

Shielding Privacy: Navigating Personal Data Protection Law in Indonesian Fintech Peer-to-Peer Lending

Hendri Khuan

hendri.khuan@gmail.com

Borobudur University, Jakarta, Indonesia

Abstract. The Indonesian P2P Lending fintech industry is growing rapidly, raising concerns about personal data protection due to the extensive collection of sensitive information. This article focuses on the regulatory landscape, especially the Personal Data Protection (PDP) Law, which aims to protect digital privacy. This study examines data management practices in Indonesian P2P Lending fintech platforms, explains the legal protection for personal data under Indonesian law, and explores the legal remedies for P2P Lending fintech users in cases of data breaches. Using a normative legal approach and descriptive legal analysis, this study uses a qualitative study to identify critical legal provisions, clarify their implications, and propose improvements. Personal data protection in Indonesian P2P Lending fintech is regulated by various regulations such as the ITE Law, the P2SK Law, the PDP Law, and POJK 10/2022. Legal protection includes preventive and repressive measures. Users can seek non-judicial or judicial remedies in the event of a data breach. This study aims to provide a comprehensive source of information for industry stakeholders, regulators, and parties interested in fintech, data protection, and Indonesian law.

Keywords: Legal Protection, Legal Certainty, Personal Data Protection, Fintech Law, Cyberlaw Indonesia Cyber Law Conference – 2023

1 Introduction

Fintech P2P Lending services, with their innovative and user-friendly platform, have enabled individuals and businesses to enjoy greater convenience and efficiency in financial transactions. FinTech is acknowledged as a critical driver for advancing financial inclusion and expanding access to the formal financial system for those currently underbanked, thereby promoting more equitable economic growth.[1] The global FinTech industry has encountered remarkable growth in recent years, with peer-to-peer lending being one of the prominent sectors, also called Information Technology-based Co-Funding Services (LPBBTI).[2] Technology-driven innovation has already demonstrated its advantages for Fintech business models and services, serving as a means to address risks.[3] The business model of Fintech

P2P Lending services facilitates lending and borrowing transactions or funding, bringing together Lenders and Borrowers directly through digital platforms based on information technology. The money lent or channeled belongs to the lender, not the P2P lending platform. The primary target recipients of funds are unbankable and underserved communities for productive and consumptive needs. General characteristics of Fintech P2P Lending provider companies include straightforward requirements with a speedy loan disbursement process and without time and place restrictions. Fintech P2P lending has introduced new services for clientele groups lacking a solid credit history and small business owners who may not possess suitable collateral or have enough personal assets or business experience.[4] The P2P Lending platform is also an attractive funding alternative for the public because it offers higher economic benefits than other financial investment products but also has a relatively high funding risk; people who are interested in funding need to be selective in choosing the party to be funded, pay attention to the quality and credit history of the borrower because credit risk is on the Lender itself. Moreover, the Indonesia Deposit Insurance Corporation (IDIC) does not guarantee the funds distributed. The expansion of P2P lending will also rely on the level of trust that lenders place in P2P platforms.[5]

Fintech P2P lending connects lenders and borrowers, aiming to remove unnecessary financial intermediaries [6], utilizing an online platform without the involvement of an intermediary bank to initiate loans for individuals and businesses.[7] According to data published by OJK as of August 2023, 101 licensed Fintech P2P Lending providers are under the Financial Services Authority (“OJK”), comprising 94 conventional providers and 7 Sharia-based providers. Although this model has expanded access to financial services and offered a more attainable lending alternative for numerous individuals and small businesses, it also entails intricate legal considerations concerning protecting personal data. The significance of personal data protection in fintech P2P lending has garnered considerable attention, emphasizing the necessity to establish legal certainty and attain a new paradigm that harmonizes legal principles with technology.[8] Fintech lenders have increasingly turned to alternative data and intricate modeling to enhance their ability to assess accurately and price credit risk, leading to quicker and more informed credit decisions. P2P lending platforms collect, process, and utilize personal data from borrowers, including sensitive information such as financial details and credit history, and propose that pre-screening borrowers' financial positions result in higher-quality loans being extended to lenders. Hence, it is vital to ensure that relevant regulations safeguard the utilization and security of this personal data.

The Fintech P2P lending industry has shown remarkable growth and resilience, as demonstrated by its positive performance during the pandemic, in contrast to the significant decline experienced by several other financial services sectors. Financial customers are the primary revenue source for fintech companies, according to statistical data released by OJK as of August 30, 2023, there were 119.80 million borrower accounts, with 19.13 million active accounts. Additionally, there were 1.08 million lender accounts, with 180.81 thousand active accounts. Active borrowers remain predominantly from the Gen-Z and Gen-Y demographics, constituting 53.50% of the user base. The accumulated funding disbursement was recorded at IDR 677.51 trillion, with an outstanding value at the end of July 2023 of IDR 53.12 trillion. This is evidence of the industry's role in promoting financial inclusion and is a crucial innovation within the digital economy. However, what must also be emphasized is the balance between innovation and convenience brought by the industry, with the side of security and protection of consumers. The digital revolution creates opportunities for financial inclusion and economic empowerment and exposes users to new, evolving risks.

