

Vol. 10, No. 1  
Januari 2024

#### Article History

Received: 12/12/2023

Revised: 27/12/2023

Accepted: 30/12/2023

## Misuse of Consumer Personal Data Through *Illegal Fintech Peer To Peer Lending*

Rivasya Dinda Syaiful<sup>1\*</sup>, Heru Sugiyono<sup>2</sup>

<sup>1</sup> Universitas Pembangunan Nasional "Veteran" Jakarta,

Email : [rivasyadindas@upnvj.ac.id](mailto:rivasyadindas@upnvj.ac.id)

<sup>2</sup> Universitas Pembangunan Nasional "Veteran" Jakarta,

Email : [herusugiyono@upnvj.ac.id](mailto:herusugiyono@upnvj.ac.id)

\*surel korespondensi: [rivasyadindas@upnvj.ac.id](mailto:rivasyadindas@upnvj.ac.id)

**Abstract:** This research examines the misuse of consumer personal data through illegal Fintech Peer To Peer Lending. The aim of this research is to determine aspects related to Peer-to-peer lending Fintech Companies with a focus on the problem of misuse of consumer data. By providing an in-depth overview of forms of data misuse, as well as analyzing the legal responsibilities of illegal peer to peer lending fintech providers who are involved in misuse of consumer data. The research focus based on the background in this research is; 1) What are the forms of misuse of consumer data through illegal fintech peer to peer lending according to decision number; 438/Pid.Sus/2020/PN Jkt.Utr. 2) What is the legal responsibility of individuals managing illegal peer to peer lending fintech who misuse consumer personal data according to Decision Number; 438/Pid.Sus/2020/PN Jkt.Utr. This research uses a type of normative juridical research using qualitative methods and analytical descriptive approaches. So that the analysis can be carried out, the author first collects materials that are appropriate to the legal issue to be studied. The research results show that illegal fintech operators often misuse consumer data by involving third parties who do not have official certification, giving rise to intimidation, threats and defamation of consumers. In addition, the practice of requesting consumer consent to access personal data in violation of certain regulations was also exposed. The conclusion of this research confirms that this act can be subject to criminal sanctions as stated in the court decision. It is hoped that legal enforcement of this practice can be an effective step to protect consumer data and prevent abuse in the peer-to-peer lending fintech industry.

**Keywords:** Misuse of personal data; illegal fintech peer-to-peer lending; positive law in Indonesia.

### INTRODUCTION

The development of technology in the economic sector by utilizing the internet raises

a variety of sites and products that aim to facilitate the economy, shorten transactions, and efficiency over time and distance<sup>1</sup>. One of the products in the economic field that utilizes technological developments and the internet and is an innovation in the economic field, especially in financial services is financial technology (Fintech)<sup>2</sup>.

Fintech itself is an industrial technology-based financial service that uses software to provide services and services in the financial sector. These fintech companies are often founded with a mission to break and change the perspective of the conventional financial system and industry players who do not utilize software optimally and optimally<sup>3</sup>.

Fintech in Indonesia is regulated in Bank Indonesia Regulation No. 19/12/PBI of 2017 Article 1 paragraph (1) concerning the Implementation of Digital Financial Services which states that financial technology is the use of technology for the financial system that produces the latest commodities, services, technology, and/or business schemes that are beneficial for financial stability, monetary stability, efficiency, smoothness, protection and credibility of the payment system<sup>4</sup>. Other fintech-related instruments include payment rules, marketing, investment management and risk management, lending and borrowing, and business fund investment.

The implementation of Fintech in Indonesia is contained in the Financial Services Authority Regulation (POJK) Number 77/POJK.01/2016 which consists of a. Market aggregators; b. Cash, transfer, clearing, and settlement. c. Risk management and investment management. d. Crowdfunding and peer-to-peer lending (P2P Lending).

Of the several services in fintech, one of the most rapidly growing is peer-to-peer lending, which is an agreement to borrow and borrow funds as well as conventional lending and borrowing money, but interested parties do not have to meet in person because there are organizers who bring them together virtually to carry out the process of borrowing funds<sup>5</sup>. The existence of peer-to-peer lending activities in fintech makes it easier for the Indonesian people to process money or credit lending very easily, time efficiently, and shorten other procedures set by conventional financial institutions that do not utilize financial technology<sup>6</sup>.

