JOURNAL OF SOCIAL SCIENCE
Printed ISSN: 2720-9938
Electronic ISSN: 2721-5202
jsss.co.id

Legal Liability of Illegal Online Loans in the Perspective of Criminal Law

Vanti Y. Rolobessy, Faissal Malik, Suwarti
Khairun Ternate University North Maluku, Indonesia
Email: valyvanty@gmail.com, faissalmalik10@gmail.com, warti730@gmail.com

ARTICLE INFO

Date received: January 2, 2023
Date revised: February 10, 2023
Date accepted: 20 March 2023

Keywords:
Legal Liability, Illegal Online Loans, Overlapping, IUP, North Maluku Province

ABSTRACT

This study aims to analyze law enforcement of misuse of personal data related to illegal online loans (fintech) as a form of mayantara crime in a cyber perspective and examine the liability of illegal online loans (illegal fintech desk collectors) in a criminal law perspective. The research method used in this study is the type of research used in the research is normative legal research as a process to find the rule of law, legal principles, and legal doctrines to answer the legal issues faced. The scientific logic that in normative legal research is built on scientific discipline and the ways in which normative legal science works, that is, legal science whose object is law itself. The results of this study show that the enforcement of the Law on Misuse of Personal Data Related to Online Loans (Illegal Fintech) as a Form of Mayantara Crime in a Cyber Perspective is based on the reason that the rampant public activities on electronic media, the Electronic Transaction Information Law was born, namely Law Number 19 of 2016 on Law Number 11 of 2008 concerning Electronic Information and Transactions concerning Electronic Information and Transactions (ITE) with Considerations can be found in the consideration section, especially in the "Considering" section which states that information globalization has placed Indonesia as part of the world information society so that it requires the establishment of regulations regarding the management of Information and Electronic Transactions at the national level so that the development of Information Technology can be carried out optimally, evenly, and spread to all levels of society in order to educate the nation's life.

INTRODUCTION

Currently, the mode of crime is increasingly varied with the support of technological developments, so that the technology is also used by deception as a mode of crime that results in crime from the technology. One growing feature is the Intranet. Information technology only explains the development of existing devices in information processors only. Electronic media and information technology can be used as a pioneer that can determine the entire world system both in economic, financial, social and cultural aspects, so that these developments can help humans in everyday life.

The development of technology today causes the emergence of financial services with information technology which is usually called Financial Technology or fintech. Through fintech, transactions become faster in making payments without having to meet face-to-face.

Technological advances at this time, can increase development in all sectors of life in society. So that it makes it easier for him to do everything he wants to do, and bring the life of people who were originally traditional patterns to be more modern or can also be called modernization.

Current technological advances should be put to good use in order to change behavior and can help solve every problem that is being faced. Many of the younger generation use the internet in their daily lives to feel the advantages of fintech that can be used more easily and practically. The second reason fintech is growing faster is because with this increasingly fast technological state, it can help work for fintech business actors to complete their work very quickly and easily.

Currently, Indonesian people seem to be increasingly familiar with the online world. No exception in financial matters, many people are now using online loan services. This can be seen from data from the Financial Services Authority (OJK) which recorded an increase in the value of online loans in September 2021 of IDR 26.09 trillion. This number has increased rapidly compared to the year-on-year with the new September 2020 of Rp.12.71 trillion.

One example of a related case is online loans, the case is much discussed because the case took many lives and many complained into criminal fraud. As the name implies, online loans are loan credit services that use information technology, this loan has begun to develop since mid-2014. Many people are starting to use online loans because in today's era the needs are no longer just limited to meeting but only using the internet, everything can be faster and easier. Even people no longer need to go to the bank and apply directly to get the loan. With this convenience, many people choose online loans instead of having to borrow from banks. From this convenience arises a gap in criminal acts. So, based on data released on August 17, 2021, the Ministry of Communication and Information has blocked more than three thousand platforms, including unlicensed online loans. This number is up two thousand five hundred more than in June 2020. This is also due to online loan cases that are increasingly found problematic.

Although there are institutions authorized to regulate online loans in Indonesia, Bank Indonesia (BI) and the Financial Services Authority (OJK). BI has several regulations regarding online loans, namely BI Regulation Number 18/40/PBI/2016 concerning the Implementation of Payment Transaction Processing, BI Regulation Number 19/12/PBI/2017 concerning the Implementation of Financial Technology, Regulation of Members of the Board of Governors Number 19/14/PADG/2017 concerning Procedures for Registration, Information Submission, and Monitoring of Financial Technology Operators. Then OJK also has OJK Regulation Number 77 / POJK.01 / 2016 concerning Information Technology-Based Money Lending and Borrowing Services. However, of the two institutions, only OJK has the authority to supervise online loan companies.

However, amid the widespread use of online loan services in the community, illegal online loan companies are also rife. The emergence of illegal online loans certainly has the potential to harm consumers who use online loan services. This is because there are often unlawful acts committed by illegal online loan companies such as the use of violence in payment collection to theft of user personal data. It does not rule out the possibility if there are still illegal loan applications that can make consumers trapped in debt and online loan fraud with the lure of ease of loan requirements. Consumers are also advised to be more careful and more selective in using loan services so as not to be entangled in cases of online loans that are even detrimental.

Here are some examples of cases of illegal online loans that harm the community. As happened to a mother in Wonogiri decided to end her life or commit suicide due to continuous acts of terror carried out by illegal online lenders. With the illegal online loan case, the authorities immediately moved quickly by arresting 3 suspects related to the case and confiscating evidence amounting to Rp. 21 billion.

Another example of an illegal loan case is threats, not infrequently the illegal online loan party threatens to spread personal data owned by customers to cyberspace. This of course often disturbs the community because currently there is also often misuse of personal data. Because there is a requirement to include personal data when applying for the loan, not infrequently many people also become victims of misuse of the data by receiving messages of unknown origin. From

this convenience arises a gap in criminal acts. Thus, legal problems that arise due to illegal online loans are fraud, extortion, threats, to invasion of privacy.

