AIRLANGGA DEVELOPMENT JOURNAL
ADJ
p-ISSN: 2528-3642

Sekolah Pascasarjana Universitas Airlangga

Jalan Airlangga No. 4-6, Surabaya - 60286
Telp. : (031) 5041566, 5041536

PERSONAL DATA MISUSE IN FINTECH LENDING PROVIDERS FROM PERSPECTIVE INDONESIAN CYBERLAW

Elvia Rahmawati[1], Miftakhul Huda[2], Ian Firstian Aldhi[3]
Departement of Law, Narotama University[1,2]
Human Resource Development, Postgraduate School, Universitas Airlangga[3]
*Email: elviarahma14@gmail.com[1], miftahul.huda@narotama.ac.id[2], ian.firstian.aldhi-2021@pasca.unair.ac.id[3]

Received:
March, 28 2022

Revised:
June 14, 2024

Accepted:
June 17, 2024

ABSTRACT

This study aims to investigate the forms of personal data misuse by fintech lending providers and the legal measures that can be taken when such misuse occurs, within the context of Indonesian cyber law. The background of this research is driven by the rapid development of fintech lending, which is often exploited for criminal activities, including personal data misuse. The method used is normative legal research with statutory and conceptual approaches. The results show that personal data misuse by fintech lending providers can take various forms, such as unauthorized data usage, illegal disclosure of personal information, and the use of malware to access data. Such violations can result in criminal penalties under Law No. 27 of 2022 on Personal Data Protection. The conclusion is that there is a need for stricter supervision of fintech lending providers and increased public awareness of personal data protection. Recommendations include the implementation of stricter regulations by the Financial Services Authority (OJK), more intensive supervision by the Indonesian Fintech Association, and public education on their rights regarding personal data.

Keywords: *fintech lending, personal data misuse, consumer protection, cyber law.*

ABSTRAK

Penelitian ini bertujuan untuk mengetahui bentuk-bentuk penyalahgunaan data pribadi oleh penyelenggara fintech lending dan langkah hukum yang dapat diambil saat terjadi penyalahgunaan tersebut dalam perspektif hukum siber di Indonesia. Latar belakang penelitian ini didasari oleh perkembangan fintech lending yang pesat, namun kerap dimanfaatkan untuk melakukan kejahatan, termasuk penyalahgunaan data pribadi. Metode yang digunakan adalah penelitian hukum normatif dengan pendekatan peraturan perundang-undangan dan konseptual. Hasil penelitian menunjukkan bahwa penyalahgunaan data pribadi oleh penyelenggara fintech lending dapat berbentuk penggunaan data tanpa izin, pengungkapan informasi pribadi secara ilegal, dan penggunaan malware untuk mengakses data. Pelanggaran ini dapat berakibat pidana sesuai dengan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Kesimpulan dari penelitian ini adalah perlunya pengawasan yang lebih ketat terhadap penyelenggara fintech lending dan peningkatan kesadaran masyarakat tentang perlindungan data pribadi. Saran yang diberikan meliputi penerapan regulasi yang lebih ketat oleh OJK, pengawasan yang lebih intensif oleh Asosiasi Fintech Indonesia, dan edukasi kepada masyarakat tentang hak-hak mereka terkait data pribadi.

Kata kunci: fintech lending, penyalahgunaan data pribadi, hhukum siber, perlindungan konsumen.

INTRODUCTION

Financial Technology, or fintech, represents a collaboration between technology and information with innovation in financial services. The term fintech itself refers to the use of technology to provide solutions to problems in the financial sector (Alt, R., Beck, R., & Smits, M. T., 2018). The definition of fintech can also be found in Bank Indonesia Regulation Number 19/12/PBI/2017 on the Implementation of Financial Technology, which defines fintech as the

use of technology in the financial system that produces new products, services, technology, and/or business models and impacts monetary stability, the financial system, and/or the efficiency, smoothness, security, and condition of the payment system.

Currently, there are various services offered by fintech, both by financial institutions supervised by the Financial Services Authority (OJK), such as banking services, insurance, or other registered financial institutions, as well as those offered by startup companies (Jafar, 2019). The development of fintech is still dominated by fintech payment and fintech lending. Fintech lending is a service that brings together lenders and borrowers to make a loan agreement through an electronic system using the internet (Wijayanto et al, 2020). Fintech lending is widely used by the public because borrowing funds can be done more practically and with less complicated prerequisites than banking, with a fast process, and loans can be requested for any reason as long as there is someone who allocates their money (Napitupula et al, 2017).

