

---

## Legal Protection of Consumer Personal Data in the Case of Fintech Peer to Peer Lending

Muhammad Abdillah Novaliando  
Universitas Muhammadiyah Purwokerto

---

### ARTICLE INFO

#### Article history:

DOI:

[10.30595/pssh.v14i.1020](https://doi.org/10.30595/pssh.v14i.1020)

Submitted:

June 08, 2023

Accepted:

September 29, 2023

Published:

November 16, 2023

---

#### Keywords:

Legal Protection, Personal Data,  
Fintech Peer to Peer Lending

---

### ABSTRACT

*Fintech is a financial product and service through the incorporation of technology platforms and business models that are innovative, effective and efficient. However, some time ago there was a case of misuse of personal data of fintech users. The offense committed is to disseminate consumer personal data without the consent or knowledge of consumers. The purpose of this study is to determine the legal protection of consumer personal data and legal remedies that can be taken by financial technology consumers if personal data is misused by the organizer. The research method used is normative juridical approach. The results of this study state that, Regulations regarding the protection of personal data to online loan users can refer to POJK No. 1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector. The regulation contains preventive and repressive protection. Victims of personal data misuse can make legal efforts by way of deliberation and complaints to the Ministry of Communication and Information or OJK (non-litigation) and if it does not resolve consumer disputes can file a civil lawsuit (litigation) on the basis of Unlawful Acts I PMH and request compensation.*

*This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).*



---

#### Corresponding Author:

**Muhammad Abdillah Novaliando**

Faculty of Law, Universitas Muhammadiyah Purwokerto

Jl. KH. Ahmad Dahlan, Kembaran, Banyumas, Jawa Tengah 53182, Indonesia

---

## I. INTRODUCTION

Advances in information and communication technology today have changed the world without boundaries, distance, space and time, which has an impact on increasing productivity and efficiency of life. The impact of global developments based on information and communication technology has changed the way people live with a new way of life, causing changes in all aspects of life. According to a survey by the Indonesian Internet Service Providers Association (APJII), internet users in 2018 were 176,716.8 people or 64.8%, an increase of around 27,916,716 people from the number in 2017. The rapid development of digital technology such as the internet and electronic products has brought various conveniences to the community. One of them is a technology-based loan service that provides convenience and shortcuts for those who need material but can provide a fast and easy process, so many people want to use the technology-based loan application (fintech).<sup>1</sup>

The development of globalization is increasingly bringing big changes in all activities carried out by humans, especially in the field of technology. The development of technology from year to year has a positive impact, especially in economic matters such as financial technology or commonly referred to as fintech. The development of fintech is currently supported by the internet, and with the development of the internet, of course,

---

<sup>1</sup> Arfian Setiantoro; Fayreizha Destika Putri; Anisah Novitarani; dan Rinitami Njatrijan. 2018. "Urgensi Perlindungan Hukum Konsumen dan Penyelesaian Sengketa E-Commerce Di Era Masyarakat Ekonomi Asean". *Jurnal RechtsVinding*. 7(1).

it has given birth to many startups in the financial sector, information technology-based online loans or "fintech peer-to-peer lending" or commonly known as P2P loans. This is very similar to a digital intermediary that connects one party to another (fund borrowers and fund lenders). This concept provides an opportunity for everyone to become an investor, lend money or provide opportunities to anyone in need without the need for intermediaries or through the services of financial institutions. Based on this interpretation, Fintech P2P Lending is expected to provide solutions to the community in terms of borrowing and lending money in a more modern way to obtain funds in the form of business loans.<sup>2</sup>

Fintech is financial products and services through the incorporation of technology platforms and innovative business models while the origins of fintech itself came from Silicon Valley one of the southern parts of the San Francisco Bay Area in California, then expanded to New York, Singapore, Hong Kong, and several global countries.<sup>3</sup> P2P lending services are a solution to answer the problem of banking financial services that are not touched by some people due to geographical factors. P2P Lending works like a bank but works through the internet and advanced technology where lending or debt is usually done with an agreement that the party who has funds will lend it to the party who lacks funds based on the principle of "freedom of contract" regulated in the Civil Code. Based on these developments, it can be said that business activities in the field of Fintech are very efficient, because they do not require a lot of human resources in running their business. Fintech looks more efficient because it can reduce operational costs so that it can distribute financing with a faster process.<sup>4</sup>

Fintech is growing very fast, this is because fintech has a positive impact on society so that it can run the economy more effectively and more efficiently. The requirements to be able to get a loan from this service are only enough with an Identity Card (KTP) and bank account number so that many people want to join. Behind the positive impact that fintech brings, there is a high risk for people who use fintech services, namely the risk of consumer data security and the risk of errors in transactions. These risks are clearly very detrimental and endanger each party involved in fintech. This risk also makes people hesitant to use fintech-based services, people are afraid that unexpected things will happen such as wiretapping, break-ins and other online crime.

In addition to online crimes, real-world crimes that disturb comfort and even endanger lives also make people afraid to participate in fintech services. Regarding some of the problems that have entered the Jakarta Legal Aid Institute (LBH) are the high interest costs that customers have to pay, unreasonable collection processes such as slander, threats, threats, including disseminating personal data to other parties, which of course this is detrimental to consumers as online loan customers and disturbs the comfort of others.<sup>5</sup>

Rupiah Plus is one example of a problematic P2P Lending fintech case. Rupiah Plus collects consumers in an unreasonable way such as accessing telephone contacts from consumers without any notification to consumers and contacting everyone in consumer contacts by telling all consumer personal data and the amount of debt to be paid. Prior to the case, OJK had issued regulations relating to fintech P2P Lending, namely "Regulation of the Financial Services Authority Number 77 of 2016 concerning "Information Technology-Based Money Lending and Borrowing Services" (POJK P2P Lending Services). This regulation requires every person as a business actor in the information technology-based lending business to officially register his business.

The previous research that discussed fintech, namely by Veronica Novinna (2020) entitled consumer protection from the dissemination of personal data by third parties, discussed the relationship or status of third parties with online loan providers as debt collectors for default and by Diva Yohana Margaretha Marbun (2021) entitled legal protection of consumers for misuse of personal data in illegal peer to peer lending financial technology applications in Indonesia, discussed legal protection regulations related to misuse of personal data by consumers in illegal peer-to-peer lending fintech applications in Indonesia. Both studies do not discuss legal remedies taken by consumers if their personal data is misused, while this study discusses the legal protection of consumer personal data in the case of Fintech Peer To Peer Lending and legal remedies taken by consumers if their personal data is misused. Therefore, the author has an idea with the title LEGAL PROTECTION OF CONSUMER PERSONAL DATA IN FINTECH PEER TO PEER LENDING CASES.

---

<sup>2</sup> Abdul Halim Barkatullah, 2009, "Perlindungan Hukum bagi Konsumen dalam Transaksi E-Commerce Lintas Negara di Indonesia". Pascasarjana FH UII Press, Yogyakarta.

<sup>3</sup> Anita, Siti Zulaikha, Khofidlotur Rofiah, & Risa Sari Pertiwi. (2019). Legal Protection of Lenders in the Implementation of Financial Technology Based on Peer to Peer Lending. *KnE Social Sciences*, pages 1305–1316. DOI 10.18502/kss.v3i13.4286, page.1307.

<sup>4</sup> Ridwan Muchlis. (2018). Analisis SWOT Financial Technology (*Fintech*) Pembiayaan Perbankan Syariah Di Indonesia (Studi Kasus 4 Bank Syariah Di Kota Medan). *Jurnal AtTawassuth: Ekonomi Syariah Universitas Islam Negeri Sumatera Utara*.v.3.no.3.2018.h.335-357

<sup>5</sup> Yudho Winarto, (2018), LBH Jakarta Terima 500 Pengaduan Terkait Fintech Bermasalah, available from: <https://keuangan.kontan.co.id/news/lbh-jakarta-terima-500-pengaduanterkait-fintech-bermasalah?page=all>.

## II. RESEARCH PROBLEMS

Based on the background explanation above, the problem formulation that I will give here is as follows:

1. How is the Legal Protection of Consumer Personal Data in the Case of Fintech Peer To Peer Lending?
2. How Legal Efforts Can Be Made By Financial Technology Consumers If Personal Data Is Misused By The Organizer?

## III. RESEARCH METHODS

The type of research used is normative legal research. Normative legal research is the process of determining legal rules, legal principles and legal doctrines to obtain answers to the legal problems at hand. Meanwhile, this type of research is descriptive, meaning that it tries to provide a detailed explanation of the topics discussed and an explanation of the relevant issues. The approach that will be used is the statutory approach, namely the approach taken by examining all laws and regulations relating to legal issues. The data sources needed in this research are sourced from the field and literature in the form of primary, secondary and tertiary data, the data collection techniques used in this research are literature studies.

## IV. RESULT AND DISCUSSION

### 1. Legal Protection of Consumer Personal Data in the Case of Fintech Peer To Peer Lending

In recent years, technological development has grown so rapidly. The development of technology has affected all sectors, one of which is the economic sector. This can be felt because it is influenced by the internet which is increasingly affordable by the community. The influence of the internet allows for exchange of personal data and/or information when transacting between communities. Data and / or personal information is part of consumer privacy that needs to be protected because the personal data can be misused by irresponsible people to commit crimes against the data owner. This shows that the importance of providing legal protection for consumer privacy and personal data.

The provision of legal protection is related to the function of law as instrument of protection for legal subjects, leading to the aim of establishing legal relations between legal subjects that are equal and fair. This goal will be realized if rights of legal subjects are fulfilled and carry out their obligations based on the applicable law.<sup>6</sup> If one of the parties feels that their rights are not fulfilled, then that is when the function of the law in providing legal protection to the community needs to be fulfilled. that is when the function of law in providing legal protection to the community needs to be carried out. In addition, consumer protection efforts aim to increase the trust of investors and consumers in transactions in the financial services sector (Market Confidence); and provide space for organizers to develop themselves fairly, efficiently, transparently. In addition, consumers understand their rights and obligations regarding characteristics, services, and products (Level Playing Field) in transactions with the Organizer. Organizers. In the long run, the financial sector will benefit as well in the long run, the financial sector will also benefit, namely being able to accelerate the increase in efficiency as a result of the reaction to the insistence on maximum service to consumers. more maximum service to consumers.<sup>7</sup>

Legal protection is all efforts to ensure legal certainty, in order to protect parties who take legal action. Legal protection must contain elements of legal certainty, protection from the government against citizens and their rights and punitive sanctions for those who violate them.<sup>8</sup> In a narrow sense, legal protection is regulations that are preventive and repressive in written and unwritten form. Legal protection is a manifestation of the function of law in creating security for all human interests in society. security for all human interests in society. While in a broad sense is protection addressed to all creatures of God and used together for the realization of a just atmosphere. for the realization of a just and peaceful atmosphere.<sup>9</sup>

A person's personal data needs to be protected because the data can be used by others in committing crimes. Therefore, data security and confidentiality are necessary. Data security is an effort to guarantee and maintain the three most important things in cyberspace, among others: First, data confidentiality, which guarantees the maintenance of the owner's privacy data while surfing the internet. Second, Data integrity, which guarantees internet users to get valid data without any changes, additions or subtractions by other parties. Third, Data availability, which guarantees users to get data when needed without being covered and without interference from

---

<sup>6</sup> Ridwan HR, *Hukum Administrasi Negara*, (Jakarta: Rajawali Press, 2016), 266

<sup>7</sup> Penjelasan atas Peraturan OJK No. 1/POJK. 07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan

<sup>8</sup> Hetty Panggabean, *Perlindungan Hukum Praktik klinik Kebidanan*, (Yogyakarta: Deepublish, 2018), 65

<sup>9</sup> Widya Justitia dan Zil Aidi, "Perlindungan Hukum Terhadap Bank sebagai kreditur baru dalam pengalihanpiutang atas kredit pemilikan rumah secara Top Up", *Jurnal Yuridis*, Vol.4, Nomor 2 (Desember, 2017), 119-120.