Cyberlaw has become essential in contemporary societies as new forms of criminal activities conducted on the Internet have become integrated into our daily lives. As the Fintech P2P Lending industry undergoes rapid growth, it becomes an attractive hub for various illicit loans that foster its expansion. On September 4, 2023, the Investment Alert Task Force took action to shut down around 5,753 illegal loan operations in Indonesia. These unlawful fintech activities lead to inadequate legal protection for vulnerable parties. The investigation and prosecution of cybercrimes are becoming increasingly challenging due to the limitations of jurisdictional legal frameworks and the continual expansion of information technology. Some cases that often occur include taking the name of an application owned by Fintech P2P lending that has been licensed by the OJK so that it seems as if it is affiliated or creating a social media account with a name that has similarities and plagiarizing all content on social media of the legal fintech organizer, then contacting potential victims by claiming to be company agents and offering to offer unreasonable payment relief, then direct the potential victim to make payments through a fictitious Virtual Account channel that has been set up. The working mechanism that is also often carried out by illegal online loans is generally done by sending SMS / WhatsApp containing a link that prospective borrowers/consumers can access, which then is accessed and submitted with only a photo ID card; prospective borrowers/consumers are lured to immediately receive loan disbursement but deducted administrative costs that are relatively large in value and loan terms are not transparent where the loan tenor, amount of interest and amount of the penalty are not informed. The debtor will then receive collection accompanied by acts of intimidation, extortion, threats of disseminating personal data, or other threats of violence.[9]

There are several cases related to personal data breaches by illegal fintech from several Court Decisions that have been that have permanent legal force (*inkracht*), including the Decision of North Jakarta District Court No.: 438/Pid.Sus/2020/PN Jkt.Utr, Decision of Lubuk Pakam District Court No.: 2077/Pid.Sus/2021/PN Lbp, and Decision of Lubuk Pakam District Court No.: 2082/Pid.Sus/2021/PN Lbp, these three decisions with permanent legal force fall under the category of special crimes, as they involve intentional and unauthorized distribution, transmission, and accessibility of Electronic Information and Electronic Documents containing personal blackmail and threats, which is a violation of the ITE Law. [10]

Fintech lending can establish a competitive advantage in evaluating potential borrowers by leveraging alternative data sources and the big data techniques inherent in technology-based lending. Personal data protection has become a pivotal concern, particularly with digital commercial platforms gathering, processing, and utilizing individual data on a significant scale for economic purposes. Regulations governing personal data protection play a crucial role in upholding state sovereignty in the digital age and cultivating a cyber-threat-free environment within Indonesia's digital industry, where underestimating losses from cybercrime reveals cybersecurity vulnerabilities and potential hurdles to the nation's digital economy development. The extensive collection, processing, and storage of personal data has made individuals more vulnerable to data breaches, identity theft, and invasive surveillance. As fintech companies continue to grow and diversify their offerings, the regulatory landscape is also evolving. Governments worldwide, including Indonesia, enact comprehensive data protection laws to ensure that individual data is handled carefully and adheres to ethical standards. The enactment of the PDP Law signifies the nation's dedication to safeguarding the digital privacy of its citizens. [11]

While offering numerous advantages, information and communication technologies have also heightened the vulnerability of individuals and businesses to the increased risk of cybercrime. Irregularities in managing personal data can harm consumers, increasing the risk of fraud, privacy violations, and exploitation. One of the legal problems that arise conflicts of legal norms is the gap or potential for legal facts that should (das sollen) and legal points that occur (das sein) related to the rampant crime committed by illegal fintech organizers to access and use users' data which is ultimately misused for unilateral interests. Insufficient public awareness further contributes to the increasing incidents of personal data violations in Indonesia. While most users value their privacy and the necessity of data protection, their behaviors often do not align with these stated preferences and intentions. This research will review personal data protection laws, explore data handling practices, navigate compliance hurdles, explore data security measures, dissect case studies to explain their practical implications and conclude with recommendations and best practices driving data privacy and security in fintech P2P lending. Thus, it is hoped that this research can provide an in-depth understanding and exploration of personal data protection issues, ultimately emphasizing the importance of compliance in the ever-evolving fintech landscape.

The formulation of the problem in this study is:

1. What is the form of legal protection of personal data for personal data of Fintech P2P Lending users in terms of the prevailing laws and regulations in Indonesia?
2. What efforts can be made if User Personal Data is misused on the Fintech P2P Lending Platform?