Based on the above facts, it becomes a logical consequence that the responsibility for debtors who fail to pay off their debts is that the debtor still has to pay off the debt because it has made an agreement and has received the loan money. However, if the debtor does not have good faith, it can be subject to Article 378 of the Criminal Code on Fraud for violating existing agreements and can be threatened with a maximum prison sentence of 4 (four) years. The criminal threat of raising funds without permission is very severe, and there is no substitute for a monetary fine if the fine cannot be met (subside) is not in the law which shows how severe the penalty is. The rise of cases in the field of online loans under the guise of investment has harmed the community a lot. The term is better known as raising funds. The criminals who raise these funds lend money on easy terms and provide very large interest so that creditors can benefit from the interest proceeds.

Criminal liability through online loans for debtors who fail to pay must still pay off their debts and if there is no good faith, they are charged with Article 378 of the Criminal Code, and creditors can be subject to Article 368 of the Criminal Code and Article 369 of the Criminal Code concerning extortion and threats, Article 29 jo. Article 45 paragraph (3) of the ITE Law. Not only involving individual actors but also corporations. Although corporations are subjects of law, the punishment is still imposed by individuals or directed directly at perpetrators who violate the law.

Based on the description that the author has stated above Together with everything related and background in this study, the author is interested in conducting a thesis research entitled "Legal Responsibility of Illegal Online Loans in a Criminal Law Perspective. In this legal research, there are several objectives that will be discussed in this study, namely For law enforcement misuse of personal data related to illegal online loans (fintech) as a form of mayantara crime in a cyber perspective. To analyze the liability of illegal online loans (illegal fintech desk collectors) in a criminal law perspective

METHOD

The type of writing research in this study is to use normative laws, because in the analysis it uses literature material as a source of research data. The normative research here is to analyze the law enforcement of the Financial Services Authority (OJK) in protection against misuse of personal data in illegal online loans and legal liability of illegal online loans in the perspective of criminal law. In legal research, this type is included in the category of normative legal research or literature law research, therefore in this research library materials are basic data which in research science is classified as secondary data.

RESULTS AND DISCUSSION

A. **Law enforcement misuse of personal data related to *online* loans (*illegal fintech*) as a form of Mayantara crime in a cyber perspective**.

The development of information technology has caused the world to become borderless and caused significant social changes to take place so quickly. Information Technology is currently a double-edged sword, because in addition to contributing to the improvement of human welfare, progress and civilization, it is also an effective means of unlawful acts, such as fraud, violations of intellectual property rights, child exploitation or pornography, *hecking*, violations of one's personal life, computer virus transmission, and defamation that is familiar in cyberspace. That way technological developments also provide solutions to crimes experienced by humans The technological and information revolution since the end of the 20th century gave birth to many new legal acts throughout the world, including in the jurisdiction of the Republic of Indonesia.

Electronic business practices develop (*e-business*), for example, the application of communication and information technology to support the business activities of a person,

group of people, or one business entity. Electronic commerce creates an exchange of products and services between traders, individuals, groups of people, and business entities (Ahmadi &; Hermawan, 2013). All organizations operate in an environment that affects the way they do business. The development strategy must consider the environment in which the business operates. To inform *e-commerce* strategy, the most significant influence is from the direct market, i.e. from the microenvironment shaped by customer needs and how services are provided to them through competitors and intermediaries.

Wider influence is exerted by local and international economic conditions and legislation along with any business practices that are acceptable to the community. Finally, technological innovation is essential in providing the opportunity to provide superior services from competitors or through changing the shape of the market. So technology is present as one of the tools for law enforcement officials to eradicate crime.

One of the rapid technological developments taking place today is *e-commerce*, which offers practical, fast, easy, and inexpensive business models around the world since the end of the 20th century. The synergy of computers and telecommunications systems creates new benefits in the form of ease, accuracy, and speed of billions of transactions per second worldwide. Commercial transaction performance is increasing through *e-commerce* which has three special advantages, namely *"accuracy, speed* and *efficiency*. The development of *e-commerce* is one example of the success of digital transformation in the economic field, in the economic context, digital transformation is defined as the massive use of technology to improve the performance or profits of business actors or companies.

One of these digital transformations is *fintech*, which when translated into Indonesian is financial technology which consists of two words, namely "technology and finance" The term technology refers to the use of new technologies and innovative business models that change traditional patterns or habits that already exist. Then the term financial refers to financial services in the banking industry, financing industry, investment, insurance industry, and other financial industries. Thus, *fintech* can be defined as the use of technology in financial service innovation through the internet network.

*Fintech*is a financial service that uses information technology innovatively, effectively and efficiently where its existence disrupts financial institutions, which have functions for payments, money transfers, submitting loan requests, purchasing insurance, asset management, and investment. The positive growth of fintech in Indonesia has made many people start using fintech for transaction services, at this time fintech has become the world's attention as one of the technologies that will be widely used by business people and companies to compete with their competitors.

According to the author, online loans are a type of loan that is submitted only enough online through a smart phone application, without the need for face-to-face meetings. This method certainly provides convenience and speed in the process of applying for a loan or credit. In Indonesia, online loans are growing rapidly. The speed and convenience offered are the main and special attraction. Applying for loans or credit that is known for a long time and difficult so far, can now be done easily, quickly, online, and does not need to meet or face to face. Prospective borrowers simply download online loan applications on mobile phones via the play store or APK.