other parties.<sup>10</sup> In the case of misuse of personal data, this falls into the scope of data confidentiality, which is responsible for ensuring that the owner's privacy data is protected. There are several components discussed in data security, as follows: (1) Privacy, The more widespread the use of the internet among the public, several advantages and disadvantages arise. The proliferation of the internet that collects personal data from each user allows for personal data leakage. Personal data can be collected through the consent of the data owner (data subject) such as when registering (on-site registration), filling out forms in order to process transactions such as buying and selling, or it may be obtained without the knowledge and consent of the data subject, for example using cookies. The purpose of internet sites that collect personal data is to be processed into a database about their users to be used as a benchmark when offering new products. The database can even be considered as a company asset that can be traded to third parties and generate huge profits. So that personal data has the potential to become an object of violation of the right to privacy of personal data. Therefore, personal data also deserves to have privacy rights because this data is information that is attached to each individual as a means of identifying the owner of the data; (2) Integrity (Consistent), Data integrity is needed to guarantee the authenticity of the data sent by the user or user and the user is really the one who sent it. In addition, data integrity must also be able to guarantee that any data sent will not be changed when the data is sent until the data is opened. The method used to keep the data in its original state is the encryption model; (3) Authenticity, The most crucial thing in data confidentiality and security is data authenticity. This component is very important in data security and confidentiality because it can be used to prove the authenticity of documents that a person uses for transactions. There are three approaches in proving the authenticity of data. First, the user has data that only he knows such as passwords or other identities. Second, the use of tools used by the user, for example printers and others. The third is to check anything that represents the user such as DNA, fingerprints, or anything else. Authenticity has two uses. First, it checks the authenticity of a data message and guarantees that it is genuine. The second is to check the identity of a person when entering a system;<sup>11</sup> (4) Availability, A data contained in a computer system is available and can be used by people who have the right to access. Therefore, if the data is easily available, it will affect data security because it can be accessed by any user who is not entitled. This is very prone to data misuse. The availability of this data must be available when needed when a request is made so that user activities are not disrupted. For example, if a user will enter a certain system but the system cannot provide the data needed by the user, then the system cannot be accessed or the server is down.<sup>12</sup>

The increase in the number of internet users naturally affects the security of users' personal data. For the sake of data security, it is necessary to protect personal data.<sup>13</sup> The protection of personal data is included in the mandate of the 1945 Constitution Article 28G which explains that everyone has the right to personal protection and the right to security. In this article, the protection of personal data is within the scope of personal protection. Therefore, it is necessary to have supporting regulations that further strengthen the protection of privacy and security of personal data in order to realize justice and security. Until now, regulations that specifically regulate the legal protection of personal data are still at the stage of the Draft Law on Personal Data Protection and are also found in several other regulations.

First, the concept of personal data protection is explained in Law No. 39 of 1999 concerning Human Rights in Article 29 paragraph 1 that everyone has the right to self-protection and all their property rights. Based on this article, everyone has the right to privacy. There are three aspects of privacy, namely privacy about communication, data, and one's person.<sup>14</sup> Personal data protection is also contained in the Law on ITE Article 26 paragraphs 1 and 2 which reads: (1) the utilization of any personal information of a person through electronic media must use the permission of the person concerned; and (2) Personal data leaked by others without the consent of the owner can make a lawsuit for the losses caused. The article gives people the right to maintain their privacy by giving prior consent. If the personal data is misused, then the injured party can file a civil suit in court. The article is a form of legal protection provided to each individual user of electronic transactions by providing the right to protect the confidentiality of their personal data. If the data has been approved for use, it cannot be misused and must be kept confidential.

Then it is also explained in Article 40 of the Banking Law that banks are required to maintain the confidentiality of deposit customer data and deposits, except in cases that are permitted. The article indicates that banks are required to maintain all customer data, not only data related to their deposits but all customer data including identity and other personal data. It is further explained in Bank Indonesia Regulation No. 7/6/PBI/2005

---

<sup>10</sup> Indra Gunawan, *Keamanan Data: Teori dan Implementasi*, (Surabaya: CV. Garuda Mas Sejahtera, 2019), 7

<sup>11</sup> Andri Kristanto, *Keamanan Data Pada Jaringan Komputer*, (Yogyakarta: Gava media, 2003), 12-13

<sup>12</sup> Harun Muchtar, *Kriptografi untuk Keamanan Data*, (Yogyakarta: Deepublish, 2018), 8.

<sup>13</sup> Sinta Dewi, 2016, "Konsep Perlindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan dengan penggunaan Cloud Computing di Indonesia", *Yustisia*, Volume 5, Nomor 1, (Januari-April 2016), 25.

<sup>14</sup> Mukhtar, *Kriptografi untuk Keamanan Data*, 7-8.



concerning Bank Product Transparency and Use of Personal Data Article 9 that in the utilization of personal data of customers, the bank must obtain written consent from the party concerned. Then in Article 11 it is explained that if the bank obtains the customer's personal data from a third party, the bank must have the written consent of the third party obtained from the party concerned.

