CYBER CRIME AND *PRIVACY RIGHT* VIOLATION CASES OF ONLINE LOANS IN INDONESIA

Fitri Maghfirah[1], Fathayatul Husna[2]

[1]*Universitas Islam Kebangsaan Indonesia (UNIKI),*
[2]*STISIP Al-Washliyah Banda Aceh,*
E-mail Kontributor: fitrie.maghfirah@gmail.com

Abstract

This article examines the phenomenon of illegal online loans in Indonesia and the government's preventive policies to deal with it. This article will be studied using a qualitative descriptive approach and using content analysis methods and literature review. In this article, the author argues that cybercrime does not only discuss online data theft or acts of harassment, but also relates to online loan crimes . The author also argues that the development of online loan crime is due to weak government regulations and policies. The government has tried to formulate legal regulations regarding the establishment of online loans legal and also legal rules that will protect victims of online loan crimes. However, in practice it still needs to be studied seriously and in depth. Many online loan crime cases are found in Indonesia, even during this pandemic it was reported that many online loan crimes were felt by the public. Therefore, through this online loan crime , the author wants to explore and examine more deeply about why online loan crimes are increasingly occurring among the public. How is the government trying to protect victims of online loan crimes by implementing the Financial Services Authority (POJK) Regulations, the Electronic Information and Transaction Law and other regulations? Also, how does the discussion of online loan crimes relate to human rights and privacy rights ?

Keywords: Cybercrime, online loans, POJK, UU ITE

A. INTRODUCTION

Along with the development of sophistication of technology and information, crime in cyberspace is not a new event in this decade, because in historical records it has been stated that crimes with this model have occurred since 1960 in America (Sejarah Cyber Crime, Https://Danrayusuma.Weebly.Com/Sejarah-Cybercrime. Html). Criminal acts in cyberspace use different methods from traditional criminal methods, among the violations in cyberspace that often occur are identity theft, *property crime* , fraud, and so on (Sara Norden, Thesis: *How The Internet Has Changed The Face Of Crime*).

Regarding the use of equivalent words to represent criminal acts in cyberspace, some call it *cybercrime* and *virtual criminology* (Sara Norden, Thesis:

How The Internet Has Changed The Face Of Crime). In this article the author chooses to use the term *cybercrime* in describing criminal acts in cyberspace. *Cybercrime* is all illegal activities carried out by criminals using computer network information system technology, and directly attacking the information system technology of the victim. But in a broader perspective, *cyber* crime can also be interpreted as any illegal act that is supported by computer technology.

As is the issue that is currently being discussed in 2021, where as new technology develops and the high use of the internet during the COVID-19 pandemic, along with the high rate of crime that occurs in cyberspace. As people are close to various technological systems in cyberspace during the COVID-19 pandemic, the crime rate is getting more intense. Based on the information the author quoted from International news, the German Federal Criminal Police (BKA) reported that the number of acts of cybercrime in 2020 (during the covid-19 pandemic) increased by 8% from previous years (Republika.co.id, 14 May 2021). In line with that, in a study it was stated that criminal acts that occur in cyberspace, the movement is very fast, and in tandem with the faster adaptation of society to the internet and economic digitization (Richard Apau & Felix Nti Koranteng, 2019). Kimberly in his research also states that, the increasing number of crime through computers (*cybercrime*), is an implication of the development of the popularity of social media and the growth of e-commerce (Kimberly Pavlik, 2017).

In the case of *cybercrime* that occurred in Indonesia, several things that became the center of attention were criminal acts in violation of rules related to P2P landing as stipulated in the POJK, the Information and Electronic Transactions Law (UU ITE), human rights and *privacy rights.* As *cybercrime* acts developed, various related regulations such as laws, government policies, and other regulations will control the supervision of these criminal acts (Kimberly Pavlik, 2017).

Based on data from the Financial Services Authority, from 2013 to June 2021, the number of legal online loan customers has reached 64 million customers, with the amount of funds already borrowed reaching Rp 221 trillion (Kompas.com, 21 Oktober 2021). It is undeniable that public interest is very high in accessing online loans, as reported by the Financial Services Authority, where online lending through P2P lending financial technology in 2021 (until September 2021) reaches Rp 24.48 trillion, this figure represents an increase in public access to online lending with an increase of 116.2% from the previous year (Tempo.Co, 27 Oktober 2021).

The increase in the number of legal online loan disbursements, as described above, is a signal that the high need for people to access loans can be caused by the weakening economy. Inevitably, the weakening economy in society has implications for making it easier for illegal online lenders to recruit customers. As according to a compass report that, the number of complaints of various cases of illegal online loans to the Financial Services Authority in Tegal rose 100% from the previous year (Kompas.com, 21 Oktober 2021). From the report, it is clear that the increase in public reports or complaints against illegal online lending practices and the criminal acts that accompany it, represents an increasing number of customers joining illegal online lending practices.

Various actions that become the mode of illegal online loan actors include, *first,* online loan offers can appear via SMS or WhatsApp from an unknown

number, which then the perpetrator claims about applying for a loan without any conditions. Meanwhile, when viewed from a legal legal perspective, there are no rules that allow *leading fintechs* to submit loan offer information through personal communication facilities without user consent; *second,* replicating names that are similar to legitimate *fintech lending* to trick victims *; third,* tricking the victim by directly transferring a sum of money, even though the victim has never applied for a loan to the illegal online loan, so that later the perpetrator will terrorize the victim with the debt bill along with the fine if it has exceeded the time period (Virdita Ratriani, 23 Oktober 2021). The illegal actions taken by the online lender are very disturbing to the public, because many victims have been tricked and deprived of their personal security rights and *privacy rights* by illegal online lenders. Departing from these problems, the author is interested in systematically exploring, through various perspectives, the criminal acts of illegal online loans.

Research related to the topic of *cybercrime* has been widely carried out by previous researchers, some of which have been described by the author in the previous paragraphs. In line with that, Rodes and Yuliana have also researched the issue of protecting the rights of online loan service users from a human rights perspective . However, the regulation on *financial technology,* in this case related to the movement of online loans, is still very weak, because there are no clear sanctions against the organizers of illegal online loans (*Rodes Ober Adi Guna Pardosi, Yuliana Primawardani,* 2020). Different from several previous studies that the authors have described previously, this research was conducted using a content analysis method based on the latest phenomena related to *cybercrime* issues , which were then mixed in several legal aspects, accompanied by a description of the *cybercrime* movement from the point of view of human rights or *privacy rights.*

This research is a qualitative research with data collection method based on content analysis from various previous studies and information obtained through virtual observation. This study focuses on several topics of discussion, namely about the *cybercrime* movement in general, as well as how cases are a real manifestation of *cybercrime* actions and human rights violations in the form of *privacy rights* . In this context, what the author focuses on is related to the criminal acts of illegal online loan actors and the impact of the violations felt by the victims. Departing from the problems and *cybercrime* actions carried out by illegal online loan actors, then the author also reviews how the legal rule for these *cybercrime* actions is *,* as well as the actions taken by the authorities in protecting victims of illegal online loans (pinjol). Some interesting perspectives to discuss related to *problem solving* of these criminal acts, including; *first,* from the point of view of normative law and its application, such as the Financial Services Authority Regulation, the Information and Electronic Transaction Law, and other regulations relating to the protection of personal data in protecting victims, and minimizing *cybercrime* actions ; *second,* relating to *cybercrime* from the point of view of human rights and *privacy rights.*

B. DISCUSSION

a. Cybercrime Action Overview

In recent years, the development of cyberspace is increasingly visible from

various regional points. This development can be felt by everyone in all parts of the world. Starting from the birth of technology and growing and evolving with the times, technology has not only emerged as a tool, but also a message (Akhmad Yani Surachman, 2021: 72). Technology evolves from hand to hand with different nuances in each generation. For example, in the 90s, technology was still in the form of cable connections, while in the 2000s, humans were slowly able to communicate wirelessly. Entering the era of 2010 to 2020, the internet began to develop, although it was not yet spelled out optimally. However, at that time, *Black Berry* products and *smartphones* were widely circulated . In that era, the competition for the latest technology products and the support of a wide internet network service began to be seen (Steven Millward, 2014).

Internet is the only concern in today's era. Every activity from various sectors is slowly starting to involve the internet as part of the job assistance. Initially the internet was indeed used to facilitate work, but with the widespread use of this network, any type of work must follow a virtual system. This enforcement certainly gave birth to pros and cons from various circles. Those who agree will say that the internet greatly facilitates every activity to be carried out. While the cons will say that the internet will only add more burden, because humans are used to manual performance. Regardless of the pros and cons of various groups, an important reason to consider using the internet is data security. Security systems are not only needed in everyday life in the real world, but are needed to protect activities in cyberspace.

Regarding security systems in cyberspace, lately this issue has become a hot topic of discussion. This security system is closely related to the problem of violence in cyberspace or known as *cyber crime* (cyber violence). Cyber violence is usually attached to cases of data theft. In fact, this form of violence is not only related to data theft, but even many other types of cases that harm users. *Cyber crime is* actually against the rule of law. The criminal process is carried out using advice/tools that are widely connected to the internet network and aim to harm others (Dista Amalia Arifa, 2011: 187). The perpetrators of these crimes are usually known as *hackers.* The stigma attached to the term *hacker* has been interpreted as a negative figure. *Hackers are* also known as smart people who are very well versed in the field of informatics and networking. He can hack various applications that are connected in cyberspace with the knowledge he has and the vision and mission he wants to achieve (Dista Amalia Arifa, 2011: 188). However, at first the term *hacker* attached to the nickname of someone who is very skilled in the field of computers and has a curiosity to explore computer operating systems. Therefore, this activity has the potential to encourage perpetrators to carry out their actions in a negative way.

The activities of *hackers* or cybercriminals usually use *tools* or software to attack computer operating systems. Usually the targets of *hackers* are credit card *databases* , bank accounts, and customer information databases (Dista Amalia Arifa, 2011: 188). In addition, *hackers* also carry out their actions to disrupt the system through *Internet Relay Chat* (IRC), *Voice Over IP* (VoIP), *Online Forums* and *Encryption* (Dista Amalia Arifa, 2011: 188). Several stages carried out by *hackers* to hack computer systems are *footprinting, enumeration, gaining access, escalating privilege, pilfering, covering tracks, creating backdoors* and *denial of service* (Thomas HA Gregory, 2005).

Footprinting is known as the most common way of searching for information. Usually the perpetrators do the practice of *scanning. Enumeration is* almost the same as *gaining access in* that both look for valid user accounts and try to steal *passwords. Escalating privilege* and *pilfering* is the stage of exploitation after the *password* has been found. *covering tracks are* carried out to control and cover priorities. At the stage of using *hide tools* to secure the exploits. *Creating backdoors is* done by creating fake accounts and running applications that have been successfully planted on the victim's account and controlled remotely. Then, if some of the steps above are not successful, the *hacker* will run an *edenial of service,* namely trying to attack the victim's computer system using *SYN flood, supernuke, trinoo* and so on.

Based on the several stages above, it can be seen that the perpetrators of cybercrime understand the science of informatics networks, computer operating systems and also control the course of community activities in cyberspace. Crimes committed by *hackers* may not benefit him and also not harm him. However, this is done on the basis of fulfillment of pleasure. However, this action is clearly against the law and violates the privacy rights of every community in cyberspace.

Not only interpreted as disruptors of computer operating systems/software networks, *hackers are* also divided into several types according to the activities carried out, such as *script kiddies, cyber-punks, hacktivists, thieves, virus writers, professionals* and *cyber-terrorists* (Machsun Rifauddin dan Arfin Nurma Halida, 2018: 101)*. Script kiddies are* usually nicknames given to *hackers* who are still shallow in their knowledge. He just carried out the action without knowing the goal to be achieved. He also only commits crimes with an adrenaline rush in him. So, this type of *hacker* will still be considered very childish. *Cyber-punks are* usually run by teenagers aged 12-18 years. They carry out their mission of *punk* mentality in cyberspace without respecting cyber ethics.

It doesn't stop there, other types of *hackers* such as *hacktivist are* almost similar to the meaning of the term *buzzer.* Usually this type of *hacker* will hide their identity in cyberspace to take revenge on other parties. Unlike *thieves* and *virus writers.* Both act to defraud some of the victim's data and create a virus that will disrupt the target's computer operating system. In addition, *professionals* are an elite group of *hackers* who offer their services according to their scientific capacity. Usually they will carry out their criminal actions as a job with the highest price offer. While *cyber-terrorists are* usually part of a country's defense that carries out their actions by attacking the protection and defense of enemies in cyberspace and protecting their own systems (Machsun Rifauddin dan Arfin Nurma Halida, 2018: 101). Of these several types of *hackers* , all of them can be classified as cybercrimes, whether they are classified as light or serious. The resulting effects will be very detrimental to the target and will get the benefits they expect.

Regarding *cyber crime,* Emile Durkheim has previously proposed anomie theory to describe the situation of de-regulation (Hardianto Djanggih dan Nurul Qamar, 2018: 13). Anomie theory is a part of criminological theory to study the causes of someone committing crimes in their social sphere. De-regulation is defined as an act of violating the applicable rules, values and norms. Someone will feel they have the right to live freely without any rules that bind him. Although classified as a classic

theory, anomie theory is often used by a number of academics to study the phenomenon of cyber crime today. Through the perspective of anomie theory, academics such as Hardianto Djanggih and Nurul Qamar explained that cybercriminals actually know that there are special protections for cyber users. However, perpetrators often ignore this form of protection. Thus, the perpetrators can be said to have ignored the norms and emerged as the seeds of cyber criminals. In addition, they assume that no one party can interfere with someone's activities in cyberspace. According to him, cyberspace is a space of freedom and freedom to do anything, whether it is related to positive or negative behavior (Hardianto Djanggih dan Nurul Qamar, 2018: 13). Therefore, the author sees that this anomie theory is appropriate to be used to study and explain the issue of cyber crime from the perspective of the perpetrator.

Through the form of neglect believed by the perpetrators, cybercrimes can drain the personal data of account users in every country. Practices are also carried out in different ways and modes. Some types of cybercrime are *online* fraud *, phishing, malware, email* bombs *,* social media *hacking and spamming ,* hacking, *cyber bullying, cyber stalking,* and *ransomware* (Ani Mardatila, 2020)*. Online* scams are run with a strategy of displaying *pop up* ads that will notify the victim that the victim is the winner of a lottery. Then, the victim will be asked to send a fraudulent *online* delivery transaction card also often referred to as *identity theft* . In fact, the victim does not get anything and financial transactions will soon be disrupted by the perpetrators. *Pishing is* usually done randomly by the perpetrator by sending a short message or telephone. The perpetrator will pretend to be a bank employee or the like and will offer certain services to the victim. Perpetrators will also pretend to act as parties who are aware of suspicious activity on the victim's device. So, the victim will follow the instructions of the perpetrator.

Not only that, *malware,* social media *spamming* and *email bombs* all three have almost similar specifications. *Malware* will usually flood the victim's device with various types of viruses, so that the perpetrator can steal credit card details and personal data information. Social media *spamming* is also done to send *spam* in bulk to the victim's account. While *the email bomb* , the perpetrator will flood the victim's email with short messages that have the potential to slow down server performance. This of course will drain the victim's hard work to fix it. In addition, *cyber stalking* and *cyber bullying have* also received special attention in recent years. both types of crime oppress victims by means of *online* harassment *.* Usually, the abuse that is committed is closely related to the life and routine of the victim. Perpetrators not only carry out their actions in text form, but also upload videos and pictures to offend the victim.

In addition to the several types of cyber crimes above, another type of crime that is currently circulating in the community is *online* loan crimes or abbreviated as 'pinjol'. *Online* loans are one of the financial services that are incorporated in *financial technology (fintech). Fintech is* known as a technology-based financial service with the advantage of facilitating financial transactions through technology, one of which is the ease of *online* lending (Istiqamah, 2019: 291)*.* However, *online* loan services do not always offer convenience to its users. this service also has an impact on increasing borrower protection and eroding borrower rights. Therefore, the discussion regarding *online* loans will be described in the next subsection in depth.

b. Cybercrime Actions : Illegal Online Loan Cases in Indonesia

Recently, *online* loans have received great attention among the public. At first, *online* loans came with the aim of facilitating *online* money lending transactions . *online* loans are incorporated in *financial technology* (*fintech*) services. This service provides a new face for the ease of processing convenience in financial transactions. With personal data and internet network assistance, loans can be made without having to go through a face-to-face process.

Regarding the *online* loan phenomenon , several academics such as Wening Novridasati, Ridwan and Allyth Prakarsa, Rodes Ober Adi Guna Pardosi and Yuliana Primawardani, and Rayyan Sugangga. Wening, Ridwan and Allyth explained that debt collection crimes committed by illegal online lending institutions are part of *cyber* crime (Wening Novridatasati, Ridwan, dan Allyth Prakarsa, 2020: 262). According to him, the crime may be subject to Article 27 Paragraph 1 of the ITE Law. He also said that the crime will greatly affect the victim's psychological and physical. Rodes and Yuliana explained that the protection obtained by victims of *online* borrowers has not been carried out optimally (Rodes Ober Adi Guna Pardosi dan Yuliana Primawardani, 2020: 353). Thus, it is necessary to draft an in-depth Financial Technology Act to handle cases of illegal *online* loans . Rayyan Sugangga explained that the current focus is not only on legal and illegal *online* loans , but rather on policies on preventive measures by conducting education and socialization. This is done as a step to educate the public in understanding the flow of advantages and disadvantages when making *online* loans (Rayyan Sugangga dan Erwin Hari Sentoso, 2020: 58).

Before *online* loans were present and busy being used, money loans were usually done manually by banks or other institutions. This process takes quite a long time and must follow a fairly complicated flow of procedures (Istiqamah, 2019: 291). The lending process will also be classified based on the amount of money to be borrowed, the type of job the borrower does, and the specified time period for repayment. Thus, the community is forced to go through a series of manual procedures to get the money loan as expected.

Currently, money loans are greatly helped by the help of technology and internet networks. Borrowers can download an *online* loan application , visit the available *website* and call the contact number listed to borrow money *online* (Anggraini Dila Pitaloka, 2020: 1597). The advantage of *online* loans *is that they* can beat manual lending procedures at banks and other institutions, namely the ease of disbursing money in just a matter of hours. Usually, if the loan is done at a bank or other institution, it takes about 7-14 days for disbursement, while *online* loans only take 4 hours – 3 days. This disbursement process is the choice of the community to switch to borrowing money *online.*

Before an *online* loan *is* made, an institution needs to pay attention to several rules and conditions that must be met to build an *online* money lending service . organizers are required to register their institutions and apply for permits to the Financial Services Authority (OJK) (Istiqamah, 2019: 291). In addition, OJK also provides a maximum loan limit of 2 billion. this has been regulated in the Financial Services Authority Regulation Number 77/POJK.01/2016 of 2016 concerning Information Technology-Based Borrowing-Lending Services and Bank Indonesia

Regulation Number 19/12/PBI/2017 of 2017 concerning the Implementation of Financial Technology (Istiqamah, 2019: 291).

Based on the legal reference above, the process of borrowing money *online* must go through all agreements made between the debtor and creditor. These agreements and agreements are carried out in *online* form to make it easier to establish mutual agreements. This agreement is contained in the deed and contract *online.* This form of agreement is considered weak because the deed issued is not authentic and notarial (Istiqamah, 2019: 298). Even though the agreement is considