Legal Protection Of Personal Data Theft Victims In Online Loan Transactions After Covid-19 Pandemic

Heni Susanti[1], Yusramizza Md Isa[2], Syafrinaldi[3], Desi Apriani[4], Evi Yanti[5], Fadillah Afrian[6]

{ heni@law.uir.ac.id[1], yusramizza@uum.edu.my[2,] syafrinaldi@law.uir.ac.id[3]
desiapriani@law.uir.ac.id[4], eviyanti1996@law.uir.ac.id[5], fadillahafrian@student.uir.ac.id[6]}

Universitas Islam Riau. Indonesia[1,2,3,4,5,5]

Abstract. One cause of increasing personal data theft incidents in the IT sector is the lack of regulation and legal protection for personal data. The Covid-19 outbreak has had little effect on the number of online borrowers. According to the Financial Services Authority, fintech lending distribution in January 2023 reached IDR 18.73 trillion, with online loan distribution rising by 35.72% over the previous year. Online loans simplify credit applications without needing to visit a provider physically. While convenient, this can harm society by exposing borrowers' sensitive information. Therefore, investigating the legal protection available to victims of personal data theft post-Covid-19 is critical. The methodology is normative, examining statutory regulations, research findings, and expert opinions. Personal Data Subjects have the right to protection, including identity clarity, legal interests, purpose of data use, and accountability of the requesting party.

Keywords: Cybercrime, Cyber Law, Law Enforcement.

1 Introduction

Technological developments in the 4.0 era are very rapid and of course affect people's life patterns. The existence of information technology influences people's life patterns, these changes are influenced by several social, cultural, economic and political aspects of society. Developments in the economic aspect, which are now all experiencing digitalization, illustrate the influence of the significant economic developments that have occurred in recent years. These changes have occurred in the financial system, which is the most important part of the financial system in providing services in the financial sector . With the development of very advanced technology, the financial sector is also developing in a more efficient and modern direction. In the current world economy, it is very important to provide technological innovation in it. Technology and finance have a related relationship.

With a population of 262 million and 140 million internet users, the nation is the most populous in Southeast Asia. Approximately 28 million people, representing a 13% YoY rise, actively conduct business online. Given that Indonesia has about 49 million MSMEs (SME's), the government is committed to making Indonesia the largest digital economy in Southeast Asia, with the goal of employing over 26 million people by 2020.[1]

ICL-C 2023, November 11, Jakarta, Indonesia

DOI 10.4108/eai.11-11-2023.2351345

The application of financial system technology to create new goods, services, technologies, and/or business models is known as fintech, according to TIF Rahma. It can affect the stability of the financial system as well as the efficiency, smoothness, security, and dependability of the payment system. The buying and selling process is part of this financial transaction process. shares, payments, fund transfers, peer-to-peer lending, retail investment, and personal finance financial planning.[2]

According to the Financial Services Authority, this number is derived from 99 online lenders that are OJK-registered and have served over 3 million customers in Indonesia with over 9 million transactions. Compared to the IDR 2.56 trillion in loan distribution through the financial technology sector in 2017, this amount has increased by nearly eight times. The non-performing loan (NPL) ratio was 1.45% of the IDR 22 trillion in credit disbursed in 2018, which was higher than the 0.99% ratio in 2017.

The public's high level of trust in financial technology companies is demonstrated by the rise in the value of online loan funding over the past three years. The vast majority of online loan borrowers are employed individuals, farmers, fishermen, craftspeople, and Micro, Small, and Medium-Sized Businesses (MSMEs). In actuality, small business players who launch and fund their enterprises on their own are the foundation of today's civilization. However, they frequently run into issues with funding (capital) when it comes time to grow their firm. Due to their lack of awareness and extended bank access, many people even fall victim to loan sharks when they need to borrow money. After that, many workers in the company struggled to pay for their living expenses and were forced to look for bank loans. However, some of them find it challenging to obtain a bank loan for a variety of reasons, including the lengthy loan application process, the complexity of the requirements, and the difficulty of meeting them. Beginning with the numerous formalities involved in lending money to banks, online loans, also known as fintech landings, have emerged as a social boon. People can quickly obtain money loans without having to wait in line at the bank or prepare a lot of paperwork; they only need to upload proof of identity, and the money will be transferred to their personal account a short while later.