The legal basis for online loans is regulated by OJK Regulation Number 77/POJK.01/2016 of 2016 concerning information technology-based lending and borrowing services. This is the implementation of financial services to bring together lenders and recipients in order to make loan agreements and borrow rupiah currency directly through an electronic system using the internet. Launching from the @ojkindonesia account, the official Instagram account of OJK, there are several main characteristics of illegal online loan applications :

1. Illegal online loans often offer via SMS spam (*SMS Spam* is a short message sent to users, it is not known who the sender is)

2. The loan fee is very high from the loan amount that can reach 40%.
3. Interest rates and fines are very high, which can reach 1% to 4% per day.
4. The loan repayment period is very short and not according to the agreement.
5. Illegal online loans always ask for access to all data on mobile phones, such as contacts, photos, videos that will be used to terrorize borrowers when defaulting.
6. Illegal online loans carry out unethical collection such as terror, intimidation, and harassment.
7. Online loans do not have a complaint service and the identity of the office is clear.
8. Online loans are not registered with OJK.

Illegal online loans often disturb the community because of several actions that make people worried. In addition to the flowers that are relatively large and far from what they should be. Illegal borrowing also often makes any customer frightened when they have arrears. Here are some examples of cases of illegal online loans that harm the community (Triansyah, Julianti, Fakhriyah, &; Afif, 2022).

1. Acts of terror that cause victims to commit suicide

   A mother in Wonogiri decided to end her life or commit suicide due to continued acts of terror carried out by illegal online lenders. With the illegal online loan case, the authorities immediately moved quickly by arresting 3 suspects related to the case and confiscating evidence amounting to Rp. 21 billion.
2. Threats made by illegal borrowing

   Another example of an illegal loan case is a threat, not infrequently the illegal online loan party threatens to spread personal data owned by customers to cyberspace. This of course often disturbs the community because currently there is also often misuse of personal data.
3. Misuse of Illegal Pinjol Personal Data

   Anotherillegal loan that is often done is the misuse of personal data from its customers. Because there is a requirement to include personal data when applying for the loan, not infrequently many people also become victims of misuse of the data by receiving messages of unknown origin. In fact, there are often cases of loans without evidence where victims get bills from loans that the victims themselves never feel borrowed from related parties.

If viewed by regulations in Indonesia, at this time there has been no unification of personal data regulation, even though problems regarding personal data have occurred in Indonesia, in 2021 there were six cases of personal data leakage in Indonesia, namely: (Nurhadi, 2022)

1. BPJS Healthcare data leak

   In May 2021, a number of BPJS user data in Indonesia was leaked due to hacking by irresponsible parties and then traded on the Raid forums market place for 0.15 Bitcoin
2. Drill data carefully and lazada

   There were 2.9 million personal data from the site from 17 companies traded on the raid market place, while Lazada had a data leak of 1.1 million personal data.
3. BRI customer data leakage

   There were 463,000 thousand personal data leaked and then traded Rp. 101.6 million which circulated widely in cyberspace, especially on social media twitter.
4. Tokopedia data leak

   As many as 91 million personal data of Tokopedia users were leaked, and traded US $ 5,000 on the darweb site, the incident was due to the actions of irresponsible parties who had hacked Tokopedia.
5. Election Commission data leak

   As many as 2.3 million personal data was leaked due to misuse from third parties and then traded freely in cyberspace such as on social media Twitter. The rise of public activities on electronic media led to the birth of the Electronic Transaction Information Law, namely Law Number 19 of 2016 on Law Number 11 of 2008 concerning Electronic

Information and Transactions on Electronic Information and Transactions (ITE) with considerations can be found in the consideration section, especially in the "Weighing" section which states (Fitri, 2022) that the globalization of information has placed Indonesia as part of the world information society so that it requires the establishment of regulations regarding the management of Electronic Information and Transactions at the national level so that the development of Information Technology can be carried out optimally, evenly, and spread to all levels of society in order to educate the nation's life. The government also needs to support the development of Information Technology through legal infrastructure and regulation so that the use of Information Technology is carried out safely to prevent its misuse by taking into account the religious and socio-cultural values of the Indonesian people.

Based on the complexity of the problem above, according to the author, law enforcement misuse of personal data related to *illegal online loans* as a form of crime in a cyber perspective can be viewed from 2 (two) main aspects as follows:

1) Policy *on the Discontinuation of Personal Data Storage in Electronic Media.*

The 4th paragraph of the Preamble to the Constitution of the Republic of Indonesia in 1945, states that the Government of the State of Indonesia has a constitutional obligation to protect the entire Indonesian nation and all Indonesian bloodshed and to promote general welfare, educate the life of the nation, and participate in implementing world order based on independence, lasting peace, and social justice. In the context of the development of information and communication technology, the purpose of the state is realized in the form of protecting personal data from every Indonesian resident or citizen.

It is generally accepted that the 1945 NRI Constitution as the Constitution provides policies in responding to personal data theft by protecting personal property from parties who try to breach or steal someone's personal data in electronic media. Law as a *legal policy* in a government administration in order to achieve state goals is an important instrument in the rule *of law* (Agang, 2015).

Such a situation results in the consequence that a regulation formed by the government is an instrument to provide legal protection and enforcement of human rights (HAM) for citizens. Thus, the urgency of providing legal protection to personal data began to strengthen along with the increasing number of mobile phone and internet users. A number of cases that arise, especially those related to the leakage of one's personal data and lead to fraud or criminal acts, especially illegal online loans (pinjol) strengthen the discourse on the importance of making legal rules to protect personal data.

The issue of personal data leakage indicates the importance of legal arrangements regarding personal data in Indonesia, this cannot be considered trivial by the government as a lawmaker (legislative institution), more and more personal data is leaked but the formation of laws regarding personal data never ends. Until now, the draft personal data law has never been passed and is still under discussion in the national legislature which has been discussed three times.

The misuse of personal data, it can be seen that there is a system weakness, lack of supervision, so that personal data can be misused and result in losses for the owner of the data. Misuse, theft, sale of personal data is a violation of law in the field of information technology and can also be categorized as a violation of human rights, because personal data is part of human rights that must be protected. In this regard, there are several examples of cases of misuse of personal data, such as online loans, where the transaction mechanism fills in data online but in the case of late payments it is not uncommon to use collectors to intimidate customers, customers' families, leaders where customers work and can even access data from customers' mobile phones.

Based on this reality, according to the author, misuse of personal data is an act that fulfills the elements of criminal acts such as elements of theft and elements of fraud and other criminal acts both in terms of objective and subjective elements. With the fulfillment of these elements, administrative sanctions, civil sanctions and criminal sanctions are not enough to accommodate the criminal act of misuse of personal data which is in fact a perfect form of crime.

Strictly speaking, actions that violate the prohibitions stipulated in the rules of law and do not fulfill or contradict the orders that have been stipulated in the applicable legal rules. Related to this, the government and non-government as well as law enforcement and the public are also required to have high integrity in an effort to realize expediency, justice and legal certainty in an effort to fortify themselves from data misuse. In addition, the urgency of personal data protection can be seen by the protection of personal data as part of human rights regulated in Article 12 of the Universal Declaration of Human Rights (UDHR) which provides a legal basis for member states in terms of state obligations to protect and respect the personal rights of their respective citizens. In addition, in the International Convenant on Civil and Political Rights (ICCPR).

The existence of this Convention further authorizes each State to make legal instruments to protect its citizens. Thus, it is the obligation of the State that has ratified the Convention to implement it.

If a criminal event occurs or there is a report of a criminal act, the officer who receives the report immediately conducts an investigation to determine to what extent the truth of the event. The report can be done in writing which must be signed by the whistleblower and can also be submitted orally (Wulan Sari, 2015). Thus, if there is misuse of personal data that are both Indonesian citizens, it will be resolved through Indonesian law and carried out in courts in Indonesian jurisdiction.

Legal protection for misuse of personal data can be done through *self-regulation* or prevention efforts, if the current regulations have not reached the system of misuse of personal data. In fact, if traced to the comparative aspect, looking at the comparison with the State of Malaysia the regulation is regulated in the *Personal Data Protection Act* (PDPA) 2010, where this regulation aims to regulate the processing of personal data by data users in the context of commercial transactions, with the aim of safeguarding the interests of the data subject. Singapore is regulated through the *Personal Data Protection Act* (PDPA) 2012 and has a *Do Not Call (DNC) Registry*. Meanwhile, the protection of pivasi data and personal data in the European Union distinguishes between "sensitive" and "non-sensitive" data based on the level of danger that will be felt by individuals if they are accessed by irresponsible parties (Sautunnida, 2018).

According to the author, when referring to the provisions of Article 26 paragraph 2 of the Law on Information and Electronic Transactions as mentioned above, the basic problem is that criminal provisions have not appeared or have not been regulated, therefore it is very necessary to reformulate the norm by adding criminal sanctions, this is in order to cause a deterrent effect even though the criminal sanctions are an ultimate remedium.

The ITE Law has regulated data protection including wiretapping, where wiretapping is an action that should not be done excluding groups who have the right to it in the framework of legal remedies. When viewed from the explanation, Article 26 of the ITE Law has a weakness, namely the absence of legal protection for the owner of data used by the operator or service provider with the aim of making a profit. The Law on Electronic Information and Transactions only alludes to the subject of personal data protection (general provisions) without following up on the implementation of such protection.

This weakness is that criminal provisions have not been accommodated is something that must be improved in order to realize the objectives of the law, namely the maintenance and guarantee of order (certainty) and order, therefore it is necessary to reformulate existing legal norms. Through the provisions of Article 28J paragraph (2) of the 1945 Constitution and the Supreme Court Decision through decisions No. 6 / PUU-VIII / 2010 and Number 006 / PUU-I / 2003 which expressed his views regarding privacy protection must be protected by the state. However, in terms of legal interests, such rights can be reduced provided through the mechanisms stipulated in the Law.

2) **Law Enforcement against Perpetrators of Criminal Acts in Illegal Online Loan Transactions as a form of cybercrime in the Indonesian Criminal Law system.**

In some literature, *cybercrime* is generally considered a *computer crime. The U.S. Department of Justice* defines computer crime as: "... *any illegal act requiring knowledge of computer technology for its perpe-tration, investigation, or prosecution". The Organization of European Community Development* shares another definition, namely: "*any illegal, un-ethical or unauthorized behavior relating to the automatic processing and/or the transmission of data*". Hamzah defines it as "a crime in the field (*computer* network system) can universally be referred to as illegal use of a PC".

From the above interpretation, Wisnubroto defines PC crime as an unlawful act that is tried by using a PC like PC facilities / equipment like an object, whether to gain profit or not, by harming other parties. In short, computer crime is defined as illegal acts committed using complex computer technology. In addition, since crimes are committed in cyberspace through the internet, the term cybercrime has emerged. For most citizens who are accustomed to using communication technology media, cybercrime is not a foreign name.

The face of crime has also been refined in such a way, conventional crimes in the real world arise into the virtual world in a virtual way. In fact, *cybercrime* has caused so many victims and moral and material losses. Victims can be netizens (*cyberspace* residents) and the general public. But in developing countries with digital inequality such as Indonesia, it does not consider it a form of crime. Just like in real life, some are black and some are white, some play the role of heroes, and some are like villains. To understand *cybercrim*e, we also need to understand what is called *hackers, crackers* and others. Compared to conventional crime, *cybercrime* has unique characteristics:

1. Such illegal, rightsless or unethical acts occur in space or cyberspace, making it impossible to determine which country's legal jurisdiction applies to such acts.
2. The act is done using any (device) that can connect to the internet.
3. The material as well as non-material harm caused by these acts is often greater than traditional crimes.
4. The culprit is a person who can master the use of the internet and its applications.
5. These actions are often carried out transnationally.

