

The Provision of Licensed Financial Technology Lending From The Perspective of Cyber Law and Criminal Law in Indonesia

Rizky Karo Karo, Teguh Prasetyo

Universitas Dirgantara Marsekal Suryadarma, Universitas Pelita Harapan
rizkykarokaro@unsurya.ac.id

Article Info

Received: 2025-04-19

Revised: 2025-06-23

Accepted: 2025-06-30

Keywords:

Legal Protection;
Criminal Sanctions for
FinTech Lending
Misconduct; Cyber Law
Framework for FinTech
Lending Operations

Abstract

This study undertakes an examination of the enforcement of legal provisions pertaining to licensed Financial Technology (FinTech) Lending, specifically from the vantage point of cyber law and criminal law. Furthermore, this article aims to provide an analytical framework and to educate users of FinTech lending regarding the legal liabilities that arise under both cyber law and criminal law within this domain. This research employed a normative juridical approach. The study exclusively utilized secondary data, comprising the 1945 Constitution, Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 regarding Information and Electronic Transactions (the ITE Law), and Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector (IL 4/2023). This data underwent a qualitative analysis. FinTech lending providers bear criminal liability should they be found to have committed criminal acts under the Electronic Information and Transactions Law (UU ITE). It is therefore incumbent upon these providers to conduct their electronic operations in strict adherence to the principles of cyber law. Furthermore, the Financial Services Authority (OJK) is empowered to impose administrative sanctions upon FinTech lending providers proven to have misused personal data, in accordance with Indonesia Law Number 4 of 2023.

I. Introduction

Legally recognized and licensed Financial Technology (FinTech) Lending significantly contributes to the growth of Micro, Small, and Medium-sized Enterprises (MSMEs) and benefits individuals across Indonesia. The Financial Services Authority (OJK) of the Republic of Indonesia, empowered by applicable laws, holds the authority to supervise, license, and impose administrative sanctions on FinTech lending entities it has authorized.

According to OJK, as of April 2025, online lending institutions have disbursed IDR 28.63 trillion in financing to the productive sector. Agusman, the Chief Executive of Supervision of Financing Institutions, Venture Capital Companies, Microfinance Institutions, and Other Financial Services Institutions (PVML) at OJK, stated on the Antara website (2025) that the proportion of financing from online peer-to-peer lending (LPBBTI or "pindar") to the productive sector and/or MSMEs reached 35.38 percent, or IDR 28.63 trillion, by April 2025. Most online lending providers serve both the productive and consumptive sectors, aligning with the financial products they offer (Liman, 2025).

As of March 2025, the outstanding financing for the peer-to-peer (P2P) lending industry—often referred to as "pindar"—demonstrated a year-on-year (yoy) growth of 28.72 percent, reaching a total of IDR 80.02 trillion. This figure slightly decreased from February 2025, when outstanding financing recorded a 31.06 percent yoy growth, amounting to IDR 80.07 trillion. The aggregate non-performing loan (NPL) ratio, known as TWP90, stood at 2.77 percent in March 2025, a marginal improvement from 2.78 percent in February 2025. In relation to minimum equity requirements, the Financial Services Authority (OJK) has issued OJK Regulation (POJK) Number 10/POJK.05/2022 concerning LPBBTI, which outlines these provisions. P2P lending providers are mandated to possess a minimum equity of IDR 12.5 billion, a requirement that becomes fully effective three years from the promulgation of the POJK. This obligation has been phased in, with providers required to meet a minimum equity of IDR 2.5 billion by July 2023, followed by IDR 7.5 billion by July 4, 2024, and finally, the full IDR 12.5 billion by July 4, 2025 (Khaerunnisa, 2025).

According to Harsasi, online peer-to-peer lending (LPBBTI) possesses five distinct characteristics: 1. Technological Foundation: LPBBTI operations are fundamentally reliant on information technology and are subject to all applicable legal provisions outlined in the Electronic Information and Transactions Law (UU ITE). 2. Profit-Driven Loan Agreements: The nature of these loan agreements is designed to provide financial benefit to the creditor through interest or, in accordance with sharia economic law, other forms of profit. These transactions are not structured as donations or for the purpose of receiving dividends. 3. Tripartite Involvement: Three parties are consistently involved in LPBBTI transactions: the creditor, the debtor, and the platform

provider. The provider is authorized to manage the entire LPBBTI process, draft agreements, and some providers even furnish debtor ratings. Additionally, providers earn a fee from the LPBBTI transactions they facilitate. 4. Dual Contractual Agreements: Due to the involvement of three parties, each LPBBTI legal action necessitates two distinct agreements: a loan agreement between the creditor and the debtor, and a management agreement between the creditor and the platform provider. 5. Prohibition on Guarantees: LPBBTI companies are expressly forbidden from providing any form of guarantee for the fulfillment of other obligations(Harsasi, 2020).

Using online peer-to-peer lending (LPBBTI) provides a fair solution for those who have difficulty accessing traditional banking services. LPBBTI helps achieve dignified justice by connecting funders with recipients through an electronic system, truly humanizing the process. For instance, as reported by Aman Sentosa, Head of the Department of Literacy, Financial Inclusion, and Communication, and quoted on CNBCIndonesia.com, 38.39% of the outstanding LPBBTI financing performance in May 2023, totaling Rp 51.46 trillion, was directed towards Micro, Small, and Medium-sized Enterprises (UMKM). This included disbursements of Rp 15.63 trillion to individual UMKM and Rp 4.13 trillion to UMKM business entities(Romys Binekasri, 2023).

