive financial data. Therefore, higher security standards need to be implemented, such as: a) Customer financial data must be encrypted end-to-end to protect the confidentiality of information during storage and transfer. b) Fintech lending companies are required to conduct regular security audits to ensure compliance with security standards and identify potential vulnerabilities.

Legal protection for debtors in online lending cases is regulated to prevent and prosecute consumer rights violations by business actors. However, in practice, legal protection for online loan debtors is still not fully optimal. This is due to several factors, including : [25]

1. Lack of public understanding of consumer rights in online lending.
2. Weak oversight and law enforcement of online lending businesses.
3. Low awareness among online lending businesses regarding compliance with laws and regulations.

The need for implementing regulations for the PDP Law reveals several important aspects. First, implementing regulations are needed to further define technical standards and procedures such as data security, consent criteria, and effective complaint mechanisms for data breaches. Second, in this digital and connected context, the regulations should also include guidelines on cross-border data transfers, which is crucial given the large number of business operations that transcend national jurisdictions.

Furthermore, given the rapid development of technology, it is possible that some provisions in the PDP Law may need to be adjusted or updated to meet emerging new challenges. For example, recent developments in artificial intelligence and machine learning may require a rethinking of how personal data is processed and the necessary privacy protections. In this regard, amendments to several articles in the PDP Law may be necessary to ensure that the law remains relevant and effective in protecting citizens' privacy rights.

In developing derivative laws for Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) in Indonesia, detailed consideration is required regarding who is involved, the form of regulation to be implemented, the implementation process, and the limitations that must be observed to prevent misuse. First, these derivative laws must clearly identify the subjects involved, including data controllers, data processors, data subjects, and technology service providers and online platforms. This is crucial for establishing the responsibilities of each party in the data processing process.

[25] Muhammad Subhan and Nabila Ihza Nur Muttaqi, "Perlindungan Hukum Bagi Korban Penyebaran Data Pribadi Oleh Penyedia Jasa Pinjaman Online Illegal Dalam Perspektif Viktimologi," *Delicti : Jurnal Hukum Pidana Dan Kriminologi* 2, no. 1 (2024). 12

Second, the regulations in these derivative laws must include clear and unambiguous provisions regarding consent, procedures for reporting and responding to violations, and effective audit and monitoring mechanisms. Clear and firm sanctions must also be established to prevent violations and provide a deterrent effect for perpetrators.

Third, the implementation of this derivative law requires close collaboration between institutions, including data protection authorities and law enforcement, as well as the implementation of education and training programs to raise awareness among data controllers and data processors about the importance of personal data protection. Civil society participation in oversight and evaluation is also vital to ensure transparency and accountability.

Finally, the derivative law must have clear boundaries to prevent excessive and irrelevant data collection, and ensure that access to personal data is limited only to legitimate purposes and has been consented to by data subjects. Transparency from data controllers and processors in all data processing activities must also be ensured. With these steps, Indonesia can strengthen the protection of its citizens' privacy in facing the challenges of the digital era, while supporting innovation and responsible growth.

Conclusion

It can be concluded that legal protection in the fintech industry is crucial for maintaining stability, security, and user trust. This protection is divided into two forms: internal protection, which focuses on operational arrangements and relationships between parties involved in fintech services through regulations governing transparency, fair treatment, data confidentiality, and risk management. Meanwhile, external protection is provided by authorities through law enforcement, administrative sanctions, and dispute resolution mechanisms to protect consumers as the more vulnerable party. With complementary regulations, the fintech industry can develop healthily and sustainably.

Although Indonesia already has several regulations, such as the Personal Data Protection Law (PDP Law), the Electronic Information and Transactions Law (ITE Law), and various Financial Services Authority (OJK) regulations related to fintech, legal protection for debtors, particularly against doxing by online lenders, still faces significant challenges in implementation. Disharmony between regulations, weak supervisory capacity, and low public and business awareness are key obstacles. Therefore, legal reform is needed, including strengthening the implementation of the PDP Law, specific regulations in the Financial Services Authority Regulation (POJK) that explicitly prohibit doxing practices, revising the ITE Law to criminalize the unauthorized dissemination of personal data, and strengthening the role of supervisory agencies and complaint services. Furthermore, legal education for the public and improving technology security standards must be integral parts of this effort.

Bibliography

Book

Dyah Ochtorina Susanti, dan A'an Efendi. *Penelitian Hukum (Legal Research)*. Jakarta: Sinar Grafika, 2018.

Fajar, Mukti dan Yulianto Achmad. *Dualisme Penelitian Hukum Normatif dan Empiris*. Yogyakarta: Pustaka Pelajar, 2017

Isnaeni, Moch. *Pengantar Hukum Jaminan Kebendaan*. Surabaya: Revka Petra Media, 2016.

Supramono, Gatot. *Perjanjian Pinjam Meminjam*. Jakarta: Prenadamedia Kencana, 2013.