The OJK Investment Alert Task Force blacklisted 947 unauthorized peer-to-peer lending fintech companies between January 2018 and April 2019. OJK Regulation Number 77/POJK.01/2016, which deals with information technology-based money lending and borrowing public services, is allegedly broken by the company, making it unlawful. According to this rule, fintech businesses need to apply to the OJK for permission to operate. The legal entity's deed of incorporation, ownership registration, shareholder data, and director and commissioner data are the prerequisites that must be fulfilled. Many unlawful fintech applications are still discovered to be operational despite efforts to block nearly a thousand of them. Online inter-party lending, or illegal fintech, is actively providing loans.

Alongside the significant promise of the digital economy and the advancement of information technology, there are a number of drawbacks, such as risks to people' rights to privacy and personal information. One of the essential rights is the right to privacy. Legal protection of the right to privacy is still highly important in this digital economy, even though it is not an absolute human right.

One important thing to keep in mind is that once we start using the internet, everything we do and the websites we visit will be recorded, creating a digital trail. Thus, safeguarding data from unauthorized use by third parties is a delicate matter that is difficult to handle. The

aforementioned advancements and challenges prompt nations and international organizations to further explore these matters and create data processing-related legal frameworks.

E-commerce businesses need to safeguard the personal information of their customers. The practice of asking for family card information when registering for a prepaid card is also controversial. When this type of behavior is confronted with concerns about privacy and the security of customer personal data, serious complications occur. Many people apply for loans online by providing personal information, such as KTPs that contain NIK, and so forth. However, after a while, the information was leaked and disseminated, and the hackers were the ones responsible. In addition to making it simpler for people to obtain loans, there is a drawback: hackers steal personal information, which is subsequently disseminated across other platforms, inevitably resulting in a variety of losses for individuals.

Personal information has frequently been leaked and used for criminal purposes in Indonesia. Crimes and violations of a person's right to privacy include the increasing prevalence of skimming or copying ATM card data and information, online loans made using someone else's personal identity, which frequently results in threats or intimidation, and even the public release of personal information, or "doxing."

Research on "legal protection for victims of personal data theft in online loan transactions after the Covid-19 pandemic" is vital given the background information mentioned above. The restrictions pertaining to personal data in Indonesia are the primary reason for producing this paper. Second, following the Covid-19 epidemic, victims of online loan theft of personal data will have legal protection.

This article's research methodology is: This research activity is an endeavor to comprehend and resolve issues in a methodical, scientific, and logical (makes sense) manner. Given that the issues being researched and studied are also based on the juridical aspect, namely on norms, regulations, and legal theories, the research method used in this study is a normative juridical approach. This research was started because there was a gap between das sollen and das sein, that is, between the existing theory and the reality that occurs in the field. To put it another way, this study is grounded in the realities that exist in the industry as well as relevant legal goods.

Descriptive analytical specifications were employed in this study because it is anticipated that a clear, comprehensive, and systematic picture will be obtained; analytical specifications are utilized because the data collected will be examined to address issues in compliance with relevant legal regulations. In order to present an unbiased image of the reality of the subject under study, the research employs analytical descriptive criteria.

2 Result and Discussion

2.1 Regulations regarding personal data are based on positive law

The right to protect personal data develops from the right to respect private life or is called the right to private life. The concept of personal life relates to humans as living creatures. Thus, individuals are the main owners of personal data protection rights. Privacy is not stated explicitly in the 1945 Constitution. However, the right to privacy is implicitly contained in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia as follows:

“Every person has the right to protection of 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 of doing or not doing something which is a human right“. [3]

Guarantees for the right to privacy are also contained in other laws, namely Article 29 paragraph (1) and Article 30 of Law Number 39 of 1999 concerning Human Rights. Personal Data is a concept that describes the process or effort to combine regulations regarding privacy and personal data which are spread across various legal instruments into one separate legal instrument. Thus the protection of privacy and personal data has a sui generis place.