2 Method

This research utilizes normative legal research methods to analyze the legal framework governing personal data protection in Fintech P2P Lending. Normative legal research identifies legal rules, principles, and doctrines to address specific legal issues. The normative legal approach involves identifying the normative foundations within positive law; it centers on interpreting and implementing legal provisions, such as laws, regulations, doctrines, and principles, to recognize pertinent legal requirements, clarify their legal implications, and suggest potential enhancements. The research follows a descriptive legal analysis approach, which involves a comprehensive review of various laws and regulations related to personal data protection in the Fintech P2P Lending sector. The study's data sources include legal documents, court decisions, legal literature, and official reports and guidelines. Data collection involves a literature study, during which relevant documents are selected and qualitatively analyzed to gain insights and formulate recommendations for enhancing the existing legal framework.

3 Discussion

3.1 Legal protection of personal data of fintech P2P lending users is reviewed from applicable laws and regulations in Indonesia

Digital transformation reshapes finance, fostering collaboration to boost efficiency and widen access to financial services. Fintech is a significant financial industry innovation fueled by the sharing economy, regulatory backing, and IT progress, it prioritizes internet-based models for accessibility and profitability to compete with traditional financial service providers, striving for cost-effectiveness. This industry is increasingly becoming a vital part of the financial services ecosystem, with Fintech P2P Lending at the forefront, catering to unbanked and underserved markets. This fact aligns with the contemporary understanding of Fintechs, which are regarded as facilitators of disintermediation and re-intermediation in the financial services and products sector through innovative technologies and solutions. In Indonesia, P2P Lending is regulated by several related laws and regulations. The three primary laws governing this matter are Law No. 4 of 2023 (P2SK Law), POJK 10/2022, and MCI ("Kominfo") Regulation No. 5 of 2020 concerning the Private Scope Electronic System Operators ("Private Scope PSE") as amended by MCI Regulation No. 10 of 2021. The P2SK Law provides a more robust legal foundation for the Fintech P2P Lending industry, especially in terms of providing a legal basis for illegal P2P Lending providers to be criminalized Article 298 paragraphs (1) and (8), which are valid 3 (three) years after issuance (2026) Article 318 letter b). The operation of Fintech P2P Lending is subject to specific regulations under POJK No. 10/ 2022, including security systems applied in organizations and electronic systems operated. It also regulates audit track records, access and use of personal data, and data deletion duration. Furthermore, in the OJK Circular Letter ("SEOJK") No. 19/SEOJK.06/ 2023 Concerning the Implementation of Information-Technology Based Co-Funding Services, it also regulates that Fintech P2P Lending Providers can only access the camera, location, and microphone on the User's device; meanwhile, to be able to access, obtain, store, manage, process and/or use User Personal Data, the organizer needs to get approval from the User first. [12]

Fintech P2P Lending Company in Article 8 of the P2SK Law jo. Article 2, paragraph (1) of POJK 10/2022, categorized as other financial service institutions³⁰, aligns with this as mentioned in article 237 of the P2SK Law jo. Article 8 paragraph (1) POJK 10/2022, Fintech P2P Lending organizers must first have permission from the OJK to carry out its business activities. Then, according to Article 2 paragraph (1) and Article 6 paragraph (1) of the MCI Regulation No. 5/2020, Fintech P2P Lending organizers are also required to register electronic systems that are owned and have an Electronic System Operator Registration Certificate (PSE)—furthermore, Article 126 paragraph (1) of the P2SK Law jo. Article 108 paragraph (1) POJK 10/2022, as a Fintech P2P company licensed and supervised by the OJK, the Fintech P2P Lending service provider must also be an associate member appointed by the OJK. [13]

The PDP Law that has been enacted and its implementing regulations that are under development are expected to have an essential role in providing legal certainty regarding the processing of personal data, thus supporting increased trust in the digital environment and creating conditions that support the growth of the fintech sector. However, the implementing regulations of the PDP Law should include parameters of sanctions exemptions and relief,

with an emphasis on encouraging compliance of personal data controllers and processors, not just the sanctions themselves. Individuals and corporations are conscious of the necessity for data protection; it refers to a collection of strategies and processes that users can employ to safeguard their data's privacy, availability, and integrity. Insufficient data protection can result in data breaches and identity theft, potentially severely affecting individuals and organizations. [14] Therefore, personal data protection requires concerted attention and action from the government, private sector, and society, hoping to create consumer trust, increase the adoption of digital technologies, and encourage investment and innovation in Indonesia's digital economy.

