Analysis of Legal Protection of Borrower's Personal Data in Online Loan Application Services (A Case Study of PT. BFI)

Ardyanus Hartony Laos[1] Ariawan Gunadi[2*]

[1] *Faculty of Law, Trisakti University, Jakarta, Indonesia*
[2]*Faculty of Law, Universitas Tarumanagara, Jakarta, Indonesia*
[*]*Corresponding author. Email: ariawang@fh.untar.ac.id*

ABSTRACT
In online loan application services (Fintech, many people have complained about problems regarding the dissemination of personal data carried out by online loan organizers (Fintech Companies) without confirmation and permission of the data owner. In this regard, it is important to study the legal protection of borrowers' personal data in online loan application services, and sanctions for breaches of personal data. The purpose of this thesis research is to examine the legal protection of the borrower's personal data in online loan application services. The method that will be used in writing this thesis is a normative research method with a statutory and a facts approach. The study result shows that legal protection and sanctions for breaches of personal data are regulated in Law no. 19 of 2016 and its amendments regarding Information and Electronic Transactions, and in the Financial Services Authority Regulation No. 77 / POJK.01 / 2016 concerning Information Technology-Based Lending and Borrowing Services, which is affirmed in Article 26, stated that: "The organizer is responsible for maintaining the confidentiality, integrity and availability of user's personal data and in its use must obtain approval from the owner of the personal data unless otherwise stipulated. by the provisions of laws and regulations.The integrity and availability of user's personal data and in its use must obtain approval from the owner of the personal data unless otherwise specified. by the provisions of laws and regulations ". integrity and availability of user's personal data and in its use must obtain approval from the owner of the personal data unless otherwise specified. by the provisions of laws and regulations.

Keywords: *legal protection, personal data, online loan*

1. INTRODUCTION

With the current industrial revolution 4.0, technological developments are no longer limited, more perfect with the emergence of Fintech (financial technology) . Fintech term is a type of financial service that uses technology that will definitely make it easier for people to carry out various transactions that can be done anywhere and anytime . With the convenience offered, many people are now switching from conventional loans through banks to loans made online by utilizing an electronic system of loans that are carried out online, not requiring prospective debtors to provide collateral (collateral) to the organizer/business operator. Financial technology loans. Even though there are so many conveniences offered by this online loan, it cannot be denied that there are risks that arise in the form of the use of personal data without the consent of the owner of personal data and the company as a business actor that provides online loan services is an illegal company. An example of a case that has occurred is the case between “PT BFI and a victim named MI. PT BFI or PT VD is a company engaged in financial technology (Fintech), conducting information technology-based business activities that provide online loans. The application used by the company in terms of providing online money loans to consumers is "Card Wallet" where this application can be accessed via mobile phones by downloading it on the Playstore. Initially in August 2019 the victim named MI received an SMS message from an application called card wallet which offered an Online (Internet)-based money loan to the victim, then because the victim was in need of money, the victim immediately clicked on the link in the SMS. then the victim is immediately redirected to the playstore (application) and told to download the card wallet application, after the victim clicks OK to download it, then the application exits the registration as a requirement to be able to make an online loan by stating: Name, residential address, office address, telephone number, salary slip, and NPWP. after that the victim's witness was ordered;/ directed to take a photo of the ID card and a selfie photo (self-portrait using a cellphone)

so that the victim's witness' face could be seen . After the victim's witness download the card wallet application and completes all the requirements, the victim immediately applies for an online loan in the application of "Rp. 1,500,000, - (one million five hundred thousand rupiah)", after being verified by the card wallet application, the victim is only given a loan of Rp. 1.050.000,- (One million and fifty thousand rupiah), which then the loan will be repaid within a period of 14 Days, but less than H-1 (Less than one day) due for payment, PT Barracuda FINtech Indonesia through its deputy director named (DXL alias TDY) provided personal data from the victim as well as all telephone numbers in the victim's cellphone to PT employees to collect the debt. After being given data of the victim, the employee from PT immediately called the victim to remind the victim that the loan was due for payment and also the employee made a phone call to the relatives and friends of the victim stated that the victim had debts. Then on December 16th 2019, the employee contacted the victim with the number 082149920291 and had a chat with harsh and threatening words, namely "will kill the victim and will mutilate the victim. If he gets caught, the victim will be stabbed, tonight I challenge you and tell me to bring a knife to kill." Not only that, in carrying out its business activities, PT Barracuda Fintech Indonesia is not registered/has a business license from the OJK in accordance with the provisions of "Article 7 Jo Article 8 POJK No.77/ POJK.01 / 2016 concerning Information Technology-Based Lending and Borrowing Services.[1] Along with this background, the author is interested in making a Research/Thesis with the title: Legal Protection of Borrower's Personal Data in Online Loan Application Services (Case Study of PT BFI)
This research discusses legal protection of borrowers or debtors personal data that missused by Online Loan Application and their existence in Financial Services Authority OJK. The research question is: What is the legal responsibility of PT BFI as a business actor for the misuse of consumer personal data? How is Law No. 19 of 2016 and its related regulations protect consumer personal data of Fintech users from misuse of personal data?