The European Union has The European Union DP Directive (Directive) was introduced in 1995 with the aim of harmonizing national regulations among EU member states. The Directive is considered one of the regime's most powerful. The latest regulations in the European Union regarding the right to privacy in personal data are in the General Data Protection Regulation (GDPR).[4]

There are laws pertaining to the protection of the right to privacy in a number of Asian nations. The first national law to fully govern privacy and personal data issues was Hong Kong's Personal Data Privacy Ordinance of 1995 (PDPO). The Personal Data Protection Act No. 709 of 2010 (PDPA Malaysia) protects the privacy of personal data in Malaysia. The Personal Data Protection Act No. 26 of 2012 Singapore (PDPA 2012 Singapore) provides sector-specific protection for personal data and privacy in Singapore. [5]

The right to privacy, which includes the protection of personal information, is acknowledged as one of the constitutional rights of citizens in its evolution, particularly following the 1945 Constitutional Amendment. This is consistent with the constitution's special chapter on human rights (the "bill of rights"), which is included in chapter XA, Articles 28A through 28J. Every individual has the right to personal protection, family, honor, dignity, and property under his control, as well as the right to a sense of security and protection from the threat of fear. Article 28G, paragraph (1), contains provisions pertaining to guarantees for the protection of personal data. to exercise or refrain from exercising a human right. A little personal The following laws restrict some personal data settings:

1) Law Number 36 of 1999 concerning Telecommunications.

The transmission, connection, and quick transfer of data and information are all strongly tied to telecommunications activities. Since this data and information transfer can happen extremely quickly, Article 18 paragraphs (1) and (2) govern telecommunications operators' obligations to record or meticulously record the usage of telecommunications services in order to maintain information traffic from telecoms providers. Paragraphs (1) and (2) of Article 18 state:

Article 18 paragraph (1):

“Telecommunications service providers are obliged to record/record in detail the use of telecommunications services used by telecommunications users“.

Article 18 paragraph (2) :

“If a user requires notes/records of the use of telecommunications services as intended in paragraph (1), the telecommunications operator is obliged to provide them“.

Telecommunications service providers are required by the Telecommunications Law's Article 42, paragraph (1), to maintain the confidentiality of information. Among other things,

confidentiality can be broken for the criminal justice system at the written request of the police chief or attorney general, or at the request of investigators. Articles 56 and 57 of the Telecommunications Law contain regulations pertaining to criminal penalties, which include fines and incarceration, for the protection of telecommunications service users' personal data.

2) Law Number 8 of 1999 concerning Consumer Protection.

In theory, the Consumer Protection Law protects information about products and services, but not about the personal information of customers. Promotions are governed by Article 1 Paragraph 6 of the Consumer Protection Law, which states that a promotion is defined as an introduction or dissemination of information about an item and/or to pique consumer interest in purchasing goods and/or services that are currently being traded.

3) Law Number 39 of 1999 concerning Human Rights

Article 29 states: "Everyone has the right to protect himself, his family, his honor, dignity and property rights."

Then in Article 14 paragraph (2) of the Human Rights Law it is stated "that everyone has the right to seek, obtain, possess, store, process and convey information using all types of available means".

Article 31 states that "independence and confidentiality in correspondence relations, including communication relations via electronic means, must not be disturbed, except by order of a judge or other legitimate authority in accordance with the provisions of statutory regulations."

4) Law Number 14 of 2008 concerning Openness of Public Information

That Information is information, statements, ideas, and signs that contain value, meaning, and messages, both data, facts, and explanations that can be seen, heard, and read, which are presented in various packages and formats in accordance with developments in electronic and non-electronic information and communication technology," according to Article 1 paragraph (1) of the KIP Law. On the other hand, information created, maintained, transmitted, and/or received by a public entity that pertains to the state's and/or other public entities' management and administration in compliance with this law, as well as other relevant information, is considered public information [6].

According to the KIP Law, information data gathering is done by a public entity. Article 6 paragraph (3) regulates the protection of public data and information gathered by public entities; among the information that public bodies are not permitted to share is information pertaining to individual rights. These public entities' violations could result in criminal penalties as outlined in Article 52, specifically: “Public Bodies that deliberately do not provide, do not give, and/or do not publish Public Information in the form of Public Information on a regular basis, Public Information that must be announced immediately, Public Information that must be available at any time, and/or Public Information that must be is given on the basis of a request in accordance with this Law, and results in loss to another person, subject to imprisonment for a maximum of 1 (one) year and/or a fine of a maximum of IDR 5,000,000.00 (five million rupiah)".