The implementation of fintech lending in Indonesia currently refers to the Financial Services Authority Regulation No. 77/POJK. 01/2016 on Information Technology-Based Lending Services (hereinafter referred to as POJK 77/2016) where the provider of Information Technology-Based Lending Services (LPMUBTT) is a legal entity or corporation in Indonesia that provides, manages, and operates LPMUBTT services, in this case, the provider is required to register and obtain a license from the OJK, currently, there are at least 121 fintech lending companies registered and licensed by the OJK. Crime always develops along with the development of society and technology, as well as in the fintech world, the momentum of fintech lending development is often exploited to commit crimes, one of which is through fintech lending platforms that are not registered and do not have a license from the OJK or illegal fintech lending. From 2018 to 2021, at least 3,193 illegal fintech lending entities have been blocked by the Investment Alert Task Force (SWI) in collaboration with the Ministry of Communication and Information Technology of the Republic of Indonesia (Kemenkominfo, 2021). In preventive legal efforts for fintech lending services, the government has issued several new regulations that specifically guarantee the security of a person's personal data. The law is "Law Number 27 of 2022 on Personal Data Protection or which is subsequently commonly referred to as the PDP Law". In addition to the law, the Financial Services Authority (OJK) is currently also regulating online lending services using the "Financial Services Authority Regulation (POJK) Number 10 /POJK.05/2022 on Technology-Based Joint Funding Services". Both regulations guarantee protection for the security of customer personal data. Meanwhile, the role of the repressive legal protection party is to function to resolve if a dispute arises in the future, in this case, it will be resolved by the court. In "POJK Number 10 /POJK.05/2022" online lending services cannot be separated from the use of personal data of its service users. The privacy policy on personal data/identity explains a person's right to decide whether to join or not in sharing personal data.

Unfortunately, in practice, many illegal fintech lending and some other Fintech Lending Implementations often impose very large and non-transparent fees and fines, use billing methods that do not follow ethical billing procedures and according to the rules, and often occur billing in rough ways that violate human rights, besides that some fintech lending also requests access to all the personal data of their consumers, namely the request for access to all the personal data of consumers such as mobile phone numbers, photos, storage, and other data that are often misused (Suseno & Yeti, 2021). Personal data is any information related to an identified or identifiable natural person, an identifiable natural person is a person who can be identified, directly or indirectly, especially by referring to identifiers such as name, identification number, location data, online identifiers or one or more specific factors for

physical, physiological, genetic, mental, economic, cultural or social identity of a person (Finck, M., & Pallas, F., 2020). As for Article 1 number 1 of Law Number 27 of 2022, it reads, "Personal Data is data about an individual who is identified or can be identified separately or in combination with other information either directly or indirectly through an electronic or non-electronic system." This is exacerbated by the consumptive actions of the public who always agree to the terms and conditions offered by fintech lending without knowing the contents. Consumers must carefully pay attention to contract clauses, loan interest rates, loan time frames, and most urgently check whether the fintech lending company is registered with the OJK or is illegal (San Andres, E. A., & Hernando, R. C., 2019). This has implications for the personal data of consumer loan borrowers, because before entering into an agreement, the borrower must fill in a number of personal data requested by the fintech company. Such as full name, place, date and year of birth, occupation, address, mother's name, mobile phone number, borrower's email, name and mobile phone number that can be contacted other than the borrower's mobile phone number, the form of kinship relationship with the owner of the mobile phone number.

In some cases, there are also several fintech lending that use malicious malware to process and collect personal data of fintech lending users (Arifin et al, 2023). The rapid growth of fintech lending service providers has not been accompanied by education to the public about online loans. This situation certainly raises various effects/risks. The risks posed include various kinds of online loans, the large number of service providers who have not registered or are illegal, and the frequent discovery of personal data of users being misused by the companies that organize or even by other parties. The public, who are interested in the ease and speed of the loan process, have carefully provided various personal data ranging from contacts, photos, videos, locations, even electronic ID card photos. If the abuse is carried out by the online lending organizer, then the protection of consumer personal data will be neglected. This is where consumer caution is needed in making agreements with fintech lending organizers. This study aims to determine the forms of misuse of personal data by fintech lending organizers and how the legal steps are when there is misuse of personal data by fintech lending organizers in the perspective of cyber law in Indonesia.

METHOD

The method used is the Normative legal research method, which aims to find solutions to legal issues and problems that arise, so that the results obtained provide prescriptions for what the legal issues should be. The technique of legal material collection is carried out through the snowball method, which starts with the collection of both primary and secondary legal materials and inventories, identifies, and takes cases relevant to the topic (Marzuki, 2016). In this study, several approaches to the problem are used, namely the Statute Approach and the Conceptual Approach. The Statute Approach is conducted by examining all laws and regulations related to the issue being addressed. The Conceptual Approach is carried out by researching existing doctrines (Tan, 2021).

RESULTS AND DISCUSSION

Forms of Personal Data Misuse by Fintech Lending Providers

The diversion of personal data of loan customers by both legal and illegal fintech companies is not only a violation of the law but also a violation of human rights in the area of privacy rights. This can also be seen in Article 29 Paragraph 1 of Law No. 39 of 1999, which states, "Every person has the right to protection of their personal self, family, honor, dignity, and property."