Online Peer-to-Peer Lending (LPBBTI) platforms operate as Electronic System Providers (PSEs), utilizing electronic systems. The legal framework governing PSEs and electronic systems is primarily found in the Electronic Information and Transactions Law (UU ITE), read in conjunction with Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP PSTE). According to Article 1, Paragraph 6a of the UU ITE, in conjunction with Article 1, Paragraph 4 of the PP PSTE, an Electronic System Provider is defined as any individual, state organizer, business entity, or community group that provides, manages, and/or operates an Electronic System. This can be done independently or collaboratively, for their own needs or for the benefit of other parties using the Electronic System. Article 2, Paragraph (1) of the PP PSTE categorizes PSEs into two main types: Public Scope PSEs: These include: 1. State organizing agencies. 2. Agencies designated by state organizing agencies.

The Illegal Financial Activities Eradication Task Force (*Satuan Tugas Pemberantasan Aktivitas Keuangan Ilegal/Satgas PASTI*), formerly known as the Investment Alert Task Force, discovered 537 illegal online loan entities on various websites and applications between February and March 2024. Additionally, they identified 48 personal loan content offers and 17 entities engaging in illegal investment or financial activities that could potentially harm the public and violate personal data dissemination regulations.

The 17 entities offering illegal investment/financial activities were comprised of: 1. One entity committing fraud through a part-time job offer scheme requiring a deposit. 2. Thirteen entities offering unauthorized investments. 3. Two entities conducting

unauthorized cryptocurrency asset trading. 4. One entity engaged in unauthorized multi-level marketing trading. Following these findings, *Satgas PASTI* coordinated with its members to block the related applications and information. They also coordinated with law enforcement agencies for follow-up actions in accordance with applicable regulations. Since 2017 up to March 31, 2024, the task force has shut down 9,062 illegal financial entities, including 1,235 illegal investment entities, 7,576 illegal online loan entities, and 251 illegal pawnshop entities. *Satgas PASTI* reiterates its warning to the public to exercise caution, remain vigilant, and avoid using illegal online loans or personal loans, as they carry the potential for harm, including the risk of misuse of borrowers' personal data. From January to February 2024, *Satgas PASTI* has blocked 195 contact numbers of debt collectors from illegal online loans who were reported for making threats, intimidation, or other actions that contravene regulations. This blocking will continue in coordination with the Ministry of Communication and Informatics of the Republic of Indonesia to suppress the ecosystem of illegal online loans that continues to trouble the public. (Otoritas Jasa Keuangan Republik Indonesia, 2024).

Article 2, Paragraph (5), letter a of the PP PSTE outlines the criteria for private scope PSEs. This category includes Electronic System Providers that are regulated or supervised by a Ministry or Agency in accordance with prevailing laws and regulations. As such, privately managed Online Peer-to-Peer Lending (LPBBTI) platforms fall under this classification of private scope PSEs. Furthermore, Article 2, Paragraph (5), letter b of the PP PSTE expands the definition of private scope PSEs to encompass Electronic System Providers that operate online portals, websites, or applications used for the following purposes:

1. Providing, managing, or operating offerings or trading of goods and/or services.
2. Providing, managing, or operating financial transaction services.
3. Delivering paid digital content or materials via data networks, whether through downloads from portals or websites, email delivery, or other applications to user devices.
4. Providing, managing, or operating communication services. This includes, but isn't limited to, text messages, voice calls, video calls, email, and online conversations in the form of digital platforms, social networking services, and social media.
5. Operating search engine services and providing Electronic Information in various formats such as text, audio, images, animations, music, video, films, games, or any combination thereof.
6. Processing Personal Data for operational activities that serve the public and are related to Electronic Transactions.

The central research question of this study is: How can the operation of licensed financial technology lending (FinTech lending) be analyzed from the perspective of cyber law and criminal law in Indonesia? Our primary objective is to critically analyze the application of cyber law and criminal law to licensed FinTech lending in Indonesia. We also aim to educate readers that FinTech providers bear legal accountability and are obligated to provide consumer protection.

This research provides an analytical discussion of cyber law and criminal law as a new area of study. The rapid development of fintech lending, particularly online loans (*pinjol*), has created a significant novelty in legal research, specifically in the integration of cyber law and criminal law. Current research no longer focuses solely on civil law aspects but also examines how technology is leveraged to commit crimes and how criminal law can be used to prosecute the perpetrators. The novelty in this research lies in the shift from treating these issues as mere civil disputes (breach of contract) between debtors and creditors to classifying them within the realm of criminal offenses. This demonstrates that the problems associated with both illegal and legal online loans are not just a matter of civil debt but also serious crimes that cause widespread harm to the public.

2. Research Method

This research aims to analyze a given problem using a defensible and rigorous research methodology (Faradiba & Yuniarti, 2021). The research employed a normative legal method. This approach involves analyzing secondary data, which includes primary, secondary, and tertiary legal materials. The purpose of this analysis is to identify and examine the gaps or discrepancies between legal issues and existing written regulations (R. K. Karo, 2025). Primary legal materials consist of applicable statutory regulations directly relevant to the research topic, which are then subjected to qualitative analysis (Budianto, 2020). Legal research can be conducted using a conceptual approach, which involves analyzing legal principles (Rahmat et al., 2024; Sujono et al., 2024).