Although there is still controversy, it can be said that Indonesia is a country with a considerable digital divide. The digital divide can be explained as the gap between those who can use communication technology and those who cannot. In addition to the gap in education and economic levels in Indonesia, access to Indonesian communication technology is also uneven. Inequality, lack of information and telecommunications can be divided into several categories. Of course, the most visited is the closest to the community information center (community).

The Indonesian legal system does not specifically control cyber law, but several laws have regulated the prevention of cybercrime, such as Law No. 36 on 1999 on Telecommunications, Law No. 19 of 2002 on Copyright, Law No. 15 of 2003 on Combating Terrorism, and Law No. 11 of 2008 on Electronic Information and Transactions. These laws and regulations have criminalized this type. *cybercrime* and the threat of punishment for each violator (Tanthawi, 2014).

Based on the content of the article, it can be concluded that personal data protection is a right or privacy rights owned by every individual and must be protected by the state and in *privacy rights* all individuals have the right to store and keep confidential things that are considered private for each individual. However, the right to privacy can become a matter of public law if perpetrators or corporations misuse personal data. As an effort to resolve through litigation, the author can analyze using the related regulations below:

Table 1 Law on Protection of Misuse of Personal Data

No	Related regulations	Article Substance	Threat of Criminal Sanctions
1	Article 27 paragraph 3 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions	Any Person intentionally and without rights distributes and/or transmits and/or makes accessible Electronic information and/or Electronic Documents that contain defamation and/or defamation	Imprisonment for a maximum of 6 (six) years and/or a maximum fine of Rp.1,000,000,000.00 (one billion rupiah)"
2	Article 369 of the Criminal Code	Whoever with intent to benefit himself or another unlawfully, by threat of defamation either orally or in writing, or by threat of revealing secrets, compels any person to give away anything wholly or partly belonging to that person or others, or to make a debt or write off a receivable, shall be punished with imprisonment for not more than four years.	Maximum imprisonment of 4 (four) years
3	Article 378 of the Criminal Code	Whoever with intent to benefit himself or others unlawfully, by using a false name or false dignity, by deceit, or by a series of lies, moves another person to deliver something to him, or to give a debt or write off a receivable shall be threatened with fraud.	The maximum penalty is imprisonment of 4 (four) years.

Based on the table above, the author can conclude that victims of data misuse in online loans can take legal action using one of the articles above. Before proceeding to the legal route, it must first be analyzed whether it is in accordance with the elements listed in each article.

The problem of data misuse in the implementation of online loans whose elements are included in defamation as stipulated in Article 27 paragraph 3 of Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions will be sanctioned with rules separate from the article. The sanction of the article is in the criminal provisions section, especially article 45 which reads:

"Any person who fulfills the elements as referred to in Article 27 paragraph 1, paragraph 2, paragraph 3, paragraph 4, shall be sentenced to a maximum imprisonment of 6 (six) years and/or a maximum fine of Rp. 1,000,000,000.00 (one billion rupiah)". Article 45 of Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions of the State Gazette of the Republic of Indonesia of 2016 Number 251, Supplement to the State Gazette of the Republic of Indonesia.

The purpose of the article is for a person who commits a criminal offense that meets the elements of article 27 paragraph 1, paragraph 2, paragraph 3, paragraph 4 will be subject to imprisonment and/or fines. Perpetrators will get sanctions between only in the form of imprisonment or imprisonment and fines with the provisions stipulated in the article.

The criminal act of misuse of personal data in online loans can also be punished with Article 369 of the Criminal Code which reads "Whoever with the intention to benefit himself or others unlawfully, by threats of defamation either orally or in writing, or by threats of revealing secrets, forces someone to give something that wholly or partly belongs to that person or others, or to make debts or write off receivables, punishable by imprisonment for not more than four years."

Article 369 of Law Number 1 of 1946 concerning the Regulation of Criminal Law State Gazette Number 127 Supplement to the State Gazette of the Republic of Indonesia Number 1660. The article can apply to criminal acts where if someone receives money from an online loan even though the person does not make a money loan in any online loan application and must return the money along with interest. There are elements of threats of pollution both verbally and in writing, or with threats of revealing secrets are things done by *debt-collectors* from online loan operators.

Another case of misuse of personal data in online loans is biased in the form of if someone uses someone else's personal data to make an online loan and the person who uses his personal data is asked to pay the money borrowed without receiving money from the online loan, then the person who uses the online loan can be punished with Article 378 of the Criminal Code which reads "whoever with the intention to benefit themselves or others unlawfully, by using a false name or false dignity, by deceit, or by a series of lies, to induce another person to deliver any thing to him, or to give a debt or write off a receivable shall be punished with fraud with imprisonment for not more than four years." Article 378 of Law Number 1 of 1946 concerning the Regulation of Criminal Law State Gazette Number 127 Supplement to the State Gazette of the Republic of Indonesia Number 1660. In the article there are elements that match the misuse of personal data such as by using a false name or false dignity here intended for someone who uses someone else's ID card to apply for a loan to an online loan application.

Discussion of future criminal law developments, *cybercrime* resolution and prevention should be balanced with regulation and development through the theory of the criminal law system, which includes the development of the structure, culture, and substance of criminal law. Under such conditions, criminal law policy occupies a strategic position in the development of modern criminal law. The criminal law policy intends to achieve peace and well-being of all people.

B. Legal Illegal Online Loan Liability (*Illegal Fintech Desk Collector*) in Criminal Law Perspective

This online loan was started by a *Financial Technology* company or better known as *fintec*h. Thus, many financial institutions including banks began to arise that tried to integrate operational systems with information technology that developed through smartphones or computers connected to the internet. Therefore, bank online loan credit services began to flourish in Indonesia. Therefore, online loans are product services in the form of loan loans that use information technology facilities. The services provided start from the process of applying for loan funds, *acceptance*, to disbursing online loan funds via email, sms, and telephone. It can be seen from the explanation above, many creditors and debtors do not meet face to face at all.