5) Law Number 10 of 1998 concerning Banking

Legal protection mechanisms for customers in banking institutions, one of the important economic activities is banking activities. In Indonesia, banking regulations are regulated in law

Number 10 of 1998 concerning Banking. In the Banking Law, the protection of customer personal data is regulated as bank secrecy. Bank secrecy is everything related to information regarding deposit customers and their deposits. Then in Article 40 it is stated that banks are obliged to keep information regarding deposit customers and their deposits confidential, except in certain permitted cases. Article 47 paragraph (2) also states that those who uphold bank secrets are members of the board of commissioners, directors, bank employees or other affiliated parties, and if they deliberately provide information that must be kept confidential according to Article 40, they are threatened with imprisonment for at least 2 (two)) year and a fine of at least IDR 4,000,000,000.00 (four billion rupiah) and a maximum of IDR 8,000,000,000.00 (eight billion rupiah).

6) Law Number 36 of 2009 concerning Health

Article 57 paragraph (1) which states a person's right to the confidentiality of their personal health conditions which have been disclosed to health service providers. Meanwhile, paragraph (2) regulates exceptions to the confidentiality of personal health conditions which do not apply in the case of:

a) Statutory orders;

b) Court order;

c) Concerned permits;

d) Community interests;

e) The person's interests.

7) Law Number 24 of 2013 Amendment to Law Number 23 of 2006 concerning Population Administration (UU Adminduk)

Individual data and/or structured aggregate data resulting from Population Registration and Civil Registration activities are considered population data, according to Article 1 of the Population Administration Law. Subsequently, Article 1 Paragraph 22 explains that personal data is defined as specific individual information that is kept, preserved, and safeguarded as confidential. We can infer from the provisions in a number of Article 1 numbers that the Population Administration Law has, in fact, attempted to safeguard the personal information of its residents. The implementing agency handling population administration matters is then required to ensure the security and confidentiality of data on population events and significant events, according to article 8 paragraph (1) The implementing agency handling population administration concerns is also required to ensure the security and confidentiality of data on population events and significant events, according to letter (e).

8) Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE)

Article 26 paragraph (1) states that the use of any information via electronic media that concerns a person's personal data must be carried out with the consent of the person concerned. The explanation of the article also contains the meaning of personal data as part of the use of Information Technology, the protection of personal data is one part of personal rights (privacy rights). Personal rights contain the following meaning:

a) Personal rights are the right to enjoy private life and be free from all kinds of interference.

b) Personal rights are the right to be able to communicate with other people without spying.

c) Personal rights are the right to monitor access to information about a person's personal life and data .

9) Law Number 27 of 2022 concerning Protection of Personal Data (UU PDP)

There is hope for legal protection against the numerous criminal cases of personal data misuse in Indonesia that stem from data leaks and theft of personal data with the ratification of Law No. 27 of 2022 about Personal Data Protection. This law's existence grants the government the power to monitor how administrators of electronic systems handle personal data. According to this law, personal data is information about natural individuals that may be directly or indirectly identified through electronic or non-electronic means, either separately or in combination with other information. Personal data protection, on the other hand, refers to the collective endeavor to safeguard personal data during the processing of personal data in order to ensure the constitutional rights of personal data subjects. This law separates personal data into two categories: personal data of a specific nature and personal data of a general nature. This allows for the proper protection of personal data and ensures that it satisfies all regulations. According to paragraph (2) of Article 4, certain categories of personal information consist of:

1. Health data and information;

2. Biometric data;

3. Genetic data;

4. Criminal record;

5. Child data;

6. Personal financial data;

7. Other data is in accordance with statutory provisions. [7]

The author believes that the regulation pertaining to criminal records is in specific data criteria where a person's criminal records receive different treatment compared to general data, as stated in Article 34, which mandates that personal data controllers conduct data protection impact assessments in cases where processing of personal data has the potential to pose a high risk to personal data subjects. In this particular data, the position of criminal records is included in a specific category of personal data. Processing unique personal data is one of the high-risk activities that might occur when processing personal data. Because the public is unaware of their criminal histories, it is thought that this will make it simpler for corrupt officials to run for office again after serving their sentence and to enter the general election process. In the meantime, paragraph (3) contains general personal data, which can be of the following types:

1. Full name;

2. Gender;

3. Citizenship

4. Religion;

5. Marital status;

6. The combined personal data identifies an individual.

3.2 Legal Protection for Victims Who Experience Personal Data Theft

Some examples of cases related to personal data in Indonesia in the form of data leaks and data buying and selling, include:

a) BRI Life Customer Data Leak Case: In 2021, two million BRI Life customers experienced a leak and were sold online. Information about the leak of BRI Life customer data was uploaded to a Twitter account on Tuesday, July 27 2021. In the upload , it was written that the perpetrator threatened to sell BRI Life's sensitive data. Hackers allegedly stole 250 gigabytes of insurance company customer data and sold it for US$ 7,000 or Rp. 101.5 million. This data contained a number of information such as photos of ID cards, accounts, taxpayer numbers, birth certificates, and even medical records .

b) Tokopedia User Data Leak Case In 2020, as many as 91 million user data and 7 million Tokopedia application merchandise data were leaked and reportedly sold on dark sites or the dark web. Based on this case, Tokopedia even confirmed that this user data leak did occur and claimed it was carried out by a third party. Managers In this case, Tokopedia confirmed that the incident of user data theft had been investigated and collaborated with the government, in this case the National Cyber and Crypto Agency (BSSN) and the Ministry of Communication and Information.

c) BPJS Health Data Leak Case: In 2021 there was also a leak of Indonesian citizens' data which was data from BPJS Health. This data contains 20 million personal photos, then the data also contains Population Identification Number (NIK), telephone number, e-mail, address and salary. In fact, this data also includes data on residents who have died. This personal data was sold for 0.15 bitcoin, which, if converted to the rupiah value at that time, was worth IDR 81.6 million.

Some of the cases above are some of the number of cases of personal data leakage in Indonesia. Some of the data that was leaked and traded illegally came from government, BUMN and private company data. This case shows evidence of Indonesia's vulnerability regarding personal data security. Data from Surfshark, a cyber security company, places Indonesia as the third country with the highest number of data leak cases in the world. Surfshark data recorded 12.74 million accounts experiencing data leaks in Indonesia during the third quarter of 2022. The most data leaks occurred in Russia, followed by France .[8]

In the context of implementing the protection of privacy as part of human rights which explains the recognition, respect and protection of human dignity. According to Danrivanto Budhijanto, protection of personal rights or private rights will increase human values, improve relations between individuals and society, increase independence or autonomy to exercise control and obtain appropriateness, as well as increase tolerance and avoid discrimination and limit government power.

The concept of the right to privacy through the protection of personal data which is inherent in every person is then divided into several types, namely:

1. Privacy of Information This contains the privacy of information relating to various personal information owned by each person, such as personal data, medical records, electronic post, electronic data encryption, and so on.

2. Physical Privacy This contains the privacy of the right not to be pressured, searched and arrested by the government which applies to individuals who exercise the right to freedom of expression in public.

3. Privacy to discover one's identity This contains privacy to determine one's identity, which is the freedom for each person to determine what they want without interference from other parties, such as abortion, suicide, changing religions, transgender, etc.

4. Privacy of Property This contains privacy for property ownership, which is the right of every person to own identity, intellectual property and physical property .

The DPR RI passed the PDP Law on September 20 2022. This was triggered by international vigilance regarding personal data protection regulations, so that currently there are 132 countries that have special legal products such as the PDP Law. At the ASEAN level, Indonesia is the 5th country that has passed a personal data protection law following Malaysia, Singapore, the Philippines and Thailand. When viewed based on its substance, the PDP Law regulates crucial matters such as the categorization of data as stated in Article 4, which reads "Personal Data consists of: a. Specific Personal Data; and b. Personal data of a general nature." Furthermore , the rights of data subjects are also emphasized in Articles 5 to Article 15. This collection of articles discusses what rights individual people have attached to their personal data. Apart from rights, there are also obligations of data controllers who consist of every person, public body and international organization who then act alone or collectively to achieve the goals and control of the processing of personal data. All matters regarding the obligations of data controllers are further detailed in Articles 20 to 50. Not only that, the PDP Law also emphasizes that the establishment of a personal data protection agency will be directly responsible to the President. This provision is contained in Articles 58 to Article 60 .