In this scholarly work, the primary legal materials used are: 1. Indonesia Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 regarding Electronic Information and Transactions (ITE Law); 2. Indonesia Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector (DSFC Law); 3. Indonesia Law of the Republic of Indonesia Number 27 of 2022 concerning Personal Data Protection (PDP Law) (Susantijo, 2025; Tanaya & Zai, 2021). The secondary legal materials include published academic journal articles, research reports, and draft legislation. Meanwhile, tertiary legal materials consist of legal dictionaries. These three types of legal materials are processed, categorized, and

analyzed in relation to relevant articles and legal principles. The author employed a qualitative analysis of the legal materials, and conclusions were drawn using a deductive method.

In conducting this research, the author has utilized the ITE Law, DSFC Law, and PDP Law due to their consistency and provision of constitutional guarantees for legal fintech operators, as well as consumer protection for users. The research employs a statutory approach, analyzing relevant norms, and a conceptual approach. This study will analyze how contracts are automatically executed within fintech systems. This approach focuses on how traditional consumer protection concepts, such as information disclosure and dispute resolution, can be applied within a digital environment. Key issues under scrutiny include data privacy, cybersecurity, and the potential for digital fraud.

3. Results and Discussion

Fintech Lending Operations in Indonesia: A Cyber Law Perspective

Cyber law, a term derived from "cyberspace law," encompasses legal aspects pertaining to individuals or legal subjects who use and leverage internet technology. Its scope begins the moment one goes online and enters cyberspace. This field of law addresses a wide range of issues arising from activities within the digital realm.(Sahat Maruli T. Situmeang, 2020). Cyber law is essential because internet-based cyber activities transcend national territorial boundaries and can occur at any time. Even though the evidence for these activities is virtual and electronic, cyber activities are virtual acts with real-world consequences(Ramli, 2006).

The researcher analyzed the norms of the Singapore Payment Services Act against legal fintech regulations in Indonesia. The Payment Services Act (PSA) in Singapore and fintech regulations in Indonesia, which are governed by Bank Indonesia (BI) and the Financial Services Authority (OJK), have distinct approaches but share a common objective: to establish a robust legal framework for digital payment services. Singapore employs a singular and comprehensive approach through the PSA, whereas Indonesia has adopted a multi-regulator, fragmented framework tailored to specific service types. The Payment Services Act (PSA) 2019 of Singapore represents a modern and comprehensive legal framework, providing regulatory clarity and fostering innovation within the fintech sector. Its primary benefit is the activity-based approach that unifies regulations for various payment services under a single act. The act also ensures strong consumer protection by mandating that large payment institutions hold customer funds separately (fund segregation) in a trust or bank account. This measure serves to safeguard customer funds in the event of a company's insolvency (Republic Of Singapore Government Gazette Acts Supplement, 2019).

In Singapore, the principles of the data protection act apply to all marketing activities that involve the collection, use, or disclosure of personal data. Before an organization can collect, use, or disclose an individual's data, it must obtain their explicit consent and provide a data protection notice. However, there are exceptions to this rule, such as when the data is used for vital interests, matters of public interest, or legitimate business interests. Personal data collection and processing must adhere to a core principle: the data must be collected for specific and lawful purposes, processed fairly and legally, and maintained as accurate and relevant (Sholehuddin et al., 2024).

The researcher's analysis utilizes the theory of regulatory compliance and cybercrime prevention frameworks. According to Teguh Prasetyo, the purpose of regulatory compliance is to deliver justice, and its implementation is carried out by all parties, both private and governmental. The theory of regulatory compliance is intrinsically linked to the principle of legality. Legal compliance theory endeavors to explain why individuals or organizations adhere to the law, positing that compliance is a rational choice. Individuals comply with the law when the benefits of compliance outweigh the costs of violation. (R. P. K. Karo & Prasetyo, 2020; Prasetyo, 2018). The researcher asserts that Regulatory Compliance Theory explains why an entity, such as a fintech company, adheres to regulations enacted by the government. This theory views compliance not merely as a legal obligation but also as a business strategy. Compliance is further driven by pressures from the social and industrial environment. Fintech companies comply to gain legitimacy, consumer trust, and recognition from stakeholders, including investors and business partners. A company that is registered and supervised by the OJK (Financial Services Authority) automatically receives a "seal" of trust. Compliance is also influenced by the decisions and culture implemented by a company's management. Proactive management that fosters a culture of compliance and invests in regulatory technology (RegTech) will achieve a higher level of compliance, even exceeding minimum requirements.

Cyber law is rapidly evolving in Indonesia. This dynamic field is guided by four core principles: 1. Principle of Legality: Cyber law operates strictly in accordance with prevailing Indonesian regulations, ranging from national statutes to implementing regulations, ministerial decrees, and head of agency regulations. 2. Principle of Enforceability: All cyber activities in Indonesia must consider the effectiveness of cyber law and the practical use of technology within society. This ensures that legal frameworks are not only theoretically sound but also practically implementable. 3. Principle of Transparency: Parties involved in cyber activities are obligated to uphold transparency. This fosters mutual trust and ensures clear communication in the digital realm. 4. Principle of Accountability: Providers operating under cyber law bear significant responsibility. They are subject to criminal, civil, and cyber liability if proven to have committed prohibited acts (KARO, 2024; R. P. K. Karo & Prasetyo, 2020).