Article 28G Paragraph (1) of the 1945 Constitution states, "Every person has the right to protection of their personal self, family, honor, dignity, and property under their control, and has the right to feel safe and protected from threats of fear to act or not act in a way that is a basic right."

The form of consumer personal data deviation carried out by fintech lending operators results in criminal consequences. Article 67 of Law No. 27 of 2022 Paragraph (1) states, "Any person who intentionally unlawfully obtains or collects Personal Data not belonging to them with the intent to benefit themselves or others that can cause loss to the Personal Data Subject as referred to in Article 65 paragraph (1) is punishable by imprisonment for up to 5 (five) years and/or a fine of up to IDR 5,000,000,000.00 (five billion rupiah)." Paragraph (2) "Any person who intentionally and unlawfully discloses Personal Data not belonging to them as referred to in Article 65 paragraph (2) is punishable by imprisonment for up to 4 (four) years and/or a fine of up to IDR 4,000,000,000.00 (four billion rupiah)." Paragraph (3) "Any person who intentionally and unlawfully uses Personal Data not belonging to them as referred to in Article 65 paragraph (3) is punishable by imprisonment for up to 5 (five) years and/or a fine of up to IDR 5,000,000,000.00 (five billion rupiah)."

Personal Data is generally categorized into two parts, namely first, data of a general nature such as name, address, email address, location data, IP Address, Web Cookie. Second, data of a specific (sensitive) nature, including race, ethnicity, religion, political views, sexual orientation, genetics, biometrics, mental and psychological conditions, criminal records (Djafar, 2019). The classification of personal data, if referring to the General Data Protection Regulation (GDPR), can be seen from the limitation of the regulation of personal data protected in the GDPR, namely in the provisions of Article 4 paragraph (1) GDPR explicitly classifying personal data into common personal data such as name, identification number, location, online identification, while specific personal data is grouped into physical, physiological, genetic, mental, economic, cultural or social identity data of a person. In addition, the provisions of Article 4 of the GDPR also limit the regulation of its personal data to genetic data, biometric data, and health-related data. Meanwhile, the classification of personal data protected according to national legal provisions can be found in Article 84 of Law No. 24/2013, which defines the personal data of residents that must be protected, namely: a) information about physical and/or mental disabilities, b) fingerprints, c) iris, d) signature, and e) data elements that are a disgrace to someone.

Article 4 of Law No. 27 of 2022 states that types of personal data are divided into two, namely specific personal data and general personal data. Specific personal data such as health data and information, biometric data, crime records, children's data, personal financial data, and/or other data according to the provisions of legislation. General personal data such as full name, gender, nationality, religion, marital status, and personal data combined to identify a person. Business actors or electronic system operators can collect personal data from customers offline or online, where digital data can be traded without the knowledge and consent of the data owner or misused (for purposes other than the provision, submission of digital personal data), it can also occur personal data that is connected is hijacked, stolen (hack) by third parties

According to Permenkominfo No. 20/2016, in Article 14 of PP No. 71/2019, fintech lending operators as electronic system operators also have an obligation to implement the principle of personal data protection in the data processing carried out. The application of the principle of personal data protection is carried out from the process of collection in the form of ensuring the consent of the owner of personal data when collecting data, data processing carried out according to the purpose of data processing, guaranteeing the rights of the owner of personal data, and processing is carried out by protecting the security of personal data from

loss, misuse, access or unauthorized disclosure, or from the occurrence of changes and destruction of personal data and in the event of a failure to protect personal data managed by fintech lending operators, based on Article 14 paragraph (5) of PP 71/2019, the operator has an obligation to inform the data owner in writing about the failure that occurred.

Cybercrime in fintech lending includes, among other things, the misuse of personal data (Sinaga, 2021). The misuse of personal data refers to actions that meet the elements of criminal acts such as fraud, theft, and other criminal acts (Bukit, A. N., & Ayunda, R, 2022). The misuse of personal data occurs, among other things, due to negligence on the part of potential victims in carrying out their daily activities. For example, when downloading applications from unreliable sites, or when accessing a fintech lending application and not paying attention to the permissions requested by the application, which unknowingly such actions have the potential to cause harm to the victim (Noor, A., & Wulandari, D, 2021). There are several forms of misuse of personal data carried out by fintech lending from the process of obtaining to the use of personal data.

The acquisition and collection of personal data by fintech lending, if referring to the provisions of Article 7 paragraph (1) of Permenkominfo No. 20/2016, the acquisition by an electronic system is limited to information that is relevant and in accordance with the purpose of acquisition and collection, and the process must be carried out accurately. Electronic system operators as fintech lending operators in the acquisition and collection of personal data are obliged to respect the owner of personal data for their privacy data, this respect is implemented in the provision of choices in the electronic system regarding the confidentiality or non-confidentiality of personal data as well as regarding changes, additions, or updates to personal data (vide Article 8 paragraph (2) of Permenkominfo No. 20/2016) and the need for owner's consent (Vide Article 9 of Permenkominfo 20/2016). Malware is malicious software often referred to as malicious software is one of the attacks on computer systems that damage security holes processed in the system without the owner's knowledge (user) works from behind and is used to access the network on the computer (Dutta et al, 2022). Malware can also be defined as a program compiled using relevant logic and algorithms used for a specific purpose. Usually malicious malware is inserted in various ways as follows (Selvaganapathy et al, 2021):

1. Malware is often smuggled into common and popular files such as applications;
2. Malware is often inserted into files needed to install an application or program;
3. Malware is disguised using commonly used file names for various purposes such as drivers (.drv), data (dat), etc., so that its existence is not realized when it is in the gadget;
4. Malware is often developed to be able to transmit itself to other places, so that gadgets can become nests of viruses/worms;
5. Malware is implanted in the computer system without the user's knowledge.

In a study that examines fintech lending applications, especially illegal fintech lending, related to the act of misusing personal data by fintech lending operators, the results found that several illegal fintech lending applications contain malware activities intentionally created by the operator, to take personal data outside the data allowed (Wahyudi, 2017). Malware attacks are basically programs designed to damage by infiltrating computer systems. One type of dangerous malware is spyware. According to one global antivirus vendor, Kaspersky, spyware is software designed to enter a computer device that has the ability to collect user's personal data and send it to others. In addition, it was found that illegal fintech lending often asks for access to give permission in the form of granting application permission to information and data on the gadget, the requested permission is READ_PHONE_CONTACTS so that it is possible to access the phone contact list on the consumer's gadget, even though the access limit

to personal data given by OJK to fintech lending is limited to microphones, locations, and cameras, for the purpose of e-know your customer. So in cases like this, personal data accessed is data outside the data needed as a loan requirement (Rosmida, 2021). In other cases, the acquisition and collection of personal data is carried out by entering the fintech lending account of the data owner, namely in the case that occurred in illegal fintech lending Vloan, namely when there are debtors who are late in making payments until the due date, some desk collectors of PT Vcard Technology access Supercash.co/Banshee Vloan using the username and password of each debtor, then they access features that contain personal data, after accessing the debtor's personal data then the desk collector creates a Whatsapp group consisting of colleagues and victims previously obtained through Supercash.co/Banshee Vloan (Novridasati, 2020). The provisions of illegal access in the ITE Law are conventionally accommodated in the Criminal Code in Article 167 paragraph (1) and paragraph (2) related to the act of entering someone's house without permission or trespassing, which provides protection for property and privacy. The concept of the act in Article 167 paragraph (1) and (2) is what is intended to be raised in Article 30 of the ITE Law, that just as the act of entering someone's house without permission is a violation of property and privacy, so no one may intentionally and without rights access computers and/or electronic systems belonging to others, especially for the purpose of obtaining electronic information and/or electronic documents belonging to others that are within the scope of privacy. Meanwhile, the acquisition and collection of personal data using malicious malware falls under criminal acts as stipulated in Article 32 paragraph (2) jo. Article 48 paragraph (2) of the ITE Law relates to acts that provide interference with data (data interference), which is also a violation of someone's privacy and electronic property. In addition to the Information and Electronic Transactions Law (ITE Law) and the Regulation of the Minister of Communication and Informatics regarding the protection of personal data, Indonesia now has a clear and definite legal umbrella in guaranteeing personal data, namely Law No. 27 of 2022 concerning Personal Data Protection, which was just ratified on October 20, 2022. In the PDP Law, personal data is defined as data about an individual who is identified or can be identified separately or combined with other information either directly or indirectly through electronic or non-electronic systems.

The new law emphasizes the importance of protecting personal data in the digital era and provides a legal framework for the processing, storage, and transmission of personal data. It sets out the rights of data subjects, including the right to access, correct, and delete their personal data, as well as the right to object to its processing. It also outlines the obligations of data controllers and processors, including the requirement to obtain consent for data processing, to protect data from unauthorized access, and to report data breaches to the authorities.

The law also establishes the Personal Data Protection Authority, an independent body responsible for overseeing the implementation of the law, handling complaints, and taking enforcement action against violators. The authority is tasked with developing regulations and guidelines to ensure the effective protection of personal data and to promote awareness of data protection issues among the public and businesses. Overall, the Personal Data Protection Law represents a significant step forward in safeguarding the privacy and security of personal data in Indonesia, and aligns the country's data protection standards with international best practices. It is expected to enhance trust in digital services and contribute to the growth of the digital economy in Indonesia.

Another case is that of Rupiah Plus. In 2018, Rupiah Plus, a fintech lending operator that had obtained a license from OJK (Financial Services Authority), went viral due to its debt collection methods towards consumers who had not paid their loan installments. The method

involved contacting all the numbers in the borrower's phone contacts, which had no relation to the loan issue. This was understandably distressing to the public, especially to online loan borrowers whose delinquent loan data was "published" by the fintech operator's collectors. In this case, savvy consumers whose personal data was misused could report the electronic data misuse to the authorities or to OJK as the institution authorized to supervise financial and banking services (Sulaiman, 2021). This could be indicated as an unpleasant act, defamation, as well as slander.

Rudiantara, the Minister of Communication and Information, later referred to as Menkominfo, emphasized that the persecution and misuse of customer personal data carried out by Rupiah Plus violated regulations. Among the regulations violated, before the enactment of Law No. 27 of 2022, were Articles 26, 27, 28, and 29 of Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 on ITE. As reported on the official Kemeninfo website, Rupiah Plus admitted its mistake for violating collection procedures, in the form of unpleasant actions towards debtors to quickly settle debts. OJK has imposed sanctions on the Rupiah Plus money lending application, with a delay in submitting an operating permit to OJK for 3 months. This demonstrates that strict law enforcement is an effective solution to suppress the misuse of personal data carried out by Rupiah Plus. OJK, as an institution given authority and the task of supervising the banking and financial services sector, must take firm steps to impose sanctions, both administratively, civilly, and criminally, on fintech companies that use customer personal data unlawfully.

Based on the perspective of Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 on Information and Electronic Transactions, henceforth referred to as the ITE Law, defamation is stipulated in Article 27 Paragraph (3) which states, "Every person who intentionally and without rights distributes and/or transmits and/or makes accessible electronic information and/or electronic documents containing insults and/or defamation" (Erwin Asmasi, 2021, p. 23). Forms of data misuse that can occur in fintech lending include (1) Misuse of e-KTP photos belonging to fintech lending consumers, (2) Dissemination of personal photos or posters or memes of fintech lending application consumers, (3) Dissemination of contact numbers of online loan application consumers, (4) Dissemination of data in the gallery of photos, videos, and others found on the gadget of fintech lending application consumers. The dissemination of disgrace, accusations, defamation, including the amount of debt of fintech lending application consumers to others or the public (Syaifuddin, 2020). Usually, these violations are committed for the purpose of debt collection from debtors. One case that occurred in the process of using and utilizing personal data is the case of debt collection with the misuse of personal data by "Rupiah Plus", which is a fintech lending registered and supervised by OJK in 2018, carrying out debt collection by threatening, intimidating, harassing, and collecting from third parties who have no relation to the customer, in addition, Rupiah Plus was reported for accessing contacts on its customers' phones for debt collection purposes (Rahmi, 2020). In this case, Article 65 of Law No. 27 of 2022 contains Prohibitions in the Use of Personal Data:

1. Every person is prohibited from unlawfully obtaining or collecting personal data that is not their own with the intent to benefit themselves or others that can cause loss to the personal data subject.
2. Every person is prohibited from unlawally disclosing personal data that is not their own.
3. Every person is prohibited from unlawfully disclosing personal data that is not their own.

In the case of app-based lending, fintech lending companies can use consumer personal data without the consumer's consent or knowledge. According to bisnis.com, Tulus Abadi, the

Chairman of the Indonesian Consumer Foundation (YLKI), stated that they received many complaints from the public related to online shopping and fintech. The majority of personal data misuse comes from illegal online loans, which account for 70 percent, although legal fintech also contributes. The most common forms of personal data misuse include telephone numbers, photos, videos, and various items stored on the consumer's phone, as all of these can be tapped by fintech parties (Hidayat, et al., 2023). Some examples of personal data misuse include (Situmeang, 2022):

Copying data and information from customer ATM cards (skimming) where the skimming perpetrator withdraws funds elsewhere.

Online loans, where the transaction mechanism involves filling in data online, but in the case of payment delays, collectors are often used to intimidate customers, their families, their workplace superiors, and even access data from the customer's phone. Online transportation, where consumers experience sexual harassment through WhatsApp numbers.

Upon further clarification, the form of personal data deviation with the use of fintech applications not only involves collectors in debt collection from consumers through terror, intimidation, and accessing all data and contact numbers on the customer's phone. It is also indicated that there is forgery of legal fintech logos, suspected to be carried out by illegal fintech or third parties such as former collectors who have worked at the fintech lending company where the consumer borrowed funds. The goal is to defraud legal fintech loan consumers, with promises such as if the consumer pays a certain amount of money through ATM billing, the remaining instalment arrears are considered paid off. Or instructing consumers to send a certain amount of credit to a predetermined mobile number.

In addition, another case occurred with an illegal fintech lending called KSP Hidup Hijau, where the organizer transferred money to the victim's personal account, and then after some time, the organizer demanded twice the amount of money previously sent to the victim's WhatsApp accompanied by threats, even though the victim never borrowed money from the KSP Hidup Hijau platform or any other fintech lending platform. This means that in such cases, there is acquisition of personal data that does not comply with the regulations, as well as the process of using and utilizing the data (Bayanuloh, 2023). Tongam L. Tobing, the Head of the OJK's Investment Alert Task Force, believes that the mysterious transfers made by some fintech lending occur due to several possibilities, namely:

1. The account owner once accessed an illegal fintech lending website or application and entered data, as well as gave access to all contacts and galleries even though the loan was canceled or rejected.
2. The account owner is a victim of personal data misuse by perpetrators who often distribute or buy data. In cases of personal data misuse, the public needs to be more cautious when using fintech lending platforms, and be careful when entering data on websites, fintech lending platforms, or other platforms (Buamona, 2024).

Legal Actions When There is Personal Data Misuse by Fintech Lending Providers

Litigation legal actions are legal actions taken in court. Meanwhile, non-litigation legal actions are legal actions taken outside of court. Non-litigation legal actions can be taken by filing a complaint with the financial services supervisory agency, in this case, the Financial Services Authority (OJK) if your personal data is misused by the online loan provider. Online loan providers that use personal data without the owner's consent can be subject to administrative sanctions based on POJK 77/2016. Fintech or online loan service users can report the violation to the Financial Services Authority (OJK) if there is no consent for personal

data processing or the provider does not comply with the obligations as regulated in the PDP Law and POJK 77/2016.

Meanwhile, litigation legal actions are repressive in nature, meaning they have entered the law enforcement process. Legal actions are submitted after the violation occurs with the intention of restoring or recovering. This legal action can be taken by filing a lawsuit in court. Filing a lawsuit in court is not only to sue the provider, in this case, the online loan that uses or disseminates personal data, but also to third parties or other parties that have no relation with the owner of the personal data who have stolen or misused the personal data so that compensation can be obtained from the irresponsible party. In Indonesia, before Law No. 27 of 2022 was enacted, the regulation of personal data protection was spread across several laws and regulations, including Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 on Information and Electronic Transactions, Law No. 8 of 1999 on Consumer Protection, Government Regulation No. 82 of 2012 on Electronic System and Transaction Operators, Minister of Communication and Informatics Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems (PM 2016) effective since December 2016. Legal actions (rechtshandeling) by nature are actions that can give rise to legal consequences (producing rights and obligations). If personal data from online loan services is misused, the borrower can take the following legal actions:

1) Reporting to the relevant institution

In the "Financial Services Authority Regulation (POJK) Number 10/POJK.05/2022 on Technology-Based Joint Funding Services," borrowers can report to the Financial Services Authority or abbreviated as OJK. Based on "POJK Number 10/POJK.05/2022," specifically in Article 41, essentially borrowers can report that if there is no consent/agreement to access personal data or if the fintech provider does not follow the regulations, then administrative orders will be applied to the fintech provider in the form of written warnings that can be followed by blocking all access to the management system, limiting commercial/business activities and revoking licensing by OJK. Apart from being regulated in POJK Number 10/POJK.05/2022, administrative sanctions are also regulated in "Law Number 27 of 2022 on Personal Data Protection (PDP Law)." In that law, Articles 57 and 58 essentially set administrative sanctions, as follows:

a) Written warning;
b) Temporary suspension of personal data processing operations;
c) Deleting/destroying personal data; and/or
d) Payment of administrative fines.

Borrowers whose personal data is misused can report to the relevant institution, in this case, the personal data protection organizer appointed by the President.

2) Filing a civil lawsuit

In the PDP Law, personal data subjects have rights. One of them is to sue the personal data manager and receive compensation for actions that violate the personal data processing process based on legal provisions. Apart from the PDP Law, borrowers can sue based on "Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 on Information and Electronic Transactions," specifically in Article 26 paragraphs (1) and (2), which essentially state that unless otherwise determined by legislation, any use of information through electronic support regarding personal data must be done with the consent of the concerned party. Therefore, anyone whose rights are violated can file for compensation. This is also reinforced by Article

1365 of the Civil Code, which essentially states that borrowers can file a lawsuit for misuse of personal data by filing a tort lawsuit.

3) Filing a criminal report

In the PDP Law, fintech providers who misuse borrowers' personal data in online loans must also be criminally prosecuted. Borrowers in online loan services who receive unfair treatment from fintech providers are more reluctant to report such treatment to the police. Thus, online lenders can continue their behavior in such negative treatment, such as in the form of threats and terror to the borrowers. If based on that, the authorities cannot act without a complaint from the borrower in the online loan service, assuming that the criminal act is included in the complaint offense (delik aduan). A complaint offense is a crime that can only be prosecuted if there is a complaint from the victim in a criminal act. Everyone, in this case, fintech providers, is prohibited from obtaining, showing, and/or using personal data, such as falsifying personal data that is not their own or creating false personal data in any way that is unlawful or intended for personal gain or others. This is stated in "Article 66 of the PDP Law" and continued with "Article 67 paragraphs (1), (2), and (3) of the PDP Law," which essentially state that if this is violated, criminal actions will be imposed in the form of imprisonment and/or fines. Furthermore, in "Article 69 of the PDP Law," fintech providers who violate can also be subject to other sanctions in the form of asset confiscation and other profits obtained from the crime and payment of fines. Civil damages must be compensated without being set aside or eliminated by criminal sanctions. In "Article 70 paragraphs (1), (2), (3), and (4) of the PDP Law," it essentially regulates corporate crimes, criminal law can be applied to directors, managers, principals, beneficial owners, and/or corporations. For criminal fines imposed on corporations or corporations, the maximum is ten times the maximum fine threatened. Additional penalties can also be imposed on corporations, in the form of:

a) Confiscation of profits or assets obtained or resulting from the crime;
b) Canceling all or part of the company's activities;
c) A permanent prohibition on performing certain actions;
d) Closing all or part of the company's business and/or activities;
e) Performing functions that cannot be ignored;
f) Paying compensation;
g) Revocation of rights and permits;
h) Dissolution of the company.

CONCLUSIONS AND SUGGESTION

Based on the discussion, the following conclusions and suggestions can be drawn:

1. Misuse of customers' personal data by fintech lending providers, whether operating legally or illegally, constitutes a serious violation of the law and human rights, especially the right to privacy. This act can result in criminal penalties in accordance with the provisions regulated in Law No. 27 of 2022. Personal data that is misused includes general information such as names and addresses, as well as sensitive data such as health information and criminal records. Forms of personal data misuse can occur through various methods, including the use of malware, unauthorized data access, and the dissemination of personal information without a legitimate legal basis. Cases of personal data misuse highlight the importance of stricter protection of personal data and more intensive supervision of fintech lending providers. The public also needs to be more cautious in providing personal information and using fintech lending platforms. The suggestion that can be given is that fintech companies are expected to

comply with consumer protection provisions issued by OJK. The Indonesian Fintech Association (Aftech) is also expected to supervise fintech companies under its umbrella and provide education and certification for employees and association members in the field of loan collection.

2. Legal steps that can be taken in cases of personal data misuse by fintech lending providers include two main legal routes that consumers can take: litigation and non-litigation. Non-litigation legal actions involve complaints to supervisory bodies such as OJK, where providers can be subject to administrative sanctions if proven to violate regulations related to personal data protection. Meanwhile, litigation legal actions involve court proceedings to obtain compensation or seek criminal accountability from the violating party. The applicable regulations include various laws and regulations, including the Personal Data Protection Law, the ITE Law, and other related regulations. The suggestion that can be given is that the public needs to increase their awareness of their rights related to personal data protection and the legal steps that can be taken if there is a violation by fintech lending providers.

BIBLILIOGRAPHY

Alt, R., Beck, R., & Smits, M. T. (2018). FinTech and the transformation of the financial industry. *Electronic markets*, *28*, 235-243.

Arief, B. N. (2011). *Kapita Selekta Hukum Pidana tentang Sistem Peradilan Pidana Terpadu (Integrated Criminal Justice System)*. Badan Penerbit, Universitas Diponegoro.

Azhar, D. P., & Mahyani, A. (2023). Pertanggungjawaban Pidana Korporasi Sebagai pelaku Tindak Pidana Penyebaran Data Pribadi. *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, *3*(1), 540-558.

Bank Indonesia. (2017). Peraturan Bank Indonesia No.19/12/PBI/2017 Tentang Penyelenggaraan Teknologi Finansial.

Bayanuloh, I., Junaedi, J., & Waluyadi, W. (2023). MISUSE OF PERSONAL DATA BY PEER TO PEER (P2P) LENDING PROVIDERS FROM A HUMAN RIGHTS VIEW. *HERMENEUTIKA: Jurnal Ilmu Hukum*, *7*(2), 310-323.

Buamona, M. W., & Apriani, R. (2024). Peran Hukum Terhadap Masuknya Dana Transfer Yang Bukan Hak Milik. *Jurnal Ilmiah Wahana Pendidikan*, *10*(3), 502-508.

Bukit, A. N., & Ayunda, R. (2022). Urgensi Pengesahan RUU Perlindungan Data Pribadi Terhadap Perlindungan Kebocoran Data Penerimaan SMS Dana Cepat. *Reformasi Hukum*, *26*(1), 1-20.

Dutta, N., Jadav, N., Tanwar, S., Sarma, H. K. D., Pricop, E., Dutta, N., ... & Pricop, E. (2022). Introduction to malware analysis. *Cyber Security: Issues and Current Trends*, 129-141.

Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 11-36.

Hidayat, S., Haris, O. K., Tatawu, G., & Fajar, N. (2023). Kebijakan Hukum Perlindungan Data Privasi dari Kejahatan Dunia Maya. *Halu Oleo Legal Research*, *5*(3), 985-1002.

Jafar, A. R. (2019). Fungsi Pengawasan Otoritas Jasa Keuangan (Ojk) Terkait Perlindungan Konsumen Pada Layanan Peer To Peer Landing Fintech. *Ahkam: Jurnal Hukum Islam*, *7*(2), 215-234.

Kemenkominfo. (2021, Juli). Kominfo bersama SWI telah blokir 3.193 fintech ilegal. Diakses pada 20 Maret 2024, dari https://aptika.kominfo.go.id/2021/07/kominfo-bersama-swi-telah-blokir-3-193-fintech-ilegal/

Noor, A., & Wulandari, D. (2021). Landasan Konstitusional Perlindungan Data Pribadi Pada Transaksi Fintech Lending di Indonesia. *Jurnal Ilmiah Dunia Hukum*, 99-110.

Novridasati, W., Ridwan, & Prakarsa, A. (2020). Pertanggungjawaban pidana desk collector fintech illegal serta perlindungan terhadap korban. *Jurnal Litigasi*, 21(2).

Pakpahan, H., & mindika Dwimaylando, C. (2021). Pertanggungjawaban pidana korporasi dalam cyber pornografi. *Jurnal Cakrawala Hukum*, *12*(3), 274-283.

Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik

Peraturan Otoritas Jasa Keuangan (POJK) Nomor 10 /POJK.05/2022 tentang Layanan Pendanaan Bersama Berbasis Teknologi Infomasi

Rahmi, A. A. (2020). Perlindungan Konsumen Dalam Penggunaan Layanan Pinjam Meminjam Berbasis Teknologi Peer To Peer Lending. *Badamai Law Journal*, *5*(2), 201-217.

Remy, S. S. (2006). Pertanggungjawaban Pidana Korporasi. *Gaffiti Pers, Jakarta*.

Rosmida, R. (2021, December). FINTECH: Pengawasan Bank Indonesia (BI) dan Otoritas Jasa Keuangan (OJK) perlu dimaksimalkan. In *Seminar Nasional Industri dan Teknologi* (pp. 113-120).

Samudra, A. H. (2020). Pencemaran Nama Baik Dan Penghinaan Melalui Media Teknologi Informasi Komunikasi Di Indonesia Pasca Amandemen UU ITE. *Jurnal Hukum & Pembangunan*, *50*(1), 91-105.

San Andres, E. A., & Hernando, R. C. (2019). APEC financial inclusion capacity building package-synthesis report. In *APEC financial inclusion capacity building package-synthesis report: San Andres, Emmanuel A.| uHernando, Rhea C.*. Singapore: Asia-Pacific Economic Cooperation Policy Support Unit, Asia-Pacific Economic Cooperation Secretariat.

Selvaganapathy, S., Sadasivam, G. S., & Ravi, V. (2021). A Review on Android Malware: Attacks, Countermeasures and Challenges Ahead. *J. Cyber Secur. Mobil.*, *10*(1), 177-230.

Sinaga, N. P. (2021). Perlindungan Hukum Bagi Konsumen Yang Data Pribadinya Diperjualbelikan Di Aplikasi Fintech Peer-To-Peer Lending.

Suleiman, A. (2021). Meningkatkan perlindungan konsumen fintech P2P lending berpenghasilan rendah. Center for Indonesian Policy Studies.

Suseno, A. W., & Yeti, S. (2021). Tanggung Jawab Korporasi Fintech Lending Ilegal dalam Perspektif Perlindungan Konsumen. *Law Review, XXI*, *1*, 117-144.

Syaifudin, A. (2020). Perlindungan Hukum Terhadap Para Pihak Di Dalam Layanan Financial Technology Berbasis Peer To Peer (P2P) Lending (Studi Kasus di PT. Pasar Dana Pinjaman Jakarta). *Dinamika*, *26*(4), 408-421.

Tan, D. (2021). Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum. *Nusantara: Jurnal Ilmu Pengetahuan Sosial*, *8*(8), 2463-2478.

Undang-Undang Dasar Negara Republik Indonesia 1945

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen

Undang-UndangNomor 39 Tahun 1999 tentang Hak Asasi Manusia

Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan

Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi

Wahyudi, D. (2017). Keamanan Jaringan Komputer: Malware. *Keamanan Jaringan Komputer: Malware*, *5*(5), 1-5.

Wijayanto, H., Muhammad, A. H., & Hariyadi, D. (2020). Analisis Penyalahgunaan Data Pribadi Dalam Aplikasi Fintech Ilegal Dengan Metode Hibrid. *Jurnal Ilmiah SINUS*, *18*(1), 1-10.