2. METHOD

"The research method used by the author in this thesis research is "Normative" legal research. Normative legal research is a research process to find the rule of law, legal principles, and legal doctrines to answer the legal problems faced.[2] The nature of the research used is analytical descriptive, and data collection that uses in this thesis research are study of literature and documents in the library related to which will be discussed in this thesis research.

3. DISCUSSION

3.1. Legal Responsibilities of PT BFI as a Business Actor for Misuse of Consumer Personal Data and Not Having a Business Permit from OJK

According to the law, responsibility is the result of a person's consequences for an action related to ethics or morals when doing an action.[3] Hans Kelsen in his theory of responsibility says that: "a person is responsible for a sanction in terms of an act he has done which is against the law."[4] Limited Liability Company (PT) is a form of legal entity in Indonesia. The form of PT as a legal entity is clearly "can be seen in the provisions of Article 1 point 1 of Law no. 40 of 2007 concerning Limited Liability Companies: "A limited liability company is a legal entity which is a capital partnership, established based on an agreement, conducting its business activities with authorized capital which is entirely divided into shares and complies with the requirements of the Limited Liability Company Act and its implementing regulations."[5]. As a legal subject, the one who representing PT both inside and outside the court is called Board of Directors. Legal relationship between service providers of lending-borrowing money technology-based and debtors is basically an ordinary debt agreement, but because transactions are carried out using electronic and digital media, everything including the agreements and requirements needed in terms of applying for credit/loans online is done electronically and digitally.
The data needed to apply for credit (loan) is personal or private data and must be used with the consent of the owner of the personal data. Operators/business actors who provide online loans in carrying out their business activities are always supervised by the financial services authority (OJK). Based on OJK regulation Number 77 of 2016 there are consequences that "will arise if the service provider /business actor of financial technology-based loan funds" misuses the personal data of the debtor/consumer that is not in accordance with its designation and also the service provider/business behavior in the form of a company does not have a license registered from OJK in terms of carrying out its business activities.
In accordance with the provisions stipulated in Article 7 POJK No. 77 of 2016: "Operators are required to apply for registration and licensing to OJK."[6] Article 26 letter a POJK No. 77 of 2016, has regulated the obligations of the operator to: Maintain the confidentiality, integrity and availability of personal data, transaction data, and financial data that it manages from the time the data is obtained until the data is destroyed."[7] If in the provisions of article 7 in conjunction with article 8 in conjunction with article 26 letter a, it is not carried out by the service provider/business actor, then there are provisions for sanctions as regulated in article 47 paragraph 1, POJK No. 77 of 2016, the OJK may impose administrative sanctions in the form of: Written warnings, fines, restrictions on business activities as well as

revocation of licenses and closure of business activities, against service providers/business actors of technology-based financial loan funds that commit violations. In addition to the administrative law regulated in POJK No. 77 of 2016, there are other legal sanctions that regulated in "Article 26 paragraphs 1 and 2 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions, stated that:" Everyone who feels that their rights have been violated can file a (civil) lawsuit for losses arising from the use of any information through electronic media concerning personal data, which must be done with the consent of the person concerned."[8] Not only administrative and civil provisions as for other legal consequences of misuse of personal data, there is the threat of criminal law if a technology-based financial loan service provider takes actions that are prohibited by the "ITE Law" such as service providers / business actors of Financial Technology-based loan funds to access the debtor's electronic system and retrieve the phone number on the debtor's smartphone device that previously downloaded the application for transaction purposes". So if this is done then there are provisions for criminal law threats which are regulated in Article 30 of the ITE Law as follows:[9]

"Every person intentionally and without rights or against the law accesses Computers and/or Electronic Systems belonging to other Persons in any way".