The connection between cyber law and the operation of FinTech lending (online loans) in Indonesia is incredibly close and crucial. Since FinTech lending operates entirely in the digital realm, every aspect of its functions relies heavily on electronic systems and data. As a result, cyber law is essential for regulating and safeguarding these online activities. P2P (peer-to-peer) lending platforms state that their purpose is to digitally link investors and borrowers. The goal is to let lenders earn a return on their money while providing loans to individuals who can't get credit from traditional banks. However, as the technology behind these platforms has grown more complex, it has also created new opportunities for unethical behavior or moral hazards (Suryono et al., 2021). Financial Technology (FinTech) has played a crucial role in transforming the landscape of financial services in Indonesia. By extending access to financial services for previously underserved populations, FinTech has successfully enhanced financial inclusion across the nation. Innovations such as digital payments and peer-to-peer (P2P) lending have enabled marginalized segments of society to participate in the formal financial system, which ultimately contributes to a reduction in social inequality and fosters more inclusive economic growth. However, despite the numerous opportunities FinTech presents, the industry also confronts significant challenges, particularly concerning regulation and data security (Jange et al., 2024).

The legal relationship between lenders and borrowers in FinTech lending is established through electronic agreements (e-contracts). In Indonesia, the primary legal basis for electronic contracts is Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 regarding Electronic Information and Transactions (the ITE Law). According to this law, an Electronic Contract is defined as an agreement between parties created through an Electronic System.

Fintech lending offers substantial advantages in Indonesia, making financing more accessible and convenient for many. Benefits of Fintech Lending, First, you can apply for small loan amounts, sometimes as low as Rp100,000. This is incredibly helpful for immediate, minor needs. Second, it's very practical; prospective borrowers simply need a smartphone to upload their ID (KTP), take a selfie, and fill in personal details. Third, the interest rates provided by online peer-to-peer lending (LPBBTI) providers are competitive with other platforms, and the OJK doesn't impose a fixed interest rate. Fourth, the loan duration for LPBBTI is typically short, which makes sense given the smaller loan amounts. Fintech lending platforms offer both consumptive and productive loans. Consumptive loans usually have a faster repayment tenor since they're used for consumer goods like gadgets or clothing. Productive loans, however, vary in duration and structure, tailored to the borrower's specific business model. Despite the benefits, LPBBTI operations do carry risks, particularly concerning non-performing loans or defaults. If a borrower defaults, the lender might not recoup their invested funds. It's also worth noting that loans with higher interest rates tend to have

a higher risk rating, indicating a greater chance of default. Conversely, lower-interest loans generally carry a lower risk.

Electronic contracts, especially in fintech lending, often contain standard clauses. Because of this, fintech lending providers must follow cyber law and the principle of legality as outlined in Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector (DSFC LAW).

According to Article 238 paragraph (4) of the DSFC LAW , when Financial Sector Business Actors (PUSK) create and use standard agreements with standard clauses, these clauses are prohibited from containing the following:

- 1) Shifting Responsibility: Clauses that transfer the responsibility or obligations of the PUSK to the Consumer.
- 2) Unilateral Authorization: Clauses granting the PUSK, directly or indirectly, the power to take unilateral actions on assets mortgaged by the Consumer, unless such actions are permitted by law.
- 3) Burden of Proof on Consumer: Clauses that require the Consumer to provide proof if the PUSK claims that the loss of utility of products and/or services purchased by the Consumer is not the PUSK's responsibility.
- 4) Reducing Product/Service Utility: Clauses that give the PUSK the right to reduce the utility of products and/or services or diminish the Consumer's assets that are the subject of the product and service agreement.
- 5) Authorization for Encumbrance: Clauses stating that the Consumer authorizes the PUSK to impose mortgage rights, pledge rights, or security rights on products and/or services purchased by the Consumer on an installment basis.
- 6) Unilateral Amendments: Clauses stating that the PUSK can unilaterally add, change, and/or provide further rules after the agreement has been approved/agreed upon.
- 7) Consumer Submission to Unilateral Changes: Clauses stating that the Consumer is subject to unilateral changes by the PUSK to the rules mentioned in point (f) after the agreement has been signed by the Consumer.
- 8) Avoiding or Limiting Clause Applicability: Clauses granting the PUSK authority to avoid or limit the applicability of a clause.
- 9) Unilateral Interpretation: Clauses stating that the PUSK has the authority to interpret the meaning of the agreement unilaterally.

- 10) Limiting Employee/Third-Party Liability: Clauses stating that the PUSK limits liability for errors and/or negligence of employees and/or third parties acting on behalf of the PUSK.
- 11) Restricting Consumer's Right to Sue: Clauses limiting the Consumer's right to sue the PUSK in the event of a dispute related to the agreement.
- 12) Limiting Admissible Evidence: Clauses limiting the evidence that can be provided by the Consumer when a dispute related to the agreement arises.

Cyber law mandates that electronic system providers maintain the confidentiality and protection of personal data (R. P. P. K. Karo, 2022). The Indonesian government requires all parties, including businesses and government agencies, to safeguard the personal data they process and manage. This means personal data can only be used for specific purposes and cannot be misused (Tan et al., 2025).

In 2022, the Indonesian Government enacted Law Number 27 of 2022 concerning Personal Data Protection (PDP LAW). Licensed Fintech lending providers engage in the processing of personal data, which, according to Article 16, Paragraph (1) of the PDP LAW, includes the following activities: a. Acquisition and collection; b. Processing and analysis; c. Storage; d. Correction and updating; e. Display, announcement, transfer, dissemination, or disclosure; f. Deletion or destruction.

Indonesia's Personal Data Protection Law (PDP LAW) clearly defines personal data as "data about an individual who is identified or can be identified, either separately or combined with other information, whether directly or indirectly, through electronic or non-electronic systems." As technology has advanced and become more integrated into our daily lives, a new type of consumer has emerged. These users are no longer passive recipients of technology; they are now more knowledgeable and sophisticated. They have greater access to information, which fuels their curiosity about the devices they use. Consequently, they have higher expectations for how these products should function and what their rights are as users (Coiduras-Sanagustín et al., 2024).