The PDP Law is not solely aimed at establishing mechanisms to address hacking, fraud, and other cybercrimes. Still, it will also install a legal accountability system for personal data controlling entities to ensure that they take appropriate measures, both in identifying their level of responsibility for data leaks and in implementing preventive measures to avoid future breaches. The presence of the PDP Law provides a universal primary regulation for Indonesia to maintain and regulate the protection of the personal data of the Indonesian people, wherever their data is located. Law No. 27/2022 also emphasizes the necessity of enhancing transaction security, reducing the misuse of individual data, and safeguarding against cyberattacks. [15]

Defined by the PDP Law, personal data refers to information about individuals that can be identified, whether separately or in combination with other data, through electronic or non-electronic systems, either directly or indirectly. Data protection laws are designed to ensure fairness and human rights in using personal data by organizations, providing rights to individuals, and imposing obligations on these organizations. The scope of personal data is vast and includes human activities (do, individual data owner. In response to users' privacy concerns and to ensure compliance with data protection laws, an increasing number of apps are now equipped with privacy policies written in plain language, making it easier for users to comprehend an app's privacy practices. Data protection standards are most effectively upheld when integrated into the technology during its creation.[16] The progressively intricate, interconnected, and ever-changing nature of modern processing environments poses a challenge to the conventional understanding of roles and responsibilities and, consequently, the effectiveness of data protection laws in safeguarding data subjects. Fintech P2P lending providers require a comprehensive fintech ecosystem, which includes credit bureaus, E-KYC providers, banks, payment gateways or aggregators, insurance/guarantee companies, digital signatures, and external collection services, to operate their business effectively, for this reason, based on Article 37 of the PDP Law, Fintech P2P Lending providers are also obliged to monitor every party involved in processing personal data. Data protection laws necessitate that organizations maintain openness and transparency regarding their utilization of personal data⁴². In addition, as stipulated in Articles 6 and 7 of the PDP Law, Fintech P2P Lending organizers must provide access to personal data owners to obtain copies, complete, update, and delete personal data. And must update and correct personal data errors no later than 3 x 24 hours after receiving the request of the personal data owner (Articles 30 and 33 of the PDP Law).

Personal data protection is also governed by Law Number 19 of 2016, which amends Law Number 11 of 2008 (UU ITE), precisely detailed in Article 26, paragraphs (1) and (2). Personal Data in the Electronic System : it defines personal data as specific, confidentially stored, and maintained information that accurately represents individuals and can be used for

identification in compliance with legal provisions. Illegal online loan platforms often resort to accessing personal data, which is subsequently misused for intimidation and harassment during the debt collection process, resulting in actions that violate the ITE Law and the Criminal Code (KUHP). In some instances of illegal online loans with permanent legal judgments (inkracht), such as the North Jakarta District Court Decision Number 438/Pid.Sus/2020/PN Jkt.Utr, Lubuk Pakam District Court Decision Number 2077/Pid.Sus/2021/PN Lbp, and Lubuk Pakam District Court Decision Number 2082/Pid.Sus/2021/PN Lbp, the criminal sanctions typically relate to Article 45 paragraph 3, jo. Article 27, paragraph 3 of the ITE Law, addresses personal data violations, including defamation. This interpretation extends the scope of Article 45, paragraph 3, jo. Article 27, paragraph 3 of the ITE Law, to encompass all forms of defamation, including those defined in Chapter XVI, Book II, of the Criminal Code, such as defamation (Article 310), slander (Article 311), light insult (Article 315), defamation complaints (Article 317), making false accusations (Article 318), and desecration of a deceased person (Articles 320 and 321). The legal basis in these cases does not stem from the platform's lack of registration or licensing but rather from the unauthorized dissemination of borrowers' personal data, intimidation, and threats by the illegal platform. With the enactment of the P2SK Law, legislative regulations are now available to criminalize actors involved in illicit platforms. [17]

Fintech P2P Lending in Indonesia must comply with all regulatory provisions. Article 44 paragraph (1) of POJK Number 10/POJK.05/2022) also requires fintech operators to provide personal data protection for user data. As part of efforts to strengthen data security, all Fintech P2P Lending providers licensed and supervised by OJK have implemented and certified with ISO 27001:2022, an international standard that regulates Information Security Management Systems. [18] Not only that, but to realize a healthy, integrity, and consumer-oriented LPBBTI industry and contribute to national economic growth in the future in the Roadmap for the Development and Strengthening of LPBBTI for the 2023-2028 Period launched by OJK, Fintech Lending companies are also required to implement and be certified with ISO Excellent Service, ISO IT Reliability, ISO Anti-Fraud, and ISO Cyber. Protecting personal data safeguards an individual's right to privacy, which holds economic value for third parties seeking to utilize this data. The above regulations provide more robust legal protection for personal data in the context of Fintech P2P lending practices in Indonesia. The legal protection for parties engaged in Fintech peer-to-peer lending operations in Indonesia relies on principles of transparency, fair treatment, reliability, confidentiality, and data security, as well as the resolution of user disputes through a simple, fast, and cost-effective process. Fintech P2P lending platforms must comply with these provisions to maintain the confidentiality and security of customers' personal data and prevent unauthorized data misuse. With this regulation, it is hoped that the legal protection of personal data in Fintech P2P Lending in Indonesia can be well guaranteed.