Article 30 sanctions provisions are regulated in article 46 which reads**:**[10]

"Every person who fulfills the elements as referred to in Article 30 paragraph (1) shall be sentenced to a maximum imprisonment of 6 (six) years and/or a maximum fine of Rp. 600.000.000,- (six hundred million rupiah)".

"In accordance with the fact that there is a form of misuse of Personal Data carried out by service providers / business actors based on Financial Technology-based loan funds (PT Barracuda Fintech Indonesia), so that for the actions carried out by PT Barracuda Fintech Indonesia, which is represented by its directors both inside and outside outside the court, criminal sanctions can be imposed in accordance with the provisions of Article 30 paragraph (1) of the ITE Law which reads: "Everyone intentionally and without rights or against the law accesses the Computer and/or Electronic System belonging to another person in any way".[11] With a criminal threat as regulated in Article 46 paragraph (1) with a maximum imprisonment of 6 (six) years and/or a maximum fine of Rp. 600,000,000, - (six hundred million rupiah).[12]

3.2. Law No. 19 of 2016 and Its Related Regulations Protecting Consumer Personal Data of Fintech Users from Misuse of Personal Data

Humans as social beings always interact with one another, because consciously or unconsciously humans always do various actions law (rechtshandeling) and legal relations (rechtsbetrekkingen). In general, legal relations can be interpreted as a relationship between two or more legal subjects. Legal relations that occur include relationships between individuals, between individuals and society, or between one community and another. In this kind of legal relationship, the rights and obligations of one party conflict with the rights and obligations of the other party. The legal relationship provides rights and obligations determined by the legislation, once violated, the perpetrator will be tried by the court. [13]

According to the provisions of Article 1 paragraph 3 of the 1945 Constitution, "Indonesia is a state of law". The existence of legal protection is strongly influenced by the principle of the rule of law according to the provisions of the 1945 Constitution of the Republic of Indonesia. "The principle of the rule of law is closely related to the principle of recognition and protection of human rights which is considered a priority for a rule of law principle. ."[14]

Philipus M. Hadjon stated that legal protection is the protection of dignity and respect for human rights possessed by legal subjects in a legal state based on the legal provisions in force in that country in order to prevent arbitrary occurrences. "Legal protection is generally in the form of a written rule, so that it is more clearly binding and can result in sanctions that must be imposed. The development of technology has had a major impact on the lives of Indonesian people. Legal protection is generally in the form of a written rule, so that it is more clearly binding and can result in sanctions that must be imposed.

The development of science and technology has had a major impact on the lives of Indonesian people. Technology allows one person to directly connect with others and can easily access the internet. Technology could bring a positive impact on people's socio-economic life and there are many applications that make it easier for us to obtain loans, such as peer-to-peer financial technology loans. But in practice, technology also allows other people to easily access personal data, especially in the form of digital personal data. "Indonesia concerns about the regulation that could bring protection to privacy and protection to personal data due to the absence of statutory instruments that clearly regulate privacy protection, data protection, and personal data protection because there is a legal vacuum or law regarding privacy and personal data", this issue of privacy protection and personal data protection can be considered to be "a fundamental agenda for legislators in Indonesia. Privacy policies are considered very important not only for economic reasons, but privacy must also be introduced and socialized as part of human rights. Privacy is one part of human rights and the protection of personal data is one of the instruments or efforts to respect this right. Privacy policy is considered very important not only for economic reasons, but privacy must also be introduced and socialized as part of human rights. Privacy is a part of Human Rights and the protection of personal data is one of the instruments or efforts in respecting this right. Privacy policy is considered very important not only for economic reasons, but privacy must also be introduced and socialized as part of human rights. Privacy is a part of human rights and the protection of personal data is one of the instruments or efforts to respect this right.

"Indonesian legal scholars mostly refer to Article 28 G of the 1945 Constitution of the Republic of Indonesia as a guideline for making more specific regulations regarding the protection of privacy data related to several fields. Article 28 G" reads as follows: "Everyone has the right to be protected for himself, his family, honor, dignity, and property under his control, and has the right to a sense of security and protection from the threat of fear to do or not do something that is rights."[15] So indirectly the protection of personal data has been mandated in words that read "personal protection". Indonesia has actually enacted several laws and regulations governing personal data. The following are some of the rules that protect a person's personal data:

3.2.1. Law No. 19 of 2016 concerning amendments to Law 11 of 2008 concerning Electronic Information And Transactions

Article 26 paragraphs 1 and 2 already regulates personal data:[16] which reads Paragraph (1): "Unless otherwise stipulated by laws and regulations, the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned." Paragraph (2): "Everyone whose rights are violated as referred to in paragraph (1) may file a lawsuit for the losses incurred under this Law

The provisions stipulated in article 26 ITE, has given the right to the owner of personal data to maintain the confidentiality of his personal data, if his personal data has been spread and misused by other parties, the owner of personal data can file a lawsuit to the district court. The lawsuit in question is in the form of a civil lawsuit filed based on statutory regulations. The provisions of this article are generally the protection of a person's personal data, which means that every activity using a person's personal data is obliged to protect that data, through this arrangement everyone has the right to the protection of the confidentiality of their personal data, so that the data they have remains private. "Any personal data that has been provided must be used in accordance with the consent of the person who owns it and it must be kept confidential."

The provisions of criminal sanctions regulated in the ITE Law in article 31 paragraph 1 stated that: " Everyone intentionally and without rights or against the law intercepts or intercepts electronic information and/or electronic documents in a certain computer and/or electronic system belonging to another person." paragraph (2): "Every person intentionally and without rights or against the law intercepts the transmission of Electronic Information and/or Electronic Documents that are not public from, to, and within a certain Computer and/or Electronic System belonging to another Person, whether it does not cause any changes or causes changes, disappearances, and/or termination of Electronic Information and/or Electronic Documents that are being transmitted" paragraph (3) stated that: "Except for interception as referred to in paragraph (1) and paragraph (2), interception is carried out in the context of law enforcement based on request by the police, prosecutors, and/or other law enforcement institutions stipulated by law."

Article 47: "Every person who fulfills the elements as referred to in Article 31 paragraph (1) or paragraph (2) shall be sentenced to a maximum imprisonment of 10 (ten) years and/or a maximum fine of Rp. 800.000.000,- (eight hundred million rupiah)."

Article 32 paragraph 1: "(i) Any person intentionally and without rights or against the law in any way alters, adds, reduces, transmits, damages, removes, transfers, hides an Electronic Information and/or Electronic Document belonging to another Person or public property." Paragraph 2: "Every person intentionally and without rights or against the law in any way transfers or transfers Electronic Information and/or Electronic Documents to the Electronic System of another person who is not entitled to." Article 48 paragraph 1: "Everyone who fulfills the elements as referred to in Article 32 paragraph (1) shall be sentenced to a maximum imprisonment of 8 (eight) years and/or a maximum fine of Rp. 2,000,000,000.00 (two billion rupiah). " Paragraph 2: "Everyone who fulfills the elements as referred to in Article 32 paragraph (2) shall be sentenced to a maximum imprisonment of 9 (nine) years and/or a maximum fine of Rp. 3.000.000.000,- (three billion rupiah)" Government Regulation No. 71 of 2019 concerning Electronic Transaction System Operators:

In the provisions of article 1 number 29 personal data is defined as follows: Personal Data is any data about a person either identified and/or can be identified separately or in combination with other information either directly or indirectly through Electronic and/or non-electronic Systems .[17]

It is also regulated in Article 1 number 30 regarding electronic data is "data in electronic form which is not limited to writing, sound, images, maps, designs, photographs, electronic ideals interchange (EDI), electronic mail (electronic mail, telegraf, telex, telepon). or the like, letters, signs, numbers, Access codes, symbols, or perforations".[18]

The provisions of this article not only provide a definition related to a person's personal data, but also constitute an authority to protect the confidentiality of personal data as a respect for a person's right to privacy.