However, on the other hand, fintech and peer-to-peer lending activities that can help facilitate activities and accelerate the economy can also be a tool for carrying out criminal

---

<sup>1</sup> Siyu Ren et al., "Digitalization and Energy: How Does Internet Development Affect China's Energy Consumption?," *Energy Economics* 98 (2021): 105220.

<sup>2</sup> M Broto Legowo, S Subanija, and Fangky Antoneus Sorongan, "Role of FinTech Mechanism to Technological Innovation: A Conceptual Framework," *International Journal of Innovative Science and Research Technology* 5, no. 5 (2020): 1–6.

<sup>3</sup> Sharad Sinha, "A Glimpse into the World of Fintech Accelerators? The Open Vault at OCBC," *IEEE Potentials* 36, no. 6 (2017): 20–23.

<sup>4</sup> Bank Indonesia, "Bank Indonesia Regulation No. 19/12/2017 on the Implementation of Financial Technology (2017)(Indonesian)" (2017).

<sup>5</sup> Nofie Iman, "Financial Technology and Financial Institutions," *Gathering of the Bank Syariah Mandiri Hotel Grand Aston Yogyakarta Linkage Partners* 22 (2016).

<sup>6</sup> Damanhuri Fajril Mukhtar and Yuliasuti Rahayu, "Analisis Pendanaan Modal Umkm Melalui Financial Technology Peer To Peer Lending (P2P)," *Jurnal Ilmu dan Riset Akuntansi (JIRA)* 8, no. 5 (2019).

activities. One of the unlawful actions by utilizing fintech peer-to-peer lending is creating peer-to-peer lending fintech applications without permission and managing them illegally as well as misuse of consumer/client personal data. This can be done by illegally disseminating personal data from customers containing customer photos, important information listed on Identity Cards, or even Family Card numbers. For example, there is a case of leakage of personal information of illegal peer-to-peer lending fintech users at PT. Barracuda Fintech Indonesia in collaboration with desk collector company PT. Vega Data Indonesia with its products called the Cash Shop application, Kascas, Toko Tunai, Lion Teck, Pysicomfort, Doku Alliance, Koo Cash, Stay Ready, Green Elephant, Ko Rupiah, Dompot Kartu, Planet Bahagia, and Duit Season is an online loan provider application whose billing work procedure is by accessing all data on the customer's cellphone. This is because there are provisions that allow some illegal peer-to-peer fintech applications to access every data and information from customers who download them<sup>7</sup>.

Customers who want to borrow money through one of these applications are required to agree to access to retrieve cellphone data, contact data, and pictures on the device, fill in personal data such as full name, place and date of birth, home address, and customer profession under the identity card<sup>8</sup>. Furthermore, customers must also provide photos along with customer ID cards, write account numbers, and proof that customers have worked, as well as 2 customer emergency contacts that can be contacted. After the customer successfully registers where the customer submits an account as a place to withdraw money from one of the applications, then the application has access to the customer's personal information.

All of these applications also utilize transaction payments through e-commerce applications that can authorize various types of payments including payment gateways such as Xendit, Bluepay, and Doku applications. The fintech peer-to-peer lending application above will also provide a virtual account number in the name of PT Vega Data Indonesia from several types of banks such as Bank Mandiri, Bank Rakyat Indonesia, Bank Nasional Indonesia, and Bank Central Asia for borrowers who will pay off debts within 7-14 working days.

Customers who have overdue their debts and have not paid off the loan are contacted by PT. Barracuda Fintech Indonesia through the Desk Collector (DC) from PT. Vega Data Indonesia will access the task feature contained in the application to find the borrower's personal information. The next desk collector action for overdue customers is to advise them to immediately pay their debts through a payment gateway, if there are customers who borrow money and it has matured for more than 30 days, then PT. Vega Data

---

<sup>7</sup> Fery Suryono and Rineke Sara, "Application of Authentication in Peer to Peer Lending Fintech Transactions to Maintain the Confidentiality of Personal Data," in *Proceedings of the First Multidiscipline International Conference, MIC 2021, October 30 2021, Jakarta, Indonesia, 2022*.

<sup>8</sup> Nur Aza Musamma, "Perlindungan Hukum Terhadap Debitur (Nasabah) Dalam Perjanjian Kredit Tanpa Agunan Di Aplikasi Digital Akulaku (Studi Kasus Pengguna Aplikasi Akulaku Di Kabupaten Jember)." (Fakultas Syari'ah Program Studi Hukum Ekonomi Syariah (Muamalah), 2021).

Indonesia through its desk collector will spread slander and terrorize customers' families and relatives through the WhatsApp application which later they will berate and vilify their names through calls and messages.

The next case is the act of illegal peer-to-peer fintech that sells consumers' data. The sale of personal data carried out by this illegal fintech is widely circulated on social media. This is in line with the statement of cyber security observers from Vaksin.com Alfons Tanujaya to CNN Indonesia<sup>9</sup>.

According to data obtained from the Indonesian Consumer Foundation Foundation, complaints about misuse of personal data are one of the reports that are widely carried out by the public. The misuse of consumer personal data as much as 70% is carried out by illegal online loan companies. Meanwhile, the OJK Investigation Alert Task Force has stopped operating around 3,365 illegal peer-to-peer lending fintechs.

Based on the background description above, some of these cases have violated Law Number 8 of 1999 concerning Consumer Protection and Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 20 of 2016 Article 1 paragraph (1) and Financial Services Authority Regulation Number 1 / POJK.07 / 2013 concerning Consumer Protection in the Financial Services Sector Article 31 and companies can be held liable according to Article 29 and Article 30. Given the risk of customer data problems, the author wants to further examine the problem with a study entitled "Misuse of Consumer Personal Data Through Illegal Fintech Peer-to-Peer Lending".

The purpose of this study is to investigate certain aspects related to Fintech Peer to peer-to-peer lending companies with a focus on the issue of misuse of consumer data. First, this study aims to provide an in-depth picture of the forms of data misuse that may occur by Fintech Peer to peer-to-peer lending companies. Second, this study aims to analyze the legal responsibility of illegal peer-to-peer lending fintech organizers involved in the misuse of consumers' data. By exploring it, this research is expected to contribute to legal understanding related to consumer data protection and provide a basis for improving policies and legislation related to the practice of Fintech Peer to peer-to-peer lending in Indonesia.

To serve as study material, in this section the researcher takes several previous studies that have a correlation with the author's research. The previous research by Laela Dwi Cahyani<sup>10</sup> with the title "Responsibility of providing services for the confidentiality of personal data for Google service users" Faculty of Law, Yogyakarta Islamic University with a discussion of the legal relationship system between service providers and Google service

---

<sup>9</sup> CNN Indonesia, "Waspada Aksi Jual Beli Data Pribadi Lewat Aplikasi Fintech," *Cnnindonesia.Com*, last modified 2019, <https://www.cnnindonesia.com/teknologi/20190729082602-185-416323/waspada-aksi-jual-beli-data-pribadi-lewat-aplikasi-fintech>.

<sup>10</sup> Laela Dwi Cahyani, "Tanggung Jawab Penyediaan Layanan Atas Kerahasiaan Data Pribadi Terhadap Pengguna Layanan Google" (2019).

users, namely service users. Google whose Gmail account is linked to the user's Google account on the same device, the user is required to agree to the "Google Terms of Service" which contains the rights and authorities of both parties. If there are no regulations that expressly prohibit it, then the Google Service Provider is not responsible for any losses that occur to users in terms of financial, information and personal data so that there is no compensation from Google either legally or otherwise. The similarity of Laela Dwi Cahyani's research is that it discusses the protection of consumers' personal data through the Information and Electronic Transactions Law as well as the construction of relationships with third party service providers, while the differences lie in the services used as research objects and the agreements for each internet application.

Research written by Erwin Asmadi<sup>11</sup> with the title "Misappropriation of personal data in the use of financial technology applications (online loans)" Faculty of Law, Muhammadiyah University of North Sumatra with a discussion of forms of personal data deviation in the use of fintech applications (online loans) between On the other hand, the organizers of legal and illegal online loan companies not only access all data on customers' cellphones, but also carry out intimidation, terror, and carry out unpleasant acts and slander by collectors against debtors who borrow funds. Apart from that, there are indications of attempted fraud, allegedly carried out by third parties or illegal online loans against consumers borrowing funds from legal fintech, by faking the logo of the organizer of the fintech lending company from which the consumer borrowed funds. The solution to minimizing personal data irregularities in the use of fintech applications (online loans) is none other than strict law enforcement against perpetrators, both corporate and individual, who misuse personal data without their rights. The similarity of Erwin Asmadi's research is that it discusses the protection of consumers' personal data through Financial Technology (Fintech) applications and relationships with third party service providers, while the difference lies in the organizers of the online companies that are used as the object of online loan research.