Article 42 paragraph 1 of the Telecommunication Law also explains that telecommunication service providers are required to maintain all personal information of telecommunication service users in the form of data sent or received by users, this is excluded if it is for the purposes of the criminal justice process at the request of the police or the attorney general. Likewise, in the OJK Law in article 33, it is explained that all persons working at OJK or acting on behalf of OJK are prohibited from utilizing or disseminating to other parties except for use in accordance with the functions and objectives in the OJK decision or legislation. Then it is also regulated in POJK No. 77/POJK.01/2016 concerning Information Technology-Based Money Lending and Borrowing Services which also regulates the protection of personal data of consumers who use online loan services. It is explained in Article 26 letter a that online lending parties are required to maintain the confidentiality, integrity and confidentiality of personal data, transaction data, and financial data that has been managed by the organizer since the data is obtained until the data is removed. In accordance with the mandate of this article, the organizer or online loan is required to maintain personal data, transaction data, and financial data for the safety and comfort of consumers when making transactions. It is further explained in Article 26 letter c of the POJK regarding Information Technology-Based Lending and Borrowing Services that online loan providers are required to ensure that the acquisition, use, utilization, and disclosure of personal data, transaction data, and financial data obtained by the organizer is based on the consent of the owner of the personal data, transaction data, and financial data, unless otherwise determined by the provisions of laws and regulations. The regulation explains that consumers as owners of personal data are given the right to protect their personal data. The organizer is given restrictions in using consumer personal data by not being allowed to utilize personal data, transaction data, and consumer financial data without obtaining permission from the party concerned first. This is done in order to provide legal certainty in protecting the personal data of online loan consumers.

Also regulated in POJK No. 1/POJK.07/2013 on Consumer Protection in the Financial Services Sector. Financial Services Sector. The regulation is an effort to provide protection to the public. In providing protection to consumers, OJK applies several principles as follows: (1) Transparency, namely informing consumers about products and / or services in a clear, complete and easy to understand manner; (2) Fair service tamper no discrimination; (3) Reliability, namely providing the right service according to regulations and reliable human resources; (4) Confidentiality and security of consumer data / information, namely efforts to protect, maintain the confidentiality of consumer data, and only be used for purposes and purposes that have been approved from consumers; (5) Serving complaints and resolving consumer disputes.

In some of the principles above, it is stated that the confidentiality and security of consumer data is a priority for OJK. This is contained in Article 2 of POJK No. 1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector. More clearly in Article 31 paragraphs 1 and 2, it is explained that regarding the confidentiality and / or security of consumer data, OJK prohibits organizers from disseminating consumer data and / or information to third parties unless they obtain written permission from consumers and / or are permitted by laws and regulations. In another case, if the organizer obtains personal data and/or information of a person and/or group from another party, it must have a written statement that the other party providing the data to the business actor has obtained written consent from the data owner regarding the granting of permission to disseminate the personal data to any party including the business actor as described in Article 31 paragraph 3. This article covers the prevention of misuse of individual personal data with the use of written permission in the use of personal data. Then based on Article 48 paragraph 1 that OJK also requires business actors to implement a supervisory system. In addition, based on Article 50, OJK is also required to have an internal control system in the context of consumer protection. Internal controls include compliance in implementing principles relating to consumer protection and the implementation of a reporting and monitoring system for following up on consumer complaints. In addition to the business actors themselves conducting supervision, Article 51 explains that the OJK is also required to directly or indirectly supervise the performance of business actors in implementing consumer protection. This article can be categorized as preventive protection. Preventive protection is protection that aims to prevent disputes.

In the POJK regarding Consumer Protection in the Financial Services Sector provides administrative sanctions, such as written warnings, fines, restrictions or freezes. administrative sanctions such as written warnings, fines, limitation or suspension of business activities, and revocation of business activity licenses. business activities, and revocation of business activity licenses. The provision of these sanctions is included in repressive protection. Repressive legal protection is protection in the form of sanctions carried out after a problem such as imprisonment, fines and other sanctions. Repressive protection aims to solve the problems that occur. However, of these sanctions, there are no sanctions intended for the misuse of personal data. Article 41 letter a explains that the sanctions are intended for violators who harm consumers who experience financial losses of Rp.

500,000,000 (five hundred million rupiah) for consumers in the fields of Banking, Capital Markets, Pension Funds, Life Insurance, Financing, Pawn Companies, or guarantees and losses of Rp. 750,000,000 (seven hundred and fifty million rupiah) for consumers in the field of General Insurance.

The losses mentioned above include material losses, namely losses that can be calculated. calculated losses. Meanwhile, in the case of misuse of personal data described above, consumers experience immaterial losses in the form of privacy violations that cause consumers' self-esteem and honor to be disturbed. Immaterial loss is difficult to estimate the value of the loss. Therefore, the sanctions listed in the OJK regulation on Consumer Protection in the Financial Services Sector cannot be applied to cases of misuse of personal data..

## **2. Legal Efforts that can be made by Financial Technology consumers if personal data is misused by the organizers of Financial Technology is misused by the organizer**

Legal remedies are legal steps taken by a person or legal entity to challenge a judge's decision or court decision because it does not fulfill a sense of justice or is considered detrimental. Consumers who feel harmed by financial technology providers who illegally distribute consumers' personal data can take various legal steps for the losses they suffer, both litigation and non-litigation legal steps.

### **a. Non-Litigation Legal Steps**

Consumers who feel harmed by the act of disseminating personal data by the Financial Technology Operator without the consent of the consumer. Financial Technology Provider without prior consent from the consumer can report the violation of the law to: 1) Ministry of Communication and Informatics of the Republic of Indonesia Users can file a complaint to the Ministry of Communication and Informatics of the Republic of Indonesia on the grounds that electronic information system organizer that fails to provide protection to the personal data of its users. protection of the personal data of its users. As far as legal action is concerned, it can be in the form of complaint, so there is no need to prove the element of loss that caused the leakage of personal data. leakage of personal data. With regard to penalties for violating the provisions of personal data protection, there is a provision in Article 36 of Regulation of the Minister of Communication and Information 20/2016, namely verbal and written warnings, for the temporary suspension of business activities and/or announcements through online sites (online sites).

### **2) Financial Services Authority (OJK).**

The sanction given can be in the form of business closure if the action is carried out by a legal Financial Technology Provider. Financial Technology Providers that are legal. The approach will be different if Fintech Providers that are illegal, OJK cannot enforce the law because often the legal domicile of such Fintech Providers are because often the legal domicile of such Fintech providers is domiciled abroad so that the perpetrators are not abroad so that the perpetrators are not subject to and bound by Indonesian law because they are outside the jurisdiction of Indonesia. outside Indonesian jurisdiction. If the perpetrator is an illegal Financial Technology Operator that is domiciled in Indonesia, the approach taken can use the formal law enforcement process or through litigation. formal law enforcement or through litigation, either with criminal proceedings or civil lawsuits.

### **b. Litigation Legal Steps**

Litigation legal steps through formal judicial institutions are the last legal effort and step (ultimum remedial). the last legal step (ultimum remedium) that can be taken in law enforcement after non-litigation efforts have reached a dead end. The use of legal remedies or legal steps in litigation can be carried out through the realm of criminal law and civil law. Legal measures in the realm of criminal law will end in legal sanctions in the form of corporal punishment (imprisonment) or substitute punishment (fine or confinement). Meanwhile, legal efforts or legal steps in the realm of civil law will end in legal sanctions in the form of fines or compensation. Legal resolution options through the realm of criminal law can use criminal offenses that exist in organic laws and in the Criminal Code (KUHP) such as offenses of illegal dissemination of electronic information, electronic data theft, threatening through electronic transactions, and may even use fraud offenses. The legal steps that can be taken by consumers who feel harmed by the illegal use of personal data by financial technology managers are as follows:

1) Police report at the local police agency. This can be done at the Sector Police level (Polsek) in a sub-district, City Police (Polresta) in a regency/city, Regional Police (Polda) in a province, or at Headquarters. regency/city, Regional Police (Polda) in a province, or at the National Police Headquarters (Mabes Polri) for the central or national level. Police (Mabes Polri) for the central or national level.

2) District Court (for the first level)

3) High Court (for appeals)

4) Supreme Court (for cassation and judicial review).