Based on Article 37 POJK No. 77 of 2016, fintech operators are obliged to be responsible for user losses arising from errors and/or negligence of the directors and/or employees of the organizers. Then in Article 12 paragraph (1) Personal Data Subjects have the right to sue and receive compensation for violations of the processing of Personal Data about themselves in accordance with statutory provisions. So personal data subjects can file a lawsuit based on Article 64 paragraph (1) of the PDP Law which states "Settlement of personal data disputes can be carried out through arbitration, court, or other alternative dispute resolution institutions in accordance with the provisions of statutory regulations . [9]

Based on the statement above, it can be said that if personal data is misused, fintech service users can take the following legal steps:

1. Report to Relevant Institutions

Fintech operators who use personal data without the owner's consent may be subject to administrative sanctions based on the PDP Law and POJK 10/2022. Users of fintech services can report violations to the Financial Services Authority (OJK) if there is no approval for processing personal data or the fintech operator does not comply with the principles as regulated in the PDP Law and POJK 10/2022. The administrative sanctions for the fintech operator are a written warning which is accompanied by blocking of the organizer's electronic system, restrictions on business activities, and revocation of permits. Meanwhile, in the PDP Law, users of fintech services can report to the agency administering personal data protection which will be determined by the President in accordance with the provisions of Article 58 of the PDP Law. The administrative sanctions based on Article 57 of the PDP Law, namely: a. Written warning; b. Temporary suspension of personal data processing activities; c. Deletion or destruction of personal data; and/or d. Administrative fines are imposed at a maximum of 2% of the annual income for variable violations.

2. Suing Civil

Based on Article 12 paragraph (1) of the PDP Law, personal data subjects have the right to sue and receive compensation for violations of the processing of personal data about themselves in accordance with statutory provisions. Regulating similar matters in Article 26 paragraph (1) of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions states "Unless otherwise determined by statutory regulations, the use of any information via electronic media shall be regarding a person's personal data must be done with the consent of the person concerned." So every person whose rights are violated can file a lawsuit for the losses caused. To file a lawsuit for misuse of personal data, the injured party can file an unlawful action based on Article 1365 of the Civil Code which states "Every unlawful act that causes harm to another person requires that the person whose fault caused the loss, compensate for these losses." A civil lawsuit begins by making a lawsuit letter tailored to the requirements, then submitting it to the district court. After checking that the lawsuit meets the requirements, a trial schedule will be set and a proper summons will be issued to attend the trial. In the trial process, the lawsuit will be read, duplicate statements, evidence will be carried out, and the judge will deliver a decision.

3. Criminal Reporting

Based on the PDP Law, if a fintech operator misuses personal data, it can be reported criminally. Article 66 of the PDP Law says "everyone is prohibited from creating false personal data or falsifying personal data with the intention of benefiting themselves or others which could result in harm to others", Then Article 65 of the PDP Law says: a. Every person is prohibited from unlawfully obtaining or collecting personal data that does not belong to him with the intention of benefiting himself or another person which could result in loss to the personal data subject. b. Everyone is unlawfully prohibited from disclosing personal data that does not belong to them.

c. Everyone is prohibited from unlawfully using personal data that does not belong to them.

Article 67

(1) Any person who intentionally and unlawfully obtains or collects nonmililoeya Personal Data with the intention of benefiting themselves or another person which may result in loss to the Personal Data Subject as intended in Article 65 paragraph (1) shall be punished with a maximum imprisonment 5 (five) years and/or a maximum fine of IDR 5,000,000,000.00 (five billion rupiah).

(2) Every person who intentionally and unlawfully discloses Personal Data that does not belong to him as intended in Article 65 paragraph (2) shall be punished by a maximum imprisonment of 4 (four) years and/or a maximum fine of Rp. 4,000,000,000, 00 (four billion rupiah).

(3) Every person who deliberately and unlawfully uses Personal Data that does not belong to him as intended in Article 65 paragraph (3) shall be punished with a maximum imprisonment of 5 (five) years and/or a maximum fine of Rp. 5,0000.000. 000.00 (five billion rupiah).

For criminal acts committed by corporations, penalties can be imposed based on Article 70 of the PDP Law, where penalties can be imposed on management, control holders, givers of orders, beneficial owners, and/or corporations. The fine imposed on a corporation is a maximum of 10 (ten) times the maximum fine threatened. Apart from that, corporations can be subject to additional criminal penalties based on Article 70 paragraph (4) of the PDP Law, namely: a. confiscation of profits and/or assets obtained or proceeds of criminal acts; b. freezing all or part of corporate business; c. permanent prohibition on carrying out certain acts; d. closure of all or part of business premises and/or corporate activities; e. carry out obligations that have been neglected; f. payment of compensation; g. revocation of permits; and/or h. dissolution of the corporation.

4. Arbitrage

Based on Article 1 paragraph (1) of Law Number 30 of 1999 concerning Arbitration and Alternative Dispute Resolution, arbitration is a method of resolving civil disputes outside the general court which is based on an arbitration agreement made in writing by the parties to the dispute, if it is related to the dispute. technology-based money lending and borrowing, then dispute resolution can only be resolved through arbitration if the parties have agreed to resolve it through arbitration which is made in the form of an agreement, or stated in the parties' electronic document agreement. Based on the Arbitration and Alternative Dispute Resolution Law, there are three stages of the dispute resolution mechanism through arbitration, namely the preparation or pre-examination stage, the examination or determination stage, and the implementation stage. The preparatory stage is the stage for preparing everything for the case examination hearing. The preparation stage includes: a. Agreement to arbitration in a written document; b. Appointment of arbitrator; c. Submission of a letter of demand by the applicant; d. Answer to the letter of demand by the respondent; e. The arbitrator's order that the parties appear before the arbitration hearing. [10]

5. Negotiation

Negotiation is one way of resolving disputes outside of court involving the disputing parties. This means that parties who are not related to the dispute cannot involve themselves in negotiations. Negotiations are carried out in the following stages: a. Preparation stage In the

preparation stage, what must be prepared is what is needed and desired, where each party must know what is in their respective interests. b. Initial offer stage: This stage, a negotiator will strategize about who should submit an offer first and how to respond to the initial offer. If there are two offers in negotiations, usually the midpoint (the point between the two offers) can be used as a solution or agreement. Before the midpoint is made into an agreement, it should be compared with the opinions of the parties. c. Stage of granting concessions This stage of concessions must be expressed depending on the context of the negotiation and the concessions granted by the opposing party. A negotiator must make the right calculations regarding aggressiveness, such as how to maintain good relations with the opposing party, empathy for the opposing party, and fairness. Negotiators have a very important role in concessions and maintaining bargaining positions until the desired agreement is reached. d. Final stage of negotiations This final stage includes making commitments or canceling previously stated commitments.

6. Mediation Dispute resolution through mediation, namely resolving disputes outside of court by inviting a third party as a mediator. The stages of mediation are:

   a. Forum formation stage
   b. Information collection and sharing stage
   c. Problem solving stage
   d. Decision making stage.[11]

4 Conclusion

The conclusion in this article is

1. Regulations regarding personal data are regulated in various laws and regulations, including Law Number 7 of 1992 concerning Banking as amended by Law Number 10 of 1998, Law Number 23 of 2006 concerning Population Administration as amended by Law. Law Number 24 of 2013 concerning Amendments to Law Number 23 of 2006 concerning Population Administration, Law Number 36 of 2009 concerning Health, Law Number 39 of 1999 concerning Rights. Human Rights, Law Number 43 of 2009 concerning Archives, Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions, Regulation of the Minister of Communication and Information Number 20 of 2016 concerning Protection of Personal Data in. Electronic Systems in force since December 2016, Government Regulation Number 80 of 2019 concerning Trading Through Electronic Systems, Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 20 of Indonesia 2016 concerning Protection of Personal Data in Electronic Systems, and finally, Financial Services Authority Circular Letter Number 14/SEOJK.07/2014 concerning Confidentiality and Security of Consumer Personal Data and/or Information and more specifically regulated in law Number 27 of 2022 regarding personal data protection.
2. Legal protection for people or legal subjects who experience data theft can take several legal steps, namely reporting to the related institution of the fintech operator, suing civilly. Based on Article 12 paragraph (1) of the PDP Law, personal data subjects have the right to sue and receive compensation for violations of personal data processing. regarding

himself in accordance with the provisions of statutory regulations, Reporting Criminally Based on the PDP Law, if a fintech operator misuses personal data, it can be reported criminally. Article 66 of the PDP Law Dispute Resolution Against Alleged Misuse of Personal Data in Fintech Services Syntax Literate, Vol. 7, no. 11, November 2022 17182 says "everyone is prohibited from creating false personal data or falsifying personal data with the intention of benefiting themselves or others which could result in harm to others", Arbitration Based on Article 1 paragraph (1) of Law Number 30 of 1999 concerning Arbitration and Alternative Dispute Resolution, that arbitration is a method of resolving civil disputes outside the general court which is based on an arbitration agreement made in writing by the parties to the dispute, if it is related to a technology-based money lending and borrowing dispute, then the new dispute resolution can be resolved through arbitration if the parties have agreed to resolve it by arbitration which is made in the form of an agreement, or stated in the parties' electronic document agreement. The dispute cannot involve itself in negotiations. Mediation Dispute resolution through mediation, namely resolving disputes outside of court by inviting a third party as a mediator.

References

[1] K. R. Anggen Suari and I. M. Sarjana, "Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia," *J. Anal. Huk.*, vol. 6, no. 1, pp. 132–142, 2023, doi: 10.38043/jah.v6i1.4484.

[2] S. Utomo, A. Alfian, and L. Aprilia, "Penegakan Hukum Terhadap Aktivitas Pinjaman Online," *Crepido*, vol. 4, no. 2, pp. 70–82, 2022, doi: 10.14710/crepido.4.2.70-82.

[3] M. Zainuddin, *Pemahaman Metode Penelitian Hukum (Pengertian, Paradigma, Dan Susunan Pembentukan)*. Yogyakarta: CV.Istana Agency, 2019.

[4] R. A. E. Wahyuni and B. E. Turisno, "Praktik Finansial Teknologi Ilegal Dalam Bentuk Pinjaman Online Ditinjau Dari Etika Bisnis," *J. Pembang. Huk. Indones.*, vol. 1, no. 3, pp. 379–391, 2019, doi: 10.14710/jphi.v1i3.379-391.

[5] E. Supriyanto and N. Ismawati, "Sistem Informasi Fintech Pinjaman Online Berbasis Web," *J. Sist. Informasi, Teknol. Inf. dan Komput.*, vol. 9, no. 2, pp. 100–107, 2019.

[6] M. H. dan I. D. W. P. CHRISTINE S.T.KANSIL, S.H., "Penyelesaian Sengketa Terhadap Dugaan Penyalahgunaan Data Pribadi Dalam Layanan Fintech," *J. Ilm. Indones.*, vol. 7, no. September, 2022.

[7] S. Tiffani and Faisal, "Analisis Hukum Terhadap Perlindungan Data Pribadi (Studi Kasus @farida.nurhan dan @codebluuuu)," *J. Ilmu Hukum, Hum. dan Polit.*, vol. 4, no. 3, pp. 291–300, 2024, doi: 10.38035/jihhp.v4i3.1915.

[8] E. Fauzi and N. A. Radika Shandy, "Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," *J. Lex Renaiss.*, vol. 7, no. 3, pp. 445–461, 2022, doi: 10.20885/jlr.vol7.iss3.art1.

[9] B. K. Arrasuli and K. Fahmi, "Perlindungan Hukum Positif Indonesia Terhadap Kejahatan Penyalahgunaan Data Pribadi," *UNES J. Swara Justisia*, vol. 7, no. 2, p. 369, 2023, doi: 10.31933/ujsj.v7i2.351.

[10] A. Ayu, T. Anindyajati, and A. Ghoffar, "Perlindungan Hak Privasi atas Data Diri di Era Ekonomi Digital," *Pus. Penelit. Dan Pengkaj. Perkara, Dan Pengelolaan Perpust. Kepaniteraan Dan Sekr. Jenderal Mahkamah Konstitusi*, p. 101, 2019.

[11] R. A. E. Wahyuni and B. E. Turisno, "Praktik Finansial Teknologi Ilegal dalam Bentuk Pinjaman Online ditinjau dari Etika Bisnis," pp. 1–23, 2016.