While the Electronic Information and Transactions Law (UU ITE) doesn't offer a specific definition for personal data, any personal information—from either funders or recipients—entered into an LPBBTI (online peer-to-peer lending) electronic system is considered electronic information. The UU ITE, in Article 1, Paragraph 1, defines electronic information broadly as "one or a collection of electronic data, including but not limited to writing, sound, images, maps, designs, photographs, electronic data interchange (EDI), electronic mail, telegrams, telex, telecopies or the like, letters, signs, numbers, access codes, symbols, or perforations that have been processed and have meaning or can be understood by those capable of understanding them."

Indonesia's Personal Data Protection Law (PDP LAW), specifically Article 16,

Paragraph (2), outlines the crucial principles that govern the processing of personal data. These principles ensure data is handled responsibly and ethically:

- 1) **Limited and Specific Collection:** Personal data must be collected in a way that's restricted to what's necessary, legally sound, and completely transparent.
- 2) **Purpose-Driven Processing:** Any processing of personal data must strictly align with its stated purpose.
- 3) **Guaranteeing Data Subject Rights:** The processing of personal data must always uphold the rights of the individual data subject.
- 4) **Accurate and Up-to-Date Data:** Personal data needs to be processed accurately, completely, without misleading information, kept current, and be fully accountable.
- 5) **Ensuring Data Security:** Protecting personal data from unauthorized access, disclosure, alteration, misuse, damage, and/or loss is paramount during processing.
- 6) **Transparent Processing Information:** The purpose and activities of data processing, along with any failures in data protection, must be clearly communicated.
- 7) **Timely Deletion or Destruction:** Personal data must be deleted and/or destroyed once its retention period ends or when requested by the data subject, unless other laws dictate otherwise.
- 8) **Accountable and Demonstrable Processing:** All personal data processing must be conducted responsibly and be clearly demonstrable.

Even if someone agrees to their data being used, laws on data protection still require fairness and openness. This means that companies handling personal data, whether they collect it (data controllers) or process it (data processors), must use proper organizational and technical methods to keep that data secure and private. These laws also acknowledge and uphold the rights of the individual whose data is being used (data subject). They specify in detail what rights a data subject has. For example, a data subject can access their data held by these companies. They also have the right to correct, delete, or block their personal data if it's found to be incorrect, incomplete, outdated, or handled illegally (Shahrullah et al., 2024).

The researcher argues that for legal fintech companies, the implementation of the PDP Law necessitates substantial investment in technological infrastructure and cybersecurity. Companies are obligated to implement adequate security measures, conduct periodic audits, and appoint a Data Protection Officer. The PDP Law establishes strict criminal sanctions to deter personal data violations. These sanctions apply to any person who unlawfully commits a prohibited act. For instance, concerning

the unlawful disclosure of personal data, an offender who unlawfully reveals personal data that does not belong to them can face imprisonment for a maximum of four years and/or a fine of up to Rp4 billion (Article 65, paragraph 2, of the PDP Law).

Criminal Liability of Licensed Fintech Lending Providers in Indonesia for Personal Data Misuse

In our opinion, Licensed FinTech lending providers are authorized to process and manage data in accordance with current laws. However, if these providers misuse personal data, they can face criminal liability. Legally recognized FinTech lending platforms are constantly collecting and processing data. We recommend that these providers use electronic systems that are highly secure, reliable, and frequently audited to ensure data integrity and user trust. Protecting data privacy is crucial for upholding the right to privacy, and this protection must begin with legal certainty. Therefore, guarantees for data privacy should be enshrined in the highest legal instrument of a country: its Constitution. The Constitution, as the supreme law, provides the strongest foundation for legal certainty, a principle that is essential for effective law enforcement in any nation. By embedding this right in its Constitution, a country demonstrates its core values, legal system, and governance approach.(Natamiharja, 2019). Licensed Fintech providers are, by their nature, corporations or companies. When a company commits a legal violation, its legal accountability generally follows a specific pattern. Corporate Criminal Liability, First, when an environmental crime is committed by, for, or on behalf of a business entity, both the business entity itself and/or the individual who ordered the criminal act, or the person acting as the leader of the criminal activity, will face criminal charges and sanctions(Hajairin et al., 2021).

Businesses and electronic system providers can collect personal data from customers or potential customers both offline and online. This digital data can unfortunately be sold without the owner's knowledge or consent, or it can be misused for purposes beyond what was originally intended. It's also possible for connected personal data to be hijacked or stolen (hacked) by third parties. The misuse of personal data highlights weaknesses in systems and a lack of oversight, leading to potential harm for the data owner. Misuse, theft, or sale of personal data is a legal violation in the field of information technology and can also be considered a violation of human rights, as personal data is a fundamental human right that must be protected. The misuse of personal data fulfills the elements of criminal acts such as theft and fraud, as well as other criminal offenses, from both objective and subjective perspectives. Given these elements are met, administrative, civil, and even existing criminal sanctions may not be enough to fully address the crime of personal data misuse, which is, in reality, a complete form of crime in itself(Sahat Maruli Tua Situmeang, 2021).

Chairul Huda posits that the foundation of a criminal act lies in the principle of

legality, while the culpability of the perpetrator is based on fault. This essentially means an individual incurs criminal liability when they commit an act that is both wrong and contrary to law. In essence, criminal liability serves as a mechanism to respond to the violation of specific, agreed-upon prohibited acts(Huda, 2006).