Different when compared to conventional loans are as follows:

a. The owner of the fund benefits from the interest set in addition to the customer;
b. Conventional banks pursue profit only;
c. The relationship established by the customer with the person who lent the funds is only limited to the customer and creditor and has no emotional bond;
d. If there is a dispute or dispute involving a conventional bank, the path taken is the legal route with the district court as the party to the dispute resolution.

According to the author, the intention in this study is the criminal liability of online loan actors which has criminal implications for the concept of Responsibility is a rule on how to treat

anyone who violates the norms, morals, religion, and laws that exist in the community (Chairul Huda, 2015).

The concept of criminal responsibility basically returns to the understanding of punishment of criminal offenders. According to Hart, the concepts of crime and criminal responsibility are very different, it can be seen from the existence of different regulatory structures. Hart suggests that "*primary laws setting standards for behavior and secondary laws specifying what officials must or may do when they are broken*". It can be seen, then, that there is a separation between primary legal rules that contain rules about behavior, and secondary legal rules that determine what should or may be done for those who violate these rules. Responsibility is defined by the relationship between the conditions that have become conditions and what legal consequences have been required (Morison, 1960).

The ability to be responsible, can be seen in the factor of reason, namely whether the perpetrator distinguishes between actions that are allowed and those that are not. In addition, it is also seen from the factor of feelings or desires of the perpetrator, namely whether the perpetrator can adjust behavior to his consciousness which is allowed or not (Morison, 1960). So a perpetrator who commits a criminal act even though legally and convincingly proven to have committed a criminal offence, will not be criminalized, because his soul is disabled in growth, or impaired due to a disease. This means that a person can be held accountable for his actions if:

a. The ability of the maker to think that allows him to master his mind, which allows him to determine his actions;
b. Therefore, he can understand the meaning and effect of his actions;
c. And therefore, he can determine his will according to his opinion (Abidin, 1987).

For criminal offenders who are mentally handicapped in growth or impaired due to an illness, the examining judge may request in his ruling that the offender be admitted to a mental hospital. **Sudarto** explained that, in order for a person to have aspects of criminal responsibility, in the sense of being convicted of a maker, there are several conditions that must be met, namely (Pohan, Santoso, &; Moerings, 2012)

1. There is a criminal act committed by the maker;
2. There is an element of error in the form of intentionality or negligence;
3. The existence of makers who are able to be responsible;
4. There is no forgiving reason.

Regarding the position as a maker and the nature of corporate criminal liability, there are corporate liability models as follows:

a. The management of the corporation as the maker and manager is responsible;
b. The corporation as maker and manager is responsible; and
c. Corporations as makers and also as responsible (Priyatno, 2017).

Criminal liability in corporations should not be charged using articles regulated in the Criminal Code because between criminal acts committed by humans and criminal acts committed by corporations have different characteristics (Ali, 2013). When discussing criminal liability, it will never be separated from the principle of criminal liability, namely "*keine strafe ohne schuld or geen straf zonder schuld or nulla poena sine culpa or actus non facit reum nisi mens rea*" (Moeljatno, 2002). Which if interpreted into Indonesian is the same as "no crime without fault" regarding participation and assistance in criminal acts (Moeljatno, 2002).

According to the Criminal Code, the subject of the Criminal Law is an individual, because in the Criminal Code there is nothing that can ensnare about corporations (legal entities that commit criminal acts). This can be seen in Article 59 of the Criminal Code which explains that the subject of law is a natural person who can commit a criminal act. According to Moeljatno, the following is the sound of Article 59 of the Criminal Code, namely:

"In cases where because the offense is determined to be criminal against the management of the members of the governing body or commissioners, the management, members of the governing body or commissioners who apparently did not interfere in the violation are not criminalized".

According to the provisions of the above Article, the description of the management of the members of the governing body or commissioners can be likened to the chairman and members and others. While the view of the Criminal Code that the subject of law is a natural human being who can solely be the subject of the criminal law, there is a thought based on that only humans have mens rea an other living things or corporations, namely bodies created by humans through law, which are considered to have no mens real (Edi Yunara, 2018).

1. Prohibited Acts in Online Loans

Before entering into prohibited acts in online loans, we must first know what a criminal act or criminal act is. In the Criminal Law (KUHP) the crime is better known as "*Strafbaar Feit*". In this "*Strafbaar Feit*", Moeljatno interprets the term criminal act as "an act prohibited by a rule of law, a prohibition which is accompanied by a threat (sanction) in the form of a certain crime for anyone who violates the prohibition" (Moeljatno, 2002).

Based on this opinion, it can be concluded that the definition of a criminal act is an act that violates a rule of law, which can be subject to criminal sanctions for anyone who violates the rule aimed at the act, while the threat or sanction can be directed at the person who committed the crime. In addition, criminal acts are prohibited in a law and have sanctions if committed.

2. **Problems and forms of legal responsibility that arise due to illegal online loans**.

a. **Criminal Fraud**

Article 378 of the Criminal Code if it is related to the current online loan case where the fraud lies is that if we borrow money of Rp. 1,000,000, - then what we get in the account is Rp. 600,000, - the agreement is not mentioned elas why the loan that was originally Rp. 1,000,000, - became Rp. 600,000, - .

The loan party only explains the deduction of administrative fees. So what is meant by fraud is that the loan given is not appropriate and many deductions are not mentioned in detail.

The approach to the case explains that the debtor has suffered a loss and there has been an element of fraud on the part of the creditor that is not in accordance with the proper agreement. This fraud offense is aimed at fintech applications that provide loans to customers that are not in accordance with the initial agreement / many deductions that are not explained to customers who borrow. So, customers who borrow the money only find out through the money that enters their account number. Creditors when the debtor does not return money in accordance with the agreed maturity limit, will be charged interest in accordance with the initial agreement.

b. **Extortion**

The provisions of Article 365 paragraphs (2), (3), and (4) apply to this crime.