Article 14 paragraph 1 states that: "Electronic System Operators are required to implement the principle of protecting Personal Data in processing Personal Data".[19] In addition, in article 15 paragraph 1 it is stated that: "every Electronic System Operator is obligated to delete irrelevant Electronic Information and/or Electronic Documents under its control at the request of the person concerned". Article 15 paragraph 2 states that the obligation to delete irrelevant Electronic Information and/or Electronic Documents as intended consists of deletion (right to erasure), and removal from the list of search engines (right to delisting).[20]

While the provisions of Article 59 paragraph 3 regulates "electronic signatures". This is because the electronic signature is a symbol of approval in an electronic transaction.[21] Government Regulation Number 71 of 2019 mostly regulates the ways and parties who receive the

mandate and obligation to maintain and minister the data for the privacy or personal data of the public.

3.2.2. POJK No.77/POJK.01/2016 concerning Information Technology-Based Lending and Borrowing Services

The protection of consumer data relating to personal data is regulated in Article 26 requiring the operator to maintain the confidentiality of the personal data of service users.[22] Then Article 29 states that: organizers (the one who runs services) are required to apply the basic principles of user protection, such as: transparency, fair handling, reliability, confidentiality and data security as well as user dispute resolution in a simple, fast and affordable cost .[23] In addition, based on the provisions of laws and regulations, the obligations given to the organizer are prohibited from providing data and/or information regarding users to third parties in any way unless the user gives electronic consent and/or because it is required by the provisions of the legislation. If the organizer violates the obligations and prohibitions in this POJK, it will be subject to administrative sanctions as stipulated in article 47. The sanctions are in the form of written warnings, obligation to pay fines in the terms of money, restrictions on business activities and revocation of licenses".

3.2.3. POJK No.1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector

Article 2 regulates that "consumer protection principles that must be provided to consumers, (including Fintech consumers as users of financial services)." These principles are "transparency, fair handling, reliability, confidentiality and security of consumer data/information, complaint handling and consumer dispute resolution in a simple, fast and affordable cost." Furthermore, Article 31 regulates prohibitions related to consumer data for Financial Services Businesses (hereinafter referred to as PUJK). The prohibition "is not to provide data and/or information about its consumers to third parties in any way except with written permission from the consumer and or because it is required by laws and regulations." Apart from prohibition, Article 49 also requires Financial Services Businesses to have and implement written policies and procedures for consumer protection. These policies must be stated in standard operating procedures which are then used as guidelines in all operational activities of the PUJK. Violation of this POJK will be subject to administrative sanctions as referred to in Article 53. The administrative sanctions are in the form of: written warnings, fines by paying a certain amount of money, restrictions on business activities, freezing of business activities and revocation of business licenses. In addition to this POJK, specific regulations regarding Fintech by OJK can be found in the Financial Services Authority Circular Letter No.14/SEOJK.07/2014 concerning Confidentiality and Security of Data and/or Consumer Personal Information and Financial Services Authority Circular Letter Number 18/SEOJK.

3.2.4. Minister of Communication and Information Regulation No. 20 of 2016 concerning Personal Data Protection in Electronic Systems

It is regulated in the provisions of Article 2 of the Regulation of the Minister of Communication and Information No. 20 of 2016 which states that paragraph (1): includes protection against the acquisition, collection, processing, analysis, storage, appearance, announcement, transmission, dissemination, and destruction of Personal Data. in Paragraph (2) it is explained that: In implementing the provisions as referred to in paragraph (1), it must be based on the principles of good Personal Data protection, which include: "respect for Personal Data as privacy; Personal Data is confidential in accordance with the Approval and/or based on the provisions of laws and regulations; based on the Agreement; relevance to the purpose of acquisition, collection, processing, analysis, storage, display, announcement, delivery, and dissemination; the feasibility of the Electronic System used; good faith to immediately notify the Personal Data Owner in writing of any failure to protect Personal Data; availability of internal rules for the management of Personal Data protection; responsibility for Personal Data that is in the control of the User; ease of access and correction of Personal Data by the Personal Data Owner; and the integrity, accuracy, and validity and up-to-date of Personal Data." Paragraph (3): Privacy as referred to in paragraph (2) letter a is the freedom of the Personal Data Owner to declare confidentiality or not to disclose the confidentiality of his Personal Data, unless otherwise specified in accordance with the provisions of the legislation. Paragraph (4): The approval as referred to in paragraph (2) letter b is given after the Personal Data Owner confirm the truth, the status of confidentiality and the purpose of managing Personal Data. Paragraph (5): The validity as referred to in paragraph (2) letter j is the legality in the acquisition, collection, processing, analysis, storage, appearance, announcement, transmission, dissemination, and destruction of Personal Data."

It is regulated in the provisions of Article 26 of the Regulation of the Minister of Communication and Information No. 20 of 2016 which states that: "every owner of personal data has the right to:

a. Confidentiality of personal data; File a complaint in the context of resolving personal data disputes over the failure to protect the confidentiality of personal data by the electronic system operator to the minister;
b. Gain access or opportunity to change or update their personal data without disturbing the personal data management system, unless otherwise stipulated by the provisions of laws and regulations;
c. Gain access or opportunity to obtain historical personal data that has been submitted to the electronic system

operator as long as it is still in accordance with the provisions of the legislation; and

d. Request the destruction of certain personal data belonging to him in the electronic system managed by the electronic system operator, unless otherwise stipulated by the provisions of the laws and regulations."

   Therefore, in accordance with the provisions stipulated in article 26, it is obligatory for users of the electronic system to maintain the confidentiality of personal data that they obtain from consumers and protect personal data and documents containing such personal data from acts of abuse; and is responsible for the personal data contained in its control, both organizational control under its authority and individuals, in the event of an act of abuse.[24]

e. Provisions for sanctions that can be given if any party that obtains, collects, processes, analyzes, stores, displays, announces, sends and/or disseminates personal data without rights or contrary to this regulation and other laws and regulations will be subject to administrative sanctions in the form of warnings, verbal warnings, written warnings, suspension of activities and/or announcements on online websites (websites).[25]

3.2.5. POJK No.13/POJK.02/2018 Regarding Digital Financial Innovation In The Financial Services Sector

According to this POJK, Fintech business operators are required to maintain the confidentiality, integrity, and availability of personal data, transaction data and financial data that they manage from the time the data is obtained until the data is destroyed. [26]

Terms of use of user data and information include: [27]

1) Obtain the consent of the user;
2) Communicate the limits on the use of data and information to users.
3) Notify users of any changes in the purpose of data and information utilization in the event that there is a change in the purpose of data and information utilization; and
4) The media and methods used in obtaining data and information are guaranteed confidentiality, security and needs.

In the provisions of Article 31, providers are required to apply the basic principles of consumer protection, such as: transparency, fair handling, reliability, confidentiality and security of consumer data/information, handling complaints and resolving consumer disputes in a simple, fast and affordable cost. In addition, the operator is also required to provide a technology-based consumer service center which at least consists of the provision of a consumer service center that can be carried out alone or through other parties. In addition to the obligations stated in Article 31, the operator has other obligations, that is providing and/or delivering the latest information to OJK and consumers regarding digital financial service activities. The information is contained in documents or other means that can be used as evidence. Article 39 regulates that any parties who violates or causes a violation of this POJK will be subject to administrative sanctions in the form of a written warning, the obligation to pay fines in the terms of money, cancellation of approval and/or cancellation of registration. The sanctions imposed by the OJK do not reduce the criminal provisions in the financial services sector. In addition to administrative sanctions, Article 40 stipulates that OJK can take certain actions against violations of this POJK.

4. CONCLUSION

Based on the overall analysis of the main problems that have been described in Chapter I, the authors can draw the conclusion that:

1. From the description of the discussion of the formulation of the first problem above, another legal relationship appear, that is between the organizer of the electronic system and the owner of personal data as we called debtor. Therefore, the legal consequences that will appear if a financial technology-based fund loan service provider abuses the debtor's personal data and those businesses does not have a permit/registered by OJK are the first is an administrative sanction against a financial technology-based fund loan service provider who violates obligations and prohibitions. The regulations contained in these regulations are in accordance with the provisions of Article 47 of the Financial Services Authority Regulation Number 77 /POJK.01/2016 concerning Information Technology-Based Lending and Borrowing Services in the form of written warnings, fines, restrictions on business activities, up to license revocation. In addition to administrative sanctions, there are also consequences of civil law that can be accepted by providers of financial technology-based loan services if they misuse or use debtor's personal data without their consent, that is as set out in Article 26 paragraphs (1) and (2) of Law Number 19 Year 2016 concerning amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions, stated that anyone who feels that his rights have been violated can file a (civil) lawsuit for the losses that come up as a result of it. There are also legal consequences of criminal threats if the financial technology-based loan service provider in its application does things that are prohibited by the ITE Law.
2. Then related to the formulation of the second problem, that is how to protect personal data of users of financial technology-based loan applications, the author through the discussion explained that basically Indonesia has several regulations regarding personal data or privacy data in Indonesia. In personal data related to financial technology-based loan funds, there are provisions that protect users' personal data of financial technology-