In the context of criminal law, "fault", as part of *mens rea*, refers to breaching a rule or violating statutory regulations. Anyone who infringes upon a law is obligated to take responsibility for their actions. This concept of fault, as an element of accountability, serves as both a safeguard for individuals and a control over personal freedom in relation to others. This guarantee protects individuals from the unlawful actions of others. It also acts as a control because anyone who commits a criminal offense is burdened with criminal liability. Criminal liability means that the objective blameworthiness inherent in a criminal act is subjectively extended to an individual who meets the criteria for being punished for that act. The foundation of a criminal offense lies in the principle of legality, while the basis for punishing the perpetrator is the principle of fault. Accountability is the means by which it's determined whether someone will be penalized for a criminal act that has occurred. To establish criminal liability, several elements must be met to assert that an individual can be held accountable(Hiariej, 2016).

The application of the principle of proportionality in criminal law aims to achieve a balance between the interests of the offender, the victim, and society (Situmorang et al., 2025). The misuse of personal data from electronic system users often involves hacking, where perpetrators illegally access databases. Once they obtain personal data such as usernames, National Identity Card (NIK) numbers, family card numbers, places and dates of birth, mobile phone numbers, and even names of family members, this information is then sold on online marketplaces. The buying and selling of personal data is highly susceptible to misuse for other activities that can harm the personal data owner. The right to privacy has significant implications: it is the right to have an undisturbed private life, the right to communicate with others without being spied on, and the right to control access to information about one's direct life and personal data(Faisal & Indriani, 2022). The Personal Data Protection Law (PDP LAW) in Indonesia establishes clear criminal provisions for individuals proven to have committed prohibited acts related to personal data. These prohibitions are detailed in Article 65 of the PDP LAW:

- a) Article 65, Paragraph (1) of the PDP LAW states: "Any Person is prohibited from unlawfully obtaining or collecting Personal Data that does not belong to them with the intent to benefit themselves or another person, which may result in harm to the Personal Data Subject."

- b) Article 65, Paragraph (2) of the PDP LAW states: "Any Person is prohibited from unlawfully disclosing Personal Data that does not belong to them."
- c) Article 65, Paragraph (3) of the PDP LAW states: "Any Person is prohibited from unlawfully using Personal Data that does not belong to them."

The criminal penalties for individuals who misuse personal data are as follows:

- a) Article 67, Paragraph (1) of the PDP LAW stipulates that "Any Person who intentionally and unlawfully obtains or collects Personal Data that does not belong to them with the intent to benefit themselves or another person, which may result in harm to the Personal Data Subject as referred to in Article 65, Paragraph (1), shall be punished with imprisonment for a maximum of 5 (five) years and/or a maximum fine of IDR 5,000,000,000.00 (five billion Rupiah)"
- b) Article 67, Paragraph (2) of the PDP LAW states that "Any Person who intentionally and unlawfully discloses Personal Data that does not belong to them as referred to in Article 65, Paragraph (2), shall be punished with imprisonment for a maximum of 4 (four) years and/or a maximum fine of IDR 4,000,000,000.00 (four billion Rupiah)."
- c) Article 67, Paragraph (3) of the PDP LAW provides that "Any Person who intentionally and unlawfully uses Personal Data that does not belong to them as referred to in Article 65, Paragraph (3), shall be punished with imprisonment for a maximum of 5 (five) years and/or a maximum fine of IDR 5,000,000,000.00 (five billion Rupiah)."

The Personal Data Protection Law (PDP LAW) also extends criminal liability to corporations. Under Article 70, Paragraph (1) of the PDP LAW, penalties for corporate offenses can be imposed on the management, controlling parties, those who give orders, beneficial owners, and/or the corporation itself. The only type of penalty that can be levied against a corporation is a fine. This fine can be up to 10 (ten) times the maximum criminal fine threatened for the offense. Beyond just fines, under Article 70, Paragraph (4) of the Personal Data Protection Law (PDP LAW), corporations can also face additional penalties. These include: 1. Forfeiture of profits and/or assets gained from the criminal act. 2. Freezing all or part of the corporation's business operations. 3. Permanent prohibition from engaging in specific activities. 4. Closure of all or part of the corporation's business premises and/or activities. 5. Fulfilling neglected obligations. 6. Paying compensation for damages. 7. Revocation of permits. 8. Dissolution of the corporation. In the context of data privacy violations, particularly concerning personal data, a "complaint offense" means that prosecution can only proceed if the aggrieved party or their representative files an official complaint. In other words, the wronged individual must actively report the incident to the authorities for legal action to be taken

against the perpetrator.

This approach—where personal data privacy breaches are considered a complaint offense—is adopted in some jurisdictions. This implies that if someone's personal data is misused or stolen, the affected individual must initiate the legal process by filing a complaint with the authorities to pursue the offender. However, it's important to note that in other jurisdictions, personal data privacy violations are treated as a "delik biasa" or "ordinary offense," allowing authorities to prosecute the perpetrator even without a formal complaint from the victim (Muzairoh et al., 2024). Concerning the concept of a criminal corporation, it is characterized by its intentional establishment for the commission of criminal acts. In this context, the corporation serves solely as a mechanism to veil or disguise the actual illicit enterprise, functioning as a mere artifice to conceal the true entities responsible. It is essential to delineate the differences among crimes committed against a corporation, corporate crimes, and criminal corporations, a distinction predicated on the respective subject matters and their resultant effects. Whereas the initial two categories designate the companies or corporations themselves as the primary subjects, a criminal corporation involves the perpetration of offenses by external parties, wherein the corporation acts as an ancillary tool. The resulting consequences shall be calibrated in proportion to the function performed by the subject. Therefore, an augmented number of perpetrators in the commission of the crime will invariably lead to an amplification of the consequences (Budianto, 2022).