Journal

Karim, Abdul, Muhlis Ruslan, Chahyono, Muh. Kafrawi Yunus, dan Amrullah Ahmad. "Fintech P2P Lending in Increasing People's Purchasing Power in South Sulawesi Province." *Journal the Winners* 5, no. 2 (2024): 116. https://doi.org/10.21512/tw.v25i2.12059

Hermawan, Risma Dewi, Aris Prio Agus Santoso, dan Kresna Agung Yudhianto. "Upaya Polri Memberikan Perlindungan Hukum bagi Konsumen dalam Perjanjian Pinjaman Online Ilegal di Surakarta." *Rechtenstudent Journal* 4, no. 1 (2023): 52–62. https://doi.org/10.35719/rch.v4i1.220

Hakim, Lukmaul, Fitriyani Fitriyani, Muhammad Ilham Cahya Permana, dan Nisa Nurul Aini. "Pengaruh Pinjaman Online terhadap Perkembangan Usaha Koperasi Syariah BMT Investa Mubarokah Cianjur." *Jurnal Keuangan dan Perbankan Syariah* 2, no. 2 (2022). https://doi.org/10.35194/arps.v2i2.2673

Julyano, M., dan A. Y. Sulistyawan. "Pemahaman Terhadap Asas Kepastian Hukum Melalui Konstruksi Penalaran Positivisme Hukum." *Jurnal Crepido* 1, no. 1 (2019).

Labib, Muhammad, and Rumawi. "Legal Protection for Financial Technology Users Against Fraud and Illegal Acts." *Rechtenstudent Journal* 4, no. 3 (2023): 216.

Novita, Windy Sonya. "Aspek Hukum Peer To Peer Lending dalam Identifikasi Permasalahan Hukum dan Mekanisme Penyelesaian." *Jurnal Yustisia Privat Law* 8, no. 1 (2020).

Rosyidah, Ambar Alimatur, Farah Fajriyah, dan Rahayu Rahayu. "Cyber Crime Against Women's Personal Data on Online Platforms and The Role of PDP Laws." *Jurnal Komunikasi Indonesia* 13, no. 2 (2024): 265. https://doi.org/10.7454/jkmi.v13i2.1229

Sari, Wina Puspita dan Asep Soegiarto. "Indonesia Government Public Relations in Using Social Media." *ICHELSS* (2021): 495–496.

Shonhadji, Nanang. "Fraud Analysis on Illegal Online Lending Using Habermas's Theory of the Public Sphere." *JIAB* 17, no. 1 (2022): 34.

Subhan, Muhammad, dan Nabila Ihza Nur Muttaqi. "Perlindungan Hukum bagi Korban Penyebaran Data Pribadi oleh Penyedia Jasa Pinjaman Online Ilegal dalam Perspektif Viktimologi." *Delicti: Jurnal Hukum Pidana dan Kriminologi* 2, no. 1 (2024).

Sudwika Utama, I Putu Raditya, and Anak Agung Gede Agung Indra Prathama. "Pengawasan Bank Indonesia dan Otoritas Jasa Keuangan terkait Penerapan Financial Technology." *Yustitia* 16, no. 2 (2022): 172.

Suwondo, Denny. "The Legal Protection of Personal Data in Perspective of Human Rights." *Law Development Journal* 5, no. 4 (2023): 420.

Syahrudidin, Nurul Insi, dan Eva Achjani Zulfa. "Personal Data Protection Violations by Fintech Lending in Indonesia." *JLPH* 4, no. 4 (2024): 1000.

Yudiana, Teguh Cahya, et al. "The Urgency of Doxing on Social Media Regulation and the Implementation of Right to Be Forgotten on Related Content for the Optimization of Data Privacy Protection in Indonesia." *PJIH* 9, no. 1 (2022): 26.

Yolanda, E., and Hutabarat. "Urgensi Lembaga Perlindungan Data Pribadi di Indonesia Berdasarkan Asas Hukum Responsif." *Syntax Literate: Jurnal Ilmiah Indonesia* 8, no. 6 (2023)

Legislation

Law Number 27 of 2022 on the Protection of Personal Data, State Gazette of the Republic of Indonesia Number 196; Supplement to the State Gazette of the Republic of Indonesia Number 6820.

Law Number 1 of 2024 on the Second Amendment to Law Number 11 of 2002 on Electronic Information and Transactions, State Gazette of the Republic of Indonesia Number 1; Supplement to the State Gazette of the Republic of Indonesia Number 6905.

Financial Services Authority Regulation (POJK) Number 10/POJK.05/2022

Financial Services Authority Regulation (POJK) Number 77/POJK.01/2016

Websites

Akbar, Caesar. "6 Kasus Kebocoran Data Pribadi Di Indonesia ," accessed July 23, 2025, https://nasional.tempo.co/read/1501790/6-kasus-kebocoran-data-pribadi-di-Indonesia.

Ulya, Fika Nurul and Sakina Rakhma Diah Setiawan, "Data Nasabah KreditPlus Bocor Ini Kata OJK," accessed July 23, 2025, https://money.kompas.com/read/2020/08/04/170900526/data-nasabah-kreditplus-bocor-ini-kataojk.

Yonatan, Agnes z. "Indonesia Peringkat 4," accessed July 23, 2025, , https://data.goodstats.id/statistic/indonesia-peringkat-4-ini-dia-7-negara-pengguna-internet-terbesar-di-dunia-FLw6V.