Research from Dwi Fidhayanti<sup>12</sup> with the title "Bank Indonesia Supervision of Confidentiality of Fintech Consumer Data in the Mobile Payment Sector", Journal of Law and Sharia volume 11 No. 1 of 2020. With research results showing that mobile payment transactions in fintech are still correlated with banks so that the regulations used are still the same as the regulations used by banks. The type of research used is normative legal research or literature, namely with a statutory approach and a conceptual approach. What research has in common with researchers lies in the form of legal protection for personal data held by customers in credit agreements. The difference lies in the research object, Dwi Fidhayanti focuses on peer-to-peer lending fintech applications.

---

<sup>11</sup> Erwin Asmadi, "Penyelewengan Data Pribadi Dalam Pemanfaatan Aplikasi Financial Teknologi (Pinjaman Online)," in *Seminar Nasional Hukum, Sosial Dan Ekonomi*, vol. 2, 2023, 135–142.

<sup>12</sup> Dwi Fidhayanti, "Pengawasan Bank Indonesia Atas Kerahasiaan Dan Keamanan Data/Informasi Konsumen Financial Technology Pada Sektor Mobile Payment," *Jurisdictie* 11, no. 1 (2020): 16.

## RESEARCH METHODS

The method used by researchers in this research is normative legal research. Normative legal research is research based on secondary data. The nature of this research is descriptive, which aims to provide an overview of the symptoms of minimizing personal data irregularities in the use of fintech applications. The data sources for this research are primary legal materials, secondary legal materials and tertiary legal materials. Primary sources include directly applicable legal rules, such as laws and court decisions. For example, a decision related to illegal fintech peer to peer lending has been issued under Decree number 438/Pid.Sus/2020/PN Jkt.Utr., which highlights the misuse of consumers' personal data. Secondary sources include interpretations and analyses of legal rules, such as law books, journals, and case summaries. On the other hand, tertiary sources offer a general view or basic information about the law, such as a legal encyclopedia or legal dictionary. The data collection method was carried out using document study techniques and analyzed using qualitative analysis techniques.

## DISCUSSION

### 1. Forms of Misuse of Consumer Data Fintech Companies Peer-to-Peer Lending

Along with the development of technology, it also has an impact on changing human interaction systems such as business, financial, and social communication. Today's sophisticated technology also makes it easier for humans to do work in various fields. However, the adverse effects result in the emergence of new crimes, for example in the case of online loans. Starting to appear since 2014, online loans that seem easy without having to go to the bank and only use the internet network without applying directly make many people tempted and take advantage of the convenience presented by online loans.

The number of people who switch to borrowing on online loans rather than at banks has triggered the emergence of online crime. One of the criminal acts that is often reported by victims of online loans is the misuse of data.

After researchers analyzed one of the factors for the occurrence of criminal misuse of data by online loan companies, it is often caused by the debtor's lack of caution. The debtor's carelessness referred to here is such as not checking and knowing online loans that are registered with the OJK and have not been registered, besides that the cause of this criminal act of misuse of personal data is that the debtor does not pay off installments according to the initial agreement that has been agreed.

Personal data that has been obtained by online loan companies by misused customers has several forms. After the author observes here are some of its forms:

#### a. Using third parties in billing matters

The dissemination of consumer personal data usually begins with a delay in the debtor/consumer in paying bills or even defaulting. Delays and defaults from consumers make illegal online loan companies collect them by harming consumers, namely spreading their data to third parties and terrorizing them as if consumers or pictured are fugitives.

In terms of billing, generally, peer to peer-to-peer lending fintech companies use third parties, namely desk collection services. Using a third party in debt collection by banks is common but in the case of PT. Barracuda Fintech Indonesia in the decision Number 438 / Pid.Sus / 2020 / PN Jkt. Utr researchers found there was a problem in terms of third parties because they did not have certification from the Indonesian Joint Funding Fintech Association. After all, the desk collector company was also illegal. In illegal desk collector service provider companies, employees do not go through proper training and certification stages, so their billing methods seem unlawful.

b. Intimidating and threatening consumers

In the decision of case Number 438/Pid.Sus/2020/PN Jkt.UTR, Dede Supardi Bin H. Supriadi who is an employee in the desk collection section of PT. Vega Data Indonesia or PT. Barracuda Fintech Indonesia, which is in charge of collection, revealed the chronology of violations committed, namely violations beginning with granting permission to access cameras and galleries on consumer devices, desk collections use this to take photos or videos that are considered Sara and pornographic. Then the collection desk will threaten consumers by spreading their data and photos to several social media so that these consumers feel afraid and immediately pay debts.