4. Conclusion

Licensed fintech lending in Indonesia stands at a crucial intersection of digital financial innovation, consumer protection, and law enforcement. From a cyber law perspective, the existing regulatory framework—especially the Electronic Information and Transactions Law (UU ITE) and the Personal Data Protection Law (PDP LAW) have pivotal role. These regulations ensure that licensed online lending operations guarantee the security of electronic systems, the confidentiality of personal data, and the validity of electronic contracts. It's absolutely essential for providers to implement adequate technical and organizational measures to protect user data from breaches and misuse, even when users have given explicit consent. The PDP LAW sets out clear penalties for individuals who commit prohibited acts related to personal data. These prohibitions are detailed in Article 65 of the PDP LAW: a. Article 65, Paragraph (1) of the PDP LAW forbids anyone from unlawfully obtaining or collecting Personal Data that isn't theirs, with the intent to benefit themselves or others, which could harm the Personal Data Subject. B. Article 65, Paragraph (2) of the PDP LAW prohibits anyone from unlawfully disclosing Personal Data that isn't theirs. C. Article 65, Paragraph (3) of the PDP LAW makes it unlawful for anyone to unlawfully use Personal Data that isn't theirs.

The harmonization of cyber and financial regulations refers to the concerted effort to align rules across the technology and financial sectors to create a cohesive framework. In the context of FinTech, particularly online lending, the objective is to ensure that technological innovation progresses in tandem with robust data security and the stability of the financial system. Specifically, the Financial Services Authority (OJK) endeavors to create regulations that govern not only financial aspects, such as interest rates and capitalization, but also technological aspects, including cybersecurity and personal data protection. This is crucial because a risk in one sector can quickly spill over into another. For instance, a cyberattack on a FinTech platform could lead to substantial financial losses for investors and disrupt market stability. The OJK recognizes that poor data governance is one of the greatest risks within the FinTech industry. The OJK should therefore establish standards aimed at protecting consumers' personal data and fostering public trust. These standards could include Technical and Procedural Standards, such as Data Encryption, which involves implementing encryption to protect user data both at rest and in transit; Restricted Access, which ensures that only authorized personnel can access sensitive data; and Emergency Response Procedures, which entails having a clear plan to address cybersecurity incidents or data breaches.

References

- Budianto, A. (2020). Legal Research Methodology Reposition in Research on Social Science. *International Journal of Criminology and Sociology*, 9, 1339–1346.
- Budianto, A. (2022). The Corporate Crime as The Power of Crime in The Economic Justification. *SASI*, 28(4), 506–520. <https://doi.org/https://doi.org/10.47268/sasi.v28i4.890>
- Coiduras-Sanagustín, A., Manchado-Pérez, E., & García-Hernández, C. (2024). Understanding perspectives for product design on personal data privacy in internet of things (IoT): A systematic literature review (SLR). *Heliyon*, 10(9).
- Faisal, B. I., & Indriani, D. E. (2022). Pertanggung Jawaban Pidana UU ITE Terhadap Pembobolan Data Pribadi di Era Serba Digital. *Civic-Culture: Jurnal Ilmu Pendidikan PKn Dan Sosial Budaya*, 6(2), 652–661.
- Faradiba, F., & Yuniarti, E. (2021). Thermodynamic Concepts on Efficiency of Aircraft Engines. *Physical Science Internasional Journal*, 24(11), 43–49.
- Hajairin, Sanusi, G., & Ma'arij, A. (2021). Pertanggungjawaban Pidana Terhadap Kerusakan Lingkungan Akibat Pengolahan Material Oleh PT Tukad Mas Kota Bima. *SASI*, 27(3), 267–276. <https://doi.org/https://doi.org/10.47268/sasi.v27i3.475>
- Harsasi, S. (2020). *Aspek Yuridis Layanan Pinjam Meminjam Uang Berbasis Teknologi*