In addition to criminal law efforts or steps, consumers who feel harmed by the actions of the using personal data illegally is through a civil lawsuit. civil lawsuit. A civil lawsuit aims to recover the loss of the plaintiff (consumer) by imposing a fine or compensation on the defendant (fintech manager) if proven guilty. (financial technology manager) if proven guilty. In this case, the lawsuit filed is tort lawsuit (PMH). Civil legal steps that can be taken by consumers who feel aggrieved by the illegal use of personal data by the fintech manager, namely:

- 1) Filing a tort lawsuit at the local District Court (for the first instance)
- 2) High Court (for appeal) Supreme Court (for cassation and judicial review or other extraordinary legal remedies)

## V. CONCLUSION

Regulations regarding the protection of personal data to online loan users can refer to POJK No. 1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector. The regulation contains preventive protection, namely requiring business actors to use consumer personal data with the written consent of the party concerned and requiring internal controls on the performance of the financial sector business actors themselves. In addition, OJK is obliged to carry out direct or indirect supervision. Then repressive protection, namely in the regulation only contains administrative sanctions aimed at disputes that cause material losses. Legal remedies used if in the future a dispute occurs and consumers suffer losses, victims of personal data misuse can make Legal Remedies by way of deliberation and complaints to the Ministry of Communication and Information or OJK (non-litigation) and if it does not resolve the dispute consumers can file a civil lawsuit (litigation) on the basis of Unlawful Acts I PMH and request compensation.

## REFERENCES

- Abdul Halim Barkatullah, 2009, "Perlindungan Hukum bagi Konsumen dalam Transaksi E-Commerce Lintas Negara di Indonesia". Pascasarjana FH UII Press, Yogyakarta.
- Adrianus Meliala, 2014, "Praktik Bisnis Curang". Sinar Harapan. Jakarta. Hal 152. Dalam, Janus Sidabolok. Hukum Perlindungan Konsumen di Indonesia. 2014. Penerbit PT Citra Aditya Bakti Bandung: Bandung.
- Anita, Siti Zulaikha, Khofidlotur Rofiah, & Risa Sari Pertiwi. (2019). Legal Protection of Lenders in the Implementation of Financial Technology Based on Peer to Peer Lending. *KnE. Social Sciences* , pages 1305–1316.
- Arfian Setiantoro; Fayreizha Destika Putri; Anisah Novitarani; dan Rinitami Njatrijan. 2018. "Urgensi Perlindungan Hukum Konsumen dan Penyelesaian Sengketa E-Commerce Di Era Masyarakat Ekonomi Asean". *Jurnal RechtsVinding*. 7(1).
- Ernama Santika, 2017, "Pengawasan Otoritas Jasa Keuangan Terhadap Financial Technology (Peraturan Otoritas Jasa Keuangan Nomor 77/POJK.01/2016)", *Ponorogo Law Jurnal*, Vol 3, Nomor 3, Tahun 2017
- Ion MICU, Alexandra MICU, 2018, "Financial Technology (Fintech) and Its Implementation On The Romanian Non-Banking Capital Market", Vol. 2, Issue 2(11)/2016, 380. Dalam Alfihca Rezita Sari. Perlindungan Hukum Bagi Pemberi Pinjaman dalam Penyelenggaraan Financial Technology Berbasis Peer To Peer Lending di Indonesia.
- Irma Muzdalifa, Inayah Aulia Rahma, dan Bella Gita Novalia, 2018, "Peran Teknologi Finansial Dalam Meningkatkan Keuangan Inklusif Pada UMKM di Indonesia (Pendekatan Keuangan Syariah)", Vol.3, No 1 Tahun 2018.
- Ridwan Muchlis. (2018). Analisis SWOT Financial Technology (*Fintech*) Pembiayaan Perbankan Syariah Di Indonesia (Studi Kasus 4 Bank Syariah Di Kota Medan) . *Jurnal AtTawassuth: Ekonomi Syariah Universitas Islam Negeri Sumatera Utara*. v.3.no.3.2018.h.335-357
- U Yunus. (2018). A Comparison Peer to Peer Lending Platforms in Singapore and Indonesia. *Journal of Physics: Conference Series*. doi:10.1088/1742-6596/1235/1/012008. p.1.
- Warassih, E. 2018, "Peran Politik Hukum Dalam Pembangunan Nasional". *Gema Keadilan*, 2018. 5(1)
- Yudho Winarto, (2018), LBH Jakarta Terima 500 Pengaduan Terkait Fintech Bermasalah. <https://keuangan.kontan.co.id/news/lbh-jakarta-terima-500-pengaduanterkait-fintech-bermasalah?page=all>.