In the ITE Criminal Code, all actions that use threats of violence or other similar acts are intended for someone to do something, namely in this case it is intended that customers pay debts can be qualified as suspected criminal acts. The general provisions referred to are the Kiab Law on Information and Electronic Transactions Article 45 paragraph (4) jo. Article 27 paragraph (4) of the ITE Law or Article 45B jo. Article 29 of the ITE Law expressly prohibits everyone from sending, distributing, transmitting, and/or making accessible electronic documents that contain the use of violence, threats of violence, and/or unpleasant treatment to force others to do something.

c. Misusing emergency contact numbers that have been registered by consumers to spread slander and incite hatred or hostility

A common problem when billing is that desk collectors collect consumer or debtor debtors by contacting other people who have nothing to do with the borrower, the phone number obtained by the desk collector is obtained from the contact access of the defaulting borrower which of course is done without the permission and knowledge of the consumer.

In this case, the online loan company is negligent and violates the law because it accesses personal data or contacts on the cellphone without the relevant consent. The billing carried out by Dede Supardi Bin H. Supriadi in the decision Number: 438 / Pid.Sus / 2020 / PN Jkt. Utr as a desk collection employee of PT Vega Data Indonesia in collaboration with PT Barracuda Fintech Indonesia which is engaged in an illegal peer-to-peer lending fintech business called Toko Tunai and Kascash is also an unreasonable collection, the article in billing through emergency contacts is carried out by spreading slander that the victim does not want to Pay the debt to the fintech company while the debt is not yet due and the owner of the debt can still be contacted by the desk collector.

In the evidence obtained from the witness, it is true that the collection desk sent collection messages and spread disgrace regarding the debts receivable of the parties concerned. The cases of dissemination mentioned above are the most common cases encountered in the online lending process, especially illegal ones.

d. Request consumer consent to access personal data

Based on the information of expert Alvin Leonardo Ezra. T in decision Number 438 / Pid.Sus / 2020 / PN Jkt.Utr that the request to access consumer personal data including the contact list contained on the consumer's cellphone is not justified because it has been regulated in the letter of the Director of Fintech Regulation, Licensing, and Supervision Number: S-72 / NB.213 / 2019, dated February 12, 2019, regarding the order to limit access to personal data on the smartphone of fintech lending users. All that is allowed by fintech companies is to access cameras, locations (GPS-location and GSM-IMEI), and microphones.

e. Disseminate personal data by trading it

Not only contacting but often online loan companies will also distribute photos and ID cards of borrowers to the contacts they access. The fact of disseminating consumers' data has been proven by the Co-Founder of Digikai Studio, Yoshua Markus Mariwu who deliberately borrowed from several illegal online loans to investigate the application and workings of illegal online loans<sup>13</sup>.

Then 4 people allegedly bought 150 ID card data from online loans and then committed E-Commerce credit fraud in Jakarta since June 2021. This crime is a fraud under the guise of data theft. Crimes are committed by buying goods in the form of mobile phones or gold that are easily resold and then using the home credit payment method with the date purchased<sup>14</sup>. The data leak of 1.3 million data by HAC is one of the data leaks highlighted by the public during the pandemic. This data should be used to track COVID-19 to meet various aviation administration needs<sup>15</sup>. In addition to disseminating consumer personal data, illegal online loan companies also have the potential to do more harm to consumers borrowing funds. Unethical illegal online loans will also sell the personal data of consumers borrowing funds.

## **2. Legal liability of illegal peer-to-peer lending fintech providers who misuse consumers' data**

There are several violations related to consumer personal data of online loan application service users. Consumers or debtors who have loans get poor collection methods by utilizing personal data in the loan collection process, namely by contacting the contact

---

<sup>13</sup> Econimics, "Alert! The Dissemination of Personal Data, Illegal Pinjos Are Interconnected," *Channel.Com*, accessed November 3, 2023, <https://www.idxchannel.com/economics/waspada-penyebaran-data-pribadi-pinjol-ilegal-interconnected->.

<sup>14</sup> James Treadwell, "From the Car Boot to Booting It up? eBay, Online Counterfeit Crime and the Transformation of the Criminal Marketplace," *Criminology & Criminal Justice* 12, no. 2 (2012): 175–191.