- Informasi (LPMUBTI) Di Indonesia*. Disertasi Program Studi Doktor Hukum Universitas Pelita Harapan.
- Hiariej, E. O. S. (2016). *Prinsip-prinsip hukum pidana*. Cahaya Atma Pustaka.
- Huda, C. (2006). *Dari Tindak Pidana Tanpa Kesalahan Menuju Kepada Tiada Pertanggung jawab Pidana Tanpa Kesalahan* (2nd ed.). Kencana.
- Jange, B., Pendi, I., & Susilowati, E. M. (2024). Peran Teknologi Finansial (Fintech) dalam Transformasi Layanan Keuangan di Indonesia. *Indonesian Research Journal on Education*, 4(3), 1199–1205.
- KARO, : RIZKY PRATAMA PUTRA KARO. (2024). *PENGUATAN PERATURAN TENTANG LAYANAN PENDANAAN BERSAMA BERBASIS TEKNOLOGI INFORMASI BERDASARKAN KEADILAN BERMARTABAT*. UNIVERSITAS PELITA HARAPAN.
- Karo, R. K. (2025). *Pengantar Metodologi Penelitian Hukum Di Era Digital* (1st ed.). RajaGrafindo Persada.
- Karo, R. P. K., & Prasetyo, T. (2020). *Pengaturan Perlindungan Data Pribadi Di Indonesia: Perspektif Teori Keadilan bermartabat*. Nusa Media.
- Karo, R. P. P. K. (2022). Borrower's right to a sense of security in illegal peer to peer lending in Indonesia perspective of dignified justice theory. *Journal of Legal, Ethical and Regulatory Issues*, 25(4), 1–10.
- Khaerunnisa, R. (2025). *Pindar tetap berpotensi tumbuh positif pada kuartal mendatang*. <https://www.antaraneews.com/berita/4844233/pindar-tetap-berpotensi-tumbuh-positif-pada-kuartal-mendatang>
- Liman, U. S. (2025). *OJK: Pembiayaan produktif "fintech lending" Rp28,63 triliun per April*. <https://www.antaraneews.com/berita/4878029/ojk-pembiayaan-produktif-fintech-lending-rp2863-triliun-per-april>
- Muzairoh, E., Suharso, Noviasari, D. T., & Syafingi, H. M. (2024). Analisis Perlindungan Hukum Terhadap Privasi Data Pribadi di Era Digital dalam Prespektif Hak Asasi Manusia. *BOROBUDUR LAW AND SOCIETY JOURNAL*, 3(1), 31–36. <https://doi.org/https://doi.org/10.31603/11824>
- Natamiharja, R. (2019). Perlindungan Data Privasi dalam Konstitusi Negara Anggota ASEAN. In *HAK KONSTITUSIONAL: TEBARAN PEMIKIRAN DAN GAGASAN*. CV. Anugrah Utama Raharja.
- Otoritas Jasa Keuangan Republik Indonesia. (2024). *Satgas Pasti Blokir 585 Pinjol Ilegal dan Pinpri serta 17 Investasi Ilegal*. <https://ojk.go.id/id/berita-dan-kegiatan/info-terkini/Pages/Satgas-Pasti-Blokir-585-Pinjol-Ilegal-dan-Pinpri-serta-17-Investasi-Ilegal.aspx>
- Prasetyo, T. (2018). *Keadilan Bermartabat: Perspektif Teori Hukum*. RajaGrafindo Persada.
- Rahmat, D., Sudarto, Sarip, Sujono, & Aziz, M. F. (2024). The Urgency of Administrative Law in Light of Ius Constituendum Regarding the Role of Village Heads. *Volksgeist*:

- Jurnal Ilmu Hukum Dan Konstitusi*, 7(1), 53–67.
- Ramli, A. M. (2006). *Cyber Law dan HAKI Dalam Sistem Hukum Indonesia*. Bandung. REPUBLIC OF SINGAPORE GOVERNMENT GAZETTE ACTS SUPPLEMENT, (2019).
- Romys Binekasri. (2023). *UMKM Lebih Suka Pinjam Dana Lewat Pinjol, Ini Data OJK*. <https://www.cnbcindonesia.com/market/20230710055410-17-452655/umkm-lebih-suka-pinjam-dana-lewat-pinjol-ini-data-ojk>
- Shahrullah, R. S., Park, J., & Irwansyah. (2024). Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment. *Hasanuddin Law Review*, 10(1), 1–20. <https://doi.org/http://dx.doi.org/10.20956/halrev.v10i1.5016>
- SHOLEHUDDIN, N., MISKAM, S., SHAHWAHID, F. M., AZIZ, T. N. R. A., & MANSOR, N. (2024). A Comparative Legal Analysis on Personal Data Protection Laws in Selected ASEAN Countries. *Journal of Muwafaqat*, 7(1), 23–38.
- Situmeang, Sahat Maruli T. (2020). *CYBER LAW* (1st (ed.)). CV.Cakra.
- Situmeang, Sahat Maruli Tua. (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber. *SASI*, 27(1), 38–52. <https://doi.org/https://doi.org/10.47268/sasi.v27i1.394>
- Situmorang, A. M., Kurniawan, I. G. A., & Darma, I. M. W. (2025). Implementation of the Principle of Proportionality in Criminal Sentencing in Indonesia. *PENA JUSTISIA: MEDIA KOMUNIKASI DAN KAJIAN HUKUM*, 24(2), 127–140.
- Sujono, Sudarto, & Putra, H. A. (2024). ANALISIS PENERAPAN RESTORATIVE JUSTICE OLEH KEJAKSAAN REPUBLIK INDONESIA DALAM BINGKAI ARAH PEMBAHARUAN POLITIK HUKUM PIDANA DI INDONESIA. *Jurnal Rectum*, 6(3), 551–564.
- Suryono, R. R., Budi, I., & Purwandari, B. (2021). Detection of fintech P2P lending issues in Indonesia. *Heliyon*, 7(4).
- Susantijo, S. (2025). A Human Rights Perspective on Granting Privileges to Descendants of PKI in Indonesia. *Fiat Justisia: Jurnal Ilmu Hukum*, 19(1), 1–20. <https://doi.org/10.25041/fiatjustisia.v19no1.3711>
- Tan, W., Karo, R. P. P. K., Situmeang, A., Rusdiana, S., Siti, & Razak, S. A. (2025). Protection of Public Services Personal Data in The Delivery of Public Services: Comparative Study in Indonesia and Malaysia. *SASI*, 31(1), 33–43. <https://doi.org/https://doi.org/10.47268/sasi.v31i1.2415>
- Tanaya, V., & Zai, J. A. (2021). PENERAPAN PEMBATAHAN SOSIAL BERSKALA BESAR (PSBB) AKIBAT PANDEMI CORONAVIRUS DISEASE 2019 (COVID-19) SEBAGAI FORCE MAJEURE DALAM KONTRAK. *Law Review*, XXI(1), 97–116.