P2P lending platforms must clearly explain to users how their data will be used, stored, and processed. This information should be presented in easy-to-understand language without ambiguity or double interpretation. [19] Users should be provided with a detailed description of the types of personal data to be collected, such as personal, financial, and transactional information. In addition, they must also know the purpose of data collection, whether it is for identity verification, credit analysis, or other purposes. Transparency is also related to users' understanding of how their data will be stored and processed. Therefore, P2P lending platforms must transparently detail their data retention policies, security measures, third-party involvement, and data confidentiality and security steps.

In addition, users should be provided with clear information regarding how the P2P Lending platform will process and use their data. Whether such data will be used to make suitable loan offers, for market analysis purposes, or for other purposes should be described in detail. Users must clearly understand how their data will affect their experience using this P2P Lending service. Ensuring that personal data is used lawfully, fairly, and transparently is essential, yet often, users are unaware of the extent to which their data is collected, processed, and shared, and they frequently provide consent without a clear understanding of how their data will be utilized. By providing clear and comprehensive information regarding the collection, storage, and use of personal data, the platform can ensure that users feel comfortable and confident in interacting with the services they offer. [20]

Data privacy concerns data collection, storage, and transfer in compliance with relevant regulations and legislation. Privacy policies provide users with details on information collection, while obtaining explicit consent from users before collecting and using personal data is an essential and ethical step to protect their integrity and privacy, establishing a legal foundation for data processing. Privacy holds immense importance in human life; users have the right to know exactly how their data will be used, including the purposes and types of information to be collected. [21] Legal protection in the context of operating a Fintech Peer to Peer Lending business aims to guarantee the fulfillment of rights and obligations for all parties involved, with particular attention to those who may be vulnerable or disadvantaged. The right to access, rectify, and delete data is crucial in giving users control over their personal information. Users have the right to access data that has been collected by the entity so that they can ensure that the data is accurate and relevant. If there are errors or inaccuracies in the data, the user also has the right to correct the information to reflect the actual condition.

Arrangements for personal data protection play a pivotal role in addressing contemporary business and economic challenges, as they frequently involve data manipulation, including customer data segmentation, data mining, and data extraction. Overall, the principle of support and control over personal data is the basis of a mutually beneficial relationship between the entity collecting the data and the individual providing the information. The active involvement of users in the decision-making process regarding their personal data enables an environment where privacy is respected and information is managed responsibly. With explicit consent and control given to individuals, personal data protection can be realized more effectively and by applicable ethical and regulatory principles. [22]

Illegal fintech firms, system failures, misinformation, transaction errors, data security concerns, the enforcement of Know Your Consumer (KYC) principles, relatively high interest rates, exoneration clauses, and the management of consumer complaints represent some of the most common risks posing a threat to the industry. Data security is an essential aspect of Fintech Peer-to-Peer (P2P) Lending operations that must be prioritized. [23] To maintain user trust, Fintech P2P Lending platforms must implement effective technical and organizational measures to prevent potential leakage or misuse of users' personal data. In addition, regular software and system updates are also an essential step in maintaining data security. From an organizational perspective, the platform should have a clear and transparent privacy policy, conduct regular employee training on data security, and have a structured incident response plan to deal with emergencies. By combining these technical and organizational measures, Fintech P2P Lending can guarantee users that their personal data is safe and protected from potential risks. [24]

The fundamental principle in data ethics and protection law is to minimize the collection and processing of personal data by default. Personal data should be used solely for the purposes communicated to the user, encompassing all information shared on digital platforms, such as names, addresses, phone numbers, and email addresses. Employing personal data for other undisclosed purposes may be seen as a breach of privacy and goes against the fundamental principle of not using this data for harmful or unethical objectives. In cases where individuals confidentially provide information to access services or programs, inappropriate or harmful utilization and disclosure of this data can jeopardize trust, violate privacy rights, and potentially discourage the use of vital services.[25]

Preserving limitations on data usage necessitates proactive engagement from digital service providers and companies gathering personal data. They must establish a clear and transparent privacy policy while ensuring users have complete control over their data. Millennials are more susceptible to privacy risks when using online financial products due to their notably lower financial knowledge than older generations. In addition, education about the importance of data privacy for users also needs to be improved so that they can be more careful in sharing their personal information in the digital world.[22] The data processing system should be developed with a clear emphasis on data privacy and protection, as restricting data usage forms a fundamental basis for upholding the integrity and confidentiality of personal data.

Transparency is crucial; both borrowers and lenders should have access to precise, comprehensive, and easily understandable information regarding interest rates, fees, loan terms, and associated risks. This transparency should extend throughout the loan and payment process, ensuring that the procedures, including loan applications, credit assessments, loan offers, and payments, are conducted without fraud or information manipulation. The principle of transparency dictates that information provided to the public or data subjects must be concise, easily accessible, and in clear and plain language, potentially incorporating visual aids when appropriate. Borrowers and Lenders should have complete visibility into the loan status, including payment progress and outstanding balances. By establishing secure and transparent processes at all stages, customers experience a sense of safety and assurance, resulting in an enhanced level of trust and a greater propensity to adopt Fintech.