<sup>15</sup> Kaitano Dube, Godwell Nhamo, and David Chikodzi, "COVID-19 Pandemic and Prospects for Recovery of the Global Aviation Industry," *Journal of Air Transport Management* 92 (2021): 102022.



number contained on the customer's device or cellphone without permission from the customer-owner because the contact number is not a contact number that has been registered as an emergency when the loan owner cannot be contacted by the collector.

In accounting for a criminal act, a person will not be convicted if he does not meet the element of guilt. This is in line with the two principles contained in criminal acts, namely *actus reus* and *mens rea*<sup>16</sup>. His actions must be contrary to the law and the existence of an element of guilt whether it is mistreatment or negligence is two elements a person can be punished and his actions can be held accountable.

This is also under the opinion expressed by Hasbullah F. Sjawie, Masrudi Muchtar relates theoretically based on the theory of criminal responsibility. The criminal liability imposed on debt collectors is individual (naturalized person) and must imply that the perpetrator can be reproached (*verwijtbaaheid*) based on his actions. This principle in criminal law is known as the principle of liability based on fault<sup>17</sup>.

Relating to the case made by desk collector Dede Supardi Bin H. Supriadi who works as a desk collector of PT. Vega Data Technology Indonesia researchers observed that in this case there was an element of error in the form of immoral content through electronic media. So that the actions of some of these desk collectors can be criminally accounted for.

Based on information from the OJK Financial Services Sector Investigation Department Team, providing information that fintech peer-to-peer lending that has been registered and licensed by the Financial Services Authority is only allowed to access voice, location, and cameras from its customers. While the company PT. Vega Data Technology Indonesia has violated the rules because the desk collectors recruited by the company themselves not only access these three things but access all data from the borrowers' mobile phones and collect virtually through telephone networks or mobile phones and the internet.

Deeds committed by PT. Vega Data Technology Indonesia in collaboration with PT. Barracuda Fintech Indonesia to three of its customers, namely Mahdi Ibrahim and Bayu Prasetya, is proof of how billing carried out by fintech desk collectors is against the law. Based on information submitted by the Investigation Team, Ditipidcyber Bareskrim Mabes Polri stated that if customers do not pay their debts until maturity, illegal fintech companies will access all debtor data through Supercash. co/Banshe. After obtaining victim or customer data, PT. Vega Data Technology Indonesia creates group chats through the WhatsApp application with its members consisting of colleagues and relatives of debtors. The creation of WhatsApp group chats is utilized by PT. Vega Data Technology Indonesia to send data from Agus Rifaid as supervisor in the form of photos of debtors, documents needed to register as well as photos, videos, and short messages containing pornographic elements. Some messages that contain elements of insult include such as "mailing bitch, cave swear family meat until death", "dog bangs at ga need lu to pay devil children to finish off all your

---

<sup>16</sup> Muhammad Ridwan Lubis, Panca Sarjana Putra, and Yasmirah Mandasari Saragih, "Corporate Criminal Liability for Criminal Acts of Corruption," *Jurnal Pembaharuan Hukum* 8, no. 1 (2021): 48–59.

<sup>17</sup> Masrudi Muchtar, *Debt Collector Dalam Optik Kebijakan Hukum Pidana* (Aswaja Pressindo, 2013).

devil children", "don't have to pay devils, which is clear your family has slaughtered all caves" and through voice messages or voice notes with words such as "woy dog lu, Don't pay either", "Dog Bitch", "son of Satan" which are insults to the victim.

The absence of clear rules in Indonesia regulating the procedures for implementing the billing of a desk collector makes it illegal for desk collectors to do things that violate the law and are contrary to the company's agreement. Even though the desk collector's job is only limited to collecting debtors or borrowers. However, the misuse of legal regulations carried out by desk collectors in the collection process can refer to Bank Indonesia Circular Letter Number 14/2/PBI Year 2012 Article 178B Paragraph (2)) concerning Amendments to Bank Indonesia Circular Letter Number 11/10/DASP Year 2009 concerning the Implementation of Payment Instrument Activities Using Cards, which reads "Credit Card Issuers must guarantee that Credit Card debt collection, whether conducted by the Credit Card Issuer itself or using a collection service provider, carried out under Bank Indonesia regulations and applicable laws and regulations."<sup>18</sup>

Based on the provisions of Article 27 of Law No. 19 of 2016 concerning Electronic Information and Transactions or the ITE Law, actions committed by desk collectors to their customers whom the researchers described above have violated the law and are criminal offenses. The content in Article 27 Paragraphs (1) to (4) of Law No. 19 of 2016 regulates the prohibition of distributing and/or transmitting and/or making accessible electronic information that has the content of decency, gambling, insults, and/or defamation and extortion and/or threats<sup>19</sup>.