Part of the element of offense in the Article, namely: (Hamzah, 2015)

1) With intent to benefit oneself or others;
2) Unlawfully;
3) Coercing someone by force or threat of violence;
4) To give away any thing, which wholly or partly belongs to that person or others, or to create a debt or write off any receivable.

In the offense of extortion and fraud is the offense of property of goods handed over in the form of intangible goods, namely debts or write-offs of receivables. If in the offense of theft, the goods taken cannot be in the form of debt relief. Debt write-off, for example, by force, someone signs a receipt in full, but he has not paid it (Hamzah, 2015).

c. Criminal Threat

This method of threatening, that is, will blaspheme or will reveal secrets to other people or the public related to the private life of the person threatened or a third person in relationship with the person threatened.

The difference is that a secret is essentially about something that really happened, but blasphemy that tells the truth or not is hidden because of certain things, while the defamation is the name and honor of the person threatened or the third person, who has a family relationship or friendship with the person threatened (Prodjodikoro, 2012) . If the secret

concerned is not only related to himself but also about what the person threatened with wanting should not be known by many people. So this is different, meaning that the secret is intended in Article 322 of the Criminal Code, which is about the disclosure of secrets by people who, because of their position or work, are obliged to keep the secret (Prodjodikoro, 2012).

d. **Criminal Breach of Privacy**

Misuse of ID card privacy that occurs in online loans has violated laws and regulations. Article 85 of the Population Administration Law, in addition to Article 17 letter (h) of Law Number 14 of 2008 which states that public information that is exempt from must be disclosed, namely: history and condition of family members, history of conditions and treatments, treatment of a person's physical and psychological health, financial condition, assets, income, and one's bank account, results of evaluations in relation to capabilities, intellect, and recommendations of one's abilities, and/or records concerning one's person relating to the activities of formal education units and non-formal education units.

e. Criminal Offences of Contempt

A criminal sanction (*punishment*), can be defined as a sorrow or suffering inflicted on people who have committed acts prohibited by criminal law (Ali, 2013). Liability for debtors who fail to pay off their debts is that the debtor still has to pay off the debt because it has made an agreement and has received the loan money. However, if the debtor does not have good faith, it can be subject to Article 378 of the Criminal Code on Fraud for violating existing agreements and can be threatened with a maximum prison sentence of 4 (four) years.

The criminal threat of raising funds without permission is very severe, and there is no substitute for a monetary fine if the fine cannot be met (*subside*) is not in the law which shows how severe the penalty is. The rise of cases in the field of online loans under the guise of investment has harmed the community a lot. The term is better known as raising funds. The criminals who raise these funds lend money on easy terms and provide very large interest so that creditors can benefit from the interest proceeds.

The easy and fast unconditional loan of money appears to deceive the public to existing suicides. However, interest rates are getting higher every day and often people who raise public funds seduce through advertisements or sending SMS to customers. In the event of fraud committed by the debtor (borrower), it can be subject to Article 378 of the Criminal Code, then it is threatened with a maximum prison sentence of 4 (four) years. In investors who commit the crime of extortion and can be charged with Article 368 of the Criminal Code, they are threatened with a maximum prison sentence of 9 (nine) years and related to threats with Article 369 of the Criminal Code, they are threatened with a maximum prison sentence of 4 (four) years.

Meanwhile, in the ITE Law, sanctions against fraudsters are not specifically regulated regarding fraud. So far, the crime of fraud is only regulated in Article 378 of the Criminal Code which can be threatened with a maximum of 4 (four) years imprisonment. Although the ITE Law does not specifically regulate fraud, it is related to consumer losses incurred in transactions. In the ITE Law, regarding sanctions against perpetrators who commit extortion crimes and threats carried out through online media are regulated in Article 29 of the ITE Law which reads "Everyone intentionally and without rights sends Electronic Information and/or Electronic Documents containing threats of violence or scare shown personally".

In accordance with the provisions of Article 45 paragraph (3), violations of Article 29 of the ITE Law are punishable by imprisonment for a maximum of 12 (twelve) years and/or a fine of 2 (two) billion rupiah. So, through the formulations of Article 368 and Article 369 of the Criminal Code when compared with Article 29 of the ITE Law, we can know that the two rules regulate different things. Article 368 and Article 369 of the Criminal Code regulate extortion and threats, while Article 29 of the ITE Law regulates extortion and threats through internet media or other electronic media whose perpetrators threaten either sexual or security against others so as to cause fear of victims

In the end, it is very necessary for police investigators to determine when to use Article 368 of the Criminal Code and when to also use the provisions in Article 29 of the ITE Law.

However, if in practice, the police can be charged with layered articles if the crime meets the elements of extortion and threats as stipulated in Article 368 and Article 369 of the Criminal Code and meets the elements in Article 29 of the ITE Law. Then these elements are fulfilled and the police can use the article. The ITE Law related to Article 29 jo. Article 45 paragraph (3) can help the shortcomings in the Criminal Code even though the ITE Law does not specifically regulate the provisions on the crime of extortion and threats, but the article can be used to sanction perpetrators in accounting for their crimes.

The perpetrators in this online loan crime are corporations, but in corporations there are not only legal entities or legal persons but also persons (humans) or natural persons. Because in online loans many establish their businesses in the form of legal entities and people (natural person). The phenomenon of debt collection by illegal online loan desk collectors almost occurs in all cities in Indonesia and the impact of desk collectors' actions can be felt both psychologically and physically and there are even some victims who are frustrated and end their lives, so that victims have the right to obtain legal protection as described in Law Number 13 of 2006 as amended by Law Number 31 of 2014 concerning Witness Protection and Victims (hereinafter referred to as the Law on Sex Workers) which according to researchers deserves to be accommodated as an effort to protect victims of illegal online loans.