based loan applications, such as: Law Number 19 of 2016 concerning Information and Electronic Transactions, Law of Government Regulation Number 71 of 2019 concerning Implementation Electronic Transaction System, Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems, and Financial Services Authority Regulation Number 77 /POJK.01/2016 concerning Information Technology-Based Borrowing-Lending Services, Financial Services Authority Regulation No. 1/POJK.07.2013 concerning Consumer Protection in the Financial Services Sector. Which is basically has acknowledged the existence of personal data and gives rights to the owner of the personal data who feels aggrieved if his personal data is misused. However, there is no provision regarding the obligations of related parties such as electronic system operators who are required to make an approval mechanism in applications using safer forms of consent such as the absence of application permissions to access data on smartphone devices automatically when the application is downloaded,

REFERENCES

[1] Decision No. 438/Pid.Sus/2020/PN JKT. Utr.

[2] Mukti Fajar ND and Yulianto Achmad, Dualism of Normative and Empirical Legal Research, Yogyakarta: Learning Library, 2010, p, 34

[3] Soekidjo Notoatmojo, Ethics and Health Law, Rineka Cipta, Jakarta, 2010, p, 21

[4] Hans Kelsen (a), as translated by Somardi, General Theory Of law and State, General Theory of Law and State, Fundamentals of Normative Law as Empirical Descriptive Law, BEE Media Indonesia, Jakarta, 2007 p. 81

[5] Article 1 point 1 of Law no. 40 of 2007 concerning limited liability companies

[6] Article 7 POJK No. 77 of 2016 concerning information technology-based lending and borrowing services

[7] Article 26 letter a POJK No. 77 of 2016 concerning information technology-based lending and borrowing services

[8] Article 26 paragraphs 1 and 2 of Law no. 19 of 2016 on Electronic Information And Transactions

[9] Article 30 of Law 19 of 2016 concerning amendments to Law number 11 of 2008 concerning information and electronic transactions.

[10] Article 46 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions.

[11] Article 30 paragraph (1) of Law Number 19 of 2016 concerning amendments to Law number 11 of 2008 concerning Information and Electronic Transactions

[12] Article 46 paragraph (1) of Law number 19 of 2016 concerning amendments to Law number 11 of 2008 concerning Information and Electronic Transactions.

[13] Soedjono Drijosisworo, Introduction to Law. PT. King Grafindo Persada. Jakarta. 2001. p.21.

[14] Philipus M. Hadjon, Legal Protection for the people of Indonesia, PT. Science Building. Surabaya, 1987, p.7

[15] Article 28 G of the 1945 Constitution.

[16] Article 26 paragraphs 1 and 2 of the ITE Law.

[17] Article 1 point 29 Government Regulation Number. 71 of 2019 concerning Electronic Transaction System Operators

[18] Article 1 number 30 Government Regulation Number. 71 of 2019 concerning Electronic Transaction System Operators

[19] Article 14 Government Regulation No. 71 of 2019 concerning Electronic Transaction System Operators.

[20] Article 15 Government Regulation No. 71 of 2019 concerning Electronic Transaction System Operators.

[21] Article 59 paragraph 3 Government Regulation No. 71 of 2019 concerning Electronic Transaction System Operators

[22] Article 26 POJK No. 77 of 2016 concerning Information Technology-Based Lending and Borrowing Services

[23] Article 29 POJK No. 77 of 2016 concerning Information Technology-Based Lending and Borrowing Services

[24] Compare Article 27 of Regulation of the minister of communication and informatics No. 20 of 2016. the protection of personal data in electronic systems

[25] Article 36 Regulation of the minister of communication and informatics No. 20 of 2016. Concerning the protection of personal data in electronic systems

[26] Article 30 paragraph (1) POJK No. 13/POJK.02/ 2018. Concerning Digital financial innovation in the financial services sector

[27] Article 30 paragraph (2) POJK No.13/ POJK .02/2018 Concerning Digital financial innovation in the financial services sector