Based on the prohibitions contained in Article 27 of Law Number 19 of 2016 above the desk collector of PT. Vega Data Technology Indonesia violates the provisions of Paragraphs (3) and (4). Desk collectors who disseminate and send messages accompanied by slanderous sentences to customers' relatives in WhatsApp chats violate the provisions of Article 27 Paragraph (3) of Law No. 19 of 2019, namely distributing and/or transmitting and/or making accessible electronic information and/or electronic documents that have the content of insult and/or defamation. Because in the way of billing, desk collectors send messages full of insults and defamation tones to customers and even customers' families.

Not only that, the desk collector of PT. Vega Data Indonesia also sent a threatening message stating that if customers have not been able to pay off their debts, there will be a WhatsApp group next and told to wait every six hours. This of course violates the provisions of Article 27 Paragraph (4), namely intentionally and without the right to distribute and/or transmit and/or make accessible information and/or electronic documents that have the content of blackmail and/or threats.

---

<sup>18</sup> Acep Rohendi, "Reporting Obligation of Credit Card Transaction: Perspective of Bank Secrecy and the Government Regulation in Lieu of Law No 1/2017 on the Access to Information for Taxation Purposes," *PADJADJARAN JURNAL ILMU HUKUM (JOURNAL OF LAW)* 5, no. 1 (2018): 143–163.

<sup>19</sup> Law Number, "Of 2016 Concerning Amendments to Law Number 11 of 2008 Concerning Information and Electronic Transactions," *the Minister of Law and Human Rights of the Republic of Indonesia* 10, no. 4 (19AD).

Regarding messages on WhatsApp that contain these threats, based on observations, the author also violates the provisions of Article 29 of Law No. 19 of 2016 concerning Electronic Information and Transactions. Because desk collectors deliberately send threatening messages to scare customers who have not paid debts.

Based on the results of the researcher's study above about desk collectors in terms of Law No. 19 of 2016 concerning Electronic Transaction Information, the criminal liability that desk collectors must undergo must be under the provisions of Article 45 of Law No. 19 of 2016 Paragraph (1) and Paragraph (3) because they violate Articles 27 and 29 of the ITE Law. Therefore, criminal liability for violating Article 27 of Law No. 19 of 2016 is a maximum of 6 (six) years imprisonment and/or a maximum fine of Rp.1,000,000,000 (one billion rupiah). Then the legal responsibility for the provisions of Article 29 of Law No. 19 of 2016 is under the provisions of Article 45 Paragraph (3) of Law No. 19 of 2016, which is sentenced to imprisonment for 12 (twelve) years and/or a maximum fine of Rp.2,000,000,000 (two billion rupiah).

In addition to the desk collector who must carry out legal or criminal responsibility for what is done to customers, the party who gives power of attorney and has a correlation to the desk collector in the debt collection process must also account for his actions to provide a deterrent effect on the perpetrators of criminal acts. In this case, the researcher refers to the court decision in the case of PT. Barracuda Fintech Indonesia in collaboration with PT. Vega Data Indonesia in terms of billing. Namely Decision Number 438 / Pid.Sus / 2020 / PN Jkt.UTR.

## **CONCLUSION**

This study discusses the negative impacts and violations of the law associated with illegal practices in the use of fintech peer-to-peer lending. The results showed that illegal fintech organizers often misuse consumer data by involving third parties who do not have official certification, resulting in intimidation, threats, and damage to the good name of consumers. In addition, the practice of seeking consumer consent to access personal data in violation of certain regulations was also disclosed. The conclusion confirms that such actions are subject to criminal penalties, as described in the Court Judgment. Law enforcement against these practices is expected to be an effective measure to protect consumer data and prevent abuse in the peer-to-peer lending fintech industry.

## **REFERENCE**

- Asmadi, Erwin. "Penyelewengan Data Pribadi Dalam Pemanfaatan Aplikasi Financial Teknologi (Pinjaman Online)." In *Seminar Nasional Hukum, Sosial Dan Ekonomi*, 2:135–142, 2023.
- Cahyanni, Laela Dwi. "TANGGUNG JAWAB PENYEDIAAN LAYANAN ATAS KERAHASIAAN DATA PRIBADI TERHADAP PENGGUNA LAYANAN GOOGLE" (2019).
- Dube, Kaitano, Godwell Nhamo, and David Chikodzi. "COVID-19 Pandemic and Prospects for

- Recovery of the Global Aviation Industry." *Journal of Air Transport Management* 92 (2021): 102022.
- Economics. "Alert! The Dissemination of Personal Data, Illegal Pinjos Are Interconnected." *Channel.Com*. Accessed November 3, 2023. <https://www.idxchannel.com/economics/waspada-penyebaran-data-pribadi-pinjol-ilegal-interconnected->.
- Fidhayanti, Dwi. "Pengawasan Bank Indonesia Atas Kerahasiaan Dan Keamanan Data/Informasi Konsumen Financial Technology Pada Sektor Mobile Payment." *Jurisdictie* 11, no. 1 (2020): 16.
- Iman, Nofie. "Financial Technology and Financial Institutions." *Gathering of the Bank Syariah Mandiri Hotel Grand Aston Yogyakarta Linkage Partners* 22 (2016).
- Indonesia, Bank. "Bank Indonesia Regulation No. 19/12/2017 on the Implementation of Financial Technology (2017)(Indonesian)" (2017).
- Indonesia, CNN. "Waspada Aksi Jual Beli Data Pribadi Lewat Aplikasi Fintech." *Cnnindonesia.Com*. Last modified 2019. <https://www.cnnindonesia.com/teknologi/20190729082602-185-416323/waspada-aksi-jual-beli-data-pribadi-lewat-aplikasi-fintech>.
- Legowo, M Broto, S Subanija, and Fangky Antoneus Sorongan. "Role of FinTech Mechanism to Technological Innovation: A Conceptual Framework." *International Journal of Innovative Science and Research Technology* 5, no. 5 (2020): 1–6.
- Lubis, Muhammad Ridwan, Panca Sarjana Putra, and Yasmirah Mandasari Saragih. "Corporate Criminal Liability for Criminal Acts of Corruption." *Jurnal Pembaharuan Hukum* 8, no. 1 (2021): 48–59.
- Muchtar, Masrudi. *Debt Collector Dalam Optik Kebijakan Hukum Pidana*. Aswaja Pressindo, 2013.
- Mukhtar, Damanhuri Fajril, and Yulastuti Rahayu. "Analisis Pendanaan Modal Umkm Melalui Financial Technology Peer To Peer Lending (P2P)." *Jurnal Ilmu dan Riset Akuntansi (JIRA)* 8, no. 5 (2019).
- Musamma, Nur Aza. "Perlindungan Hukum Terhadap Debitur (Nasabah) Dalam Perjanjian Kredit Tanpa Agunan Di Aplikasi Digital Akulaku (Studi Kasus Pengguna Aplikasi Akulaku Di Kabupaten Jember)." Fakultas Syari'ah Program Studi Hukum Ekonomi Syariah (Muamalah), 2021.
- Number, Law. "Of 2016 Concerning Amendments to Law Number 11 of 2008 Concerning Information and Electronic Transactions." *the Minister of Law and Human Rights of the Republic of Indonesia* 10, no. 4 (19AD).
- Ren, Siyu, Yu Hao, Lu Xu, Haitao Wu, and Ning Ba. "Digitalization and Energy: How Does Internet Development Affect China's Energy Consumption?" *Energy Economics* 98 (2021): 105220.
- Rohendi, Acep. "Reporting Obligation of Credit Card Transaction: Perspective of Bank Secrecy and the Government Regulation in Lieu of Law No 1/2017 on the Access to Information for Taxation Purposes." *PADJADJARAN JURNAL ILMU HUKUM (JOURNAL OF LAW)* 5, no. 1 (2018): 143–163.
- Sinha, Sharad. "A Glimpse into the World of Fintech Accelerators? The Open Vault at OCBC." *IEEE Potentials* 36, no. 6 (2017): 20–23.
- Suryono, Fery, and Rineke Sara. "Application of Authentication in Peer to Peer Lending

Fintech Transactions to Maintain the Confidentiality of Personal Data." In *Proceedings of the First Multidiscipline International Conference, MIC 2021, October 30 2021, Jakarta, Indonesia, 2022*.

Treadwell, James. "From the Car Boot to Booting It up? EBay, Online Counterfeit Crime and the Transformation of the Criminal Marketplace." *Criminology & Criminal Justice* 12, no. 2 (2012): 175–191.