It is clear that protection for victims is not only if the perpetrators of crimes have been convicted and processed but must also be fulfilled the rights of victims as justice-seeking parties such as obtaining restoration of good name (rehabilitation), provision of compensation (restitution, compensation, social welfare guarantees/compensation), and so on. It is appropriate for law enforcement officials to provide appropriate sanctions for perpetrators (desk collectors and company administrators) and provide protection for victims for billing carried out by illegal fintech desk collectors so that the rule of law is truly enforced and order is created in society. Based on the background as described, the problem to be studied is how the form of criminal liability that should be applied to illegal fintech desk collectors and how to protect victims of illegal fintech desk collectors.

CONCLUSION

Law Enforcement: Misuse of Personal Data Related to Online Loans (Illegal Fintech) as a Form of Mayantara Crime in a Cyber Perspective Based on the reason that the rise of public activities on electronic media, the Electronic Transaction Information Law was born, namely Law Number 19 of 2016 on Law Number 11 of 2008 concerning Electronic Information and Transactions on Electronic Information and Transactions (ITE) with considerations can be found in part of the consideration, especially in the "Weighing" section which states that information globalization has placed Indonesia as part of the world information society so that it requires the establishment of regulations regarding the management of Electronic Information and Transactions at the national level so that the development of Information Technology can be carried out optimally, evenly, and spread to all levels of society in order to educate the nation's life. Based on the complexity of the problem above, law enforcement of misuse of personal data related to illegal online loans as a form of crime in a cyber perspective can be reviewed from 2 (two) main aspects: 1) Policy on the Discontinuation of Personal Data Storage in Electronic Media. 2) Law Enforcement against Perpetrators of Criminal Acts in Illegal Online Loan Transactions as a form of cybercrime in the Indonesian Criminal Law system.

Liability for Legal Illegal Online Loans (Illegal Fintech Desk Collector) in the Perspective of Criminal Law starts from the emergence of various kinds of criminal acts in online loans, due to the motive of someone who wants to benefit in unlawful ways, because they use the opportunity not to meet between the debtor and creditor. The provisions that can be imposed are Article 378 on fraud, Article 368 and Article 369 of the Criminal Code on extortion and threats, Article 29 jo. Article 45 paragraph (3) of the ITE Law. Criminal liability through online loans for debtors who fail to pay must still pay off their debts and if there is no good faith, they are charged with Article 378 of the Criminal Code, and creditors can be subject to Article 368 of the Criminal Code and

Article 369 of the Criminal Code concerning extortion and threats, Article 29 jo. Article 45 paragraph (3) of the ITE Law. Not only involving individual actors but also corporations. Although corporations are subjects of law, the punishment is still imposed by individuals or directed directly at perpetrators who violate the law.

REFERENCES

Abidin, Andi Zainal. (1987). *Principles of criminal law: part one*. Publisher Alumi.

Agang, Mohammad Ilham. (2015). Human Rights in the Development of the Rule of Law. *Humanitas: Journal of Human Rights Studies and Education*, *6*(1), 116–135.

Ahmadi, Candra, &; Hermawan, Dadang. (2013). E-business &; e-commerce. *Yogyakarta: Andi*.

Ali, Mahrus. (2013). *Principles of corporate criminal law*. PT RajaGrafindo Persada.

Chairul Huda, S. H. (2015). From 'No *Criminal Without Fault', to 'No Criminal Responsibility Without Fault'*. Gold.

Edi Yunara, S. H. (2018). *Corruption and Corporate Criminal Liability*. PT Citra Aditya Bakti.

Fitri, Sherly Nelsa. (2022). Legal Politics of the Establishment of Cyber Law on Information and Electronic Transactions Law in Indonesia. Journal of *Justisia: Journal of Law, Legislation and Social Institutions, 7*(1), 104–124.

Hamzah, Andi. (2015). *Certain delicts (Speciale Delicten) in the Criminal Code*. Ray Grafika.

Moeljatno, S. H. (2002). Principles of Criminal Law. *Rineka Cipta, Jakarta*.

Morison, W. (1960). *Ross: On Law and Justice*.

Nurhadi. (2022). Here Are 7 Cases of Alleged Personal Data Leaks Throughout 2022. *Tempo.Co*. Retrieved from https://nasional.tempo.co/read/1632043/inilah-7-kasus-dugaan-kebocoran-data-pribadi-sepanjang-2022

Pohan, Augustine, Santoso, Topo, &; Moerings, Martin. (2012). Criminal law in perspective. *Bali: Larasan Library*.

Priyatno, H. Dwidja. (2017). *Corporate criminal liability systems: in legislation policy*. Pretone Media.

Prodjodikoro, Wirjono. (2012). Certain Crimes in Indonesia, ed. 3 cet. 4. *Refika Aditama, Bandung, 1*.

Sautunnida, Lia. (2018). The Urgency of Personal Data Protection Law in Indonesia: A Comparative Study of UK and Malaysian Law. *Canon Journal of Legal Sciences*, *20*(2), 369–384.

Tanthawi, Dahlan. (2014). PROTECTION OF VICTIMS OF CYBER CRIME IN THE INDONESIAN CRIMINAL LAW SYSTEM. *Journal of Legal Sciences*, *2*(1).

Triansyah, Abdurrazaq, Julianti, Putri Nur Siti, Fakhriyah, Nadyva, &; Afif, Andi M. (2022). The Role of the Financial Services Authority in Legal Protection for Illegal Online Loan Users (Case Study of Illegal Loans in Yogyakarta). *Cross-Border*, *5*(2), 1090–1104.

Wulan Sari, Febilita. (2015). *Legal Protection of Customer Personal Data in the Provision of Internet Banking Services Connected with Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking*.

Journal of Social Science