Moreover, fairness is a fundamental principle in the Fintech P2P Lending sector, entailing equal and impartial treatment to all borrowers and lenders. It necessitates the implementation of objective credit assessments for all borrowers to evaluate loan risks precisely. Similarly, to improve lenders' decision-making processes and understanding of the choices, lenders should also have equitable access to borrower information. Fair and ethical business principles, encompassing clear information, process transparency, and equitable treatment of borrowers and lenders, are fundamental for a sustainable Fintech P2P Lending platform and for building trust among all stakeholders.

The significance of individual rights within Peer-to-Peer (P2P) Lending platforms is undeniable; these rights encompass access, correction, and deletion of personal data held by the P2P Lending platform. Adhering to and implementing these individual rights is a pivotal step for P2P Lending platforms to strike a balance between fintech advancements and safeguarding personal privacy.[26] Thus, referring to the principles of personal data protection, Fintech P2P lending must ensure that customers' personal data is collected only with valid permission, used only for the purposes described, managed securely, not accessed without permission, and not misused. Compliance with relevant laws and applying equitable

principles in safeguarding personal and business data are fundamental for Fintech P2P Lending to foster user confidence and uphold operational integrity. To achieve this, Fintech P2P lending must consistently monitor the evolving landscape of personal data protection and fintech-related regulations, ensuring ongoing compliance and sustaining customer trust and the overall integrity of the Fintech industry.

3.2 Efforts can be made if user personal data is misused on the Fintech P2P Lending Platform

As laws and regulations ensure, the legal framework for personal data protection establishes the foundation for legal actions in personal data breaches. Fintech P2P Lending service users, who are consumers, can pursue legal remedies when they believe their privacy rights have been violated or have suffered harm. These remedies can take the form of litigation, conducted within the court system (litigation), or non-litigation, which occurs outside the court. Legal remedies through litigation are considered the final recourse if non-litigation efforts fail.

Dispute resolution in Fintech P2P Lending outside the court can be made by alternative dispute resolution institutions (LAPS) as stipulated in the Financial Services Authority Regulation No. 1/POJK.07/2014 concerning alternative dispute resolution institutions in the financial services sector article 1 paragraph (2). An effective dispute resolution mechanism through an Alternative Dispute Resolution Institution is essential to resolve disputes quickly. [27]

Fintech P2P Lending users can also pursue litigation legal remedies through civil and criminal law fields. In civil law, consumers can file a lawsuit against the organizer or other parties to the district court of their jurisdiction. Where the act can cause good harm to the victim and, therefore, the show can be included in the unlawful act. This civil lawsuit intends to obtain consumer compensation, namely, users of Fintech P2P Lending services, as plaintiffs sued against the defendant, who in this case is the organizer of Fintech P2P Lending.[25] In addition, court proceedings may prosecute not only Fintech P2P Lending organizers but also third parties who misuse personal data and individuals who are not directly related to the owner of personal data.

Meanwhile, legal settlements through criminal law can use criminal offenses such as electronic data theft offenses, illegal dissemination of electronic information, threats through electronic transactions, fraud, and defamation such as the ITE Law, PDP Law, P2SK Law, and the Criminal Code.[28] Therefore, the victim can file a police report with the local police agency. For illegal loan perpetrators, criminal sanctions can be charged based on Article 305 of the P2SK Law with a minimum prison sentence of 5 years and a maximum of 10 years, a fine of at least IDR 1 billion, and a maximum of IDR 1 trillion; or blocking sanctions for illegal lending platforms that are not registered as according to Article 7 paragraph 2 of the MCI Regulation No. 5 of 2020 concerning Private Scope Electronic System Operators ("Private Scope PSE") as amended by MCI Regulation No. 10 of 2021, if the Private Scope PSE does not register, administrative sanctions may be given in the form of Termination of Access to Electronic Systems (access blocking).[29]

Perpetrators of illegal online loan and licensed P2P Lending Companies can also be charged with criminal sanctions under Article 45B of Law No.11 of 2008 concerning Electronic Information and Transactions as amended by Law No.19 of 2016 if collecting with threats; Article 368 paragraph (1) of the Criminal Code when collecting by force; and Article

67 paragraphs (1) and (2) of the PDP Law when disseminating Personal Data without permission.[30]

Meanwhile, for non-litigation legal remedies as a preventive measure, you can report the misuse of illegal fintech personal data to the regulator, in this case, the Investment Alert Task Force, which is a joint team from the police, OJK and Kominfo, or through the AFPI association. If proven to have violated the personal data leakage law, OJK will provide administrative sanctions in the form of written warnings or fines imposed on online loan service providers either separately or simultaneously with sanctions in the form of restrictions on business activities or revocation of their business licenses. Conditions in the business activities in question limit the capacity to receive service users for a certain period. The provision of fines is intended to pay a sum of money as an obligation of online loan providers provided by OJK to create a deterrent effect due to violations and losses to other parties carried out by the organizer.

4 Conclusion

The Personal Data Protection Law is expected to solve personal data leakage because victims of data leak reporting have legal certainty and a clear legal basis to report their problems to law enforcement officials so that victims can be followed up. Fintech P2P Lending providers must maintain the confidentiality of personal, transaction, and financial data they manage from obtaining data until consumer data is destroyed. Forms of legal protection for the personal data of Fintech P2P Lending users include preventive and repressive legal protection. In preventive legal protection, especially in Fintech P2P Lending services, the government, through OJK, has issued OJK regulations related to Information Technology-Based Co-Funding Services, namely POJK 10/2022 and OJK Circular Letter (“SEOJK”) No. 19/SEOJK.06/ 2023 Concerning the Implementation of Information-Technology Co-Funding Services. With the issuance of POJK 10/2022 and SEOJK No.19/SEOJK.06/2023, OJK's role emphasizes strengthening the quality of the P2P Lending industry so that, in the long run, P2P Lending services are expected to be safer, more comfortable, grow sustainably, and more stable. In addition, there is also repressive protection that can resolve disputes in the future through the Court within the scope of the General Court or through Government Agencies, which are administrative appellate institutions, by providing administrative sanctions for violators. Efforts that Fintech P2P Lending users can make if they find a leak of user personal data on the Fintech P2P Lending provider platform are being able to carry out non-judicial or non-litigation legal remedies (outside the court) or judicial or litigation legal remedies (judicial).

References

- [1] A. Demir, V. Pesqué-Cela, Y. Altunbas, and V. Murinde, "Fintech, financial inclusion and income inequality: a quantile regression approach," *Eur. J. Financ.*, vol. 28, no. 1, pp. 86–107, 2022, doi: 10.1080/1351847X.2020.1772335.
- [2] M. F. Arkanuddin, F. D. Saragih, and B. Y. Nugroho, "The key role of the financial regulation in fintech ecosystem: A model validation," *Estud. Econ. Apl.*, vol. 39, no. 12, 2021, doi: 10.25115/eea.v39i12.6239.
- [3] L. Grassi and D. Lanfranchi, *RegTech in public and private sectors: the nexus between data, technology and regulation*, vol. 49, no. 3. Springer International Publishing, 2022. doi: 10.1007/s40812-022-00226-0.
- [4] P. Gomber, R. J. Kauffman, C. Parker, and B. W. Weber, "On the Fintech Revolution: Interpreting the Forces of Innovation, Disruption, and Transformation in Financial Services," *J. Manag. Inf. Syst.*, vol. 35, no. 1, pp. 220–265, 2018, doi: 10.1080/07421222.2018.1440766.
- [5] A. V. Thakor, "Fintech and banking: What do we know?," *J. Financ. Intermediation*, vol. 41, no. August, 2020, doi: 10.1016/j.jfi.2019.100833.
- [6] M. V. d Christophe Croux a, Julapa Jagtiani b, Tarunsai Korivi c, *Important factors deteming fintech loan default*, vol. 173, no. May. 2020.
- [7] S. Agarwal and J. Zhang, "FinTech, Lending and Payment Innovation: A Review," *Asia-Pacific J. Financ. Stud.*, vol. 49, no. 3, pp. 353–367, 2020, doi: 10.1111/ajfs.12294.
- [8] C. A. Comelles, "Smart contracts or Code is Law: legal remedies for contractual robotization," *InDret*, vol. 2, no. Marzo, pp. 1–41, 2020, doi: 10.31009/InDret.2020.i2.01.
- [9] L. Yu *et al.*, "PPChecker: Towards Accessing the Trustworthiness of Android Apps' Privacy Policies," *IEEE Trans. Softw. Eng.*, vol. 47, no. 2, pp. 221–242, 2021, doi: 10.1109/TSE.2018.2886875.
- [10] Menteri Komunikasi dan Informatika Republik Indonesia, "Peraturan Menteri Komunikasi Dan Informatika Republik Indonesia Nomor 5 Tahun 2020 Tentang Penyelenggara Sistem Elektronik Lingkup Privat," *Kementerian. Komun. dan Inform. Republik Indones.*, 2020.
- [11] Otoritas Jasa Keuangan, "Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 10 /Pojk.05/2022 Tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi," no. 184, pp. 1–27, 2022.
- [12] Otoritas Jasa Keuangan, "SURAT EDARAN OTORITAS JASA KEUANGAN REPUBLIK INDONESIA NOMOR 19/SEOJK.06/ 2023 TENTANG PENYELENGGARAAN LAYANAN PENDANAAN BERSAMA BERBASIS TEKNOLOGI INFORMASI," vol. 4, no. 1, pp. 88–100, 2023.
- [13] Indonesia, "Undang-undang Perlindungan Data Pribadi," no. 016999, pp. 1–50, 2022.
- [14] Y. Zhao and X. Chen, "The relationship between the withdrawal of the digital

economy's innovators, government interventions, the marketization level and market size based on big data," *J. Enterp. Inf. Manag.*, vol. 35, no. 4–5, pp. 1202–1232, 2022, doi: 10.1108/JEIM-01-2021-0050.

- [15] M. Veale and F. Z. Borgesius, "Adtech and Real-Time Bidding under European Data Protection Law," *Ger. Law J.*, vol. 23, no. 2, pp. 226–256, 2022, doi: 10.1017/glj.2022.18.
- [16] U. Tatar, Y. Gokce, and B. Nussbaum, "Law versus technology: Blockchain, GDPR, and tough tradeoffs," *Comput. Law Secur. Rev.*, vol. 38, pp. 1–11, 2020, doi: 10.1016/j.clsr.2020.105454.
- [17] S. Taekema, "Theoretical and Normative Frameworks for Legal Research: Putting Theory into Practice," *Law Method*, pp. 1–17, 2018, doi: 10.5553/rem/.000031.
- [18] S. Suryanto, H. A. Muhyi, P. S. Kurniati, and N. Mustapha, "Banking Financial Performance in the Industry Financial Technology Era," *J. East. Eur. Cent. Asian Res.*, vol. 9, no. 5, pp. 889–900, 2022, doi: 10.15549/jeeecar.v9i5.1075.
- [19] H. Stewart and J. Jürjens, "Data security and consumer trust in FinTech innovation in Germany," *Inf. Comput. Secur.*, vol. 26, no. 1, pp. 109–128, 2018, doi: 10.1108/ICS-06-2017-0039.
- [20] C. Schmit, K. Kelly, and J. Bernstein, "Cross Sector Data Sharing: Necessity, Challenge, and Hope," *J. Law, Med. Ethics*, vol. 47, no. 2_suppl, pp. 83–86, 2019, doi: 10.1177/1073110519857325.
- [21] I. A. Priskarini, Pranoto, and K. Tejomurti, "The Role of The Financial Services Authority in The Legal Protection of Privacy Rights in Connection with Personal Data of Fintech Lending Debtor in Indonesia," *Padjadjaran J. Ilmu Huk.*, vol. 6, no. 3, pp. 556–575, 2019, doi: 10.22304/pjih.v6n3.a7.
- [22] R. H. N. Azmi, "Indonesian Cyber Law Formulation in The Development Of National Laws In 4.0 Era," *Lex Sci. Law Rev.*, vol. 4, no. 1, pp. 49–62, 2020, doi: 10.15294/lesrev.v4i1.38109.
- [23] T. A. Christiani, "Normative and Empirical Research Methods: Their Usefulness and Relevance in the Study of Law as an Object," *Procedia - Soc. Behav. Sci.*, vol. 219, pp. 201–207, 2016, doi: 10.1016/j.sbspro.2016.05.006.
- [24] G. Buchak, "FINTECH, REGULATORY ARBITRAGE, AND THE RISE OF SHADOW BANKS," *Angew. Chemie Int. Ed.* 6(11), 951–952., vol. 1, no. April, 2015.
- [25] I. Lee and Y. J. Shin, "Fintech: Ecosystem, business models, investment decisions, and challenges," *Bus. Horiz.*, vol. 61, no. 1, pp. 35–46, 2018, doi: 10.1016/j.bushor.2017.09.003.
- [26] M. Botta and K. Wiedemann, "The interaction of EU competition, consumer, and data protection law in the digital economy: The regulatory dilemma in the facebook odyssey," *Antitrust Bull.*, vol. 64, no. 3, pp. 428–446, 2019, doi: 10.1177/0003603X19863590.
- [27] R. Ayunda, "Personal Data Protection to E-Commerce Consumer: What Are the Legal Challenges and Certainties?," *Law Reform J. Pembaharuan Huk.*, vol. 18, no. 2, pp.

144–163, 2022, doi: 10.14710/Ir.v18i2.43307.

- [28] D. B. Kharisma, “Urgency of financial technology (Fintech) laws in Indonesia,” *Int. J. Law Manag.*, vol. 63, no. 3, pp. 320–331, 2021, doi: 10.1108/IJLMA-08-2020-0233.
- [29] H. H. H. Aldboush and M. Ferdous, “Building Trust in Fintech: An Analysis of Ethical and Privacy Considerations in the Intersection of Big Data, AI, and Customer Trust,” *Int. J. Financ. Stud.*, vol. 11, no. 3, 2023, doi: 10.3390/ijfs11030090.
- [30] S. D. Jayasekara and I. Abeysekara, “Digital forensics and evolving cyber law: case of BIMSTEC countries,” *J. Money Laund. Control*, vol. 22, no. 4, pp. 744–752, 2019, doi: 10.1108/JMLC-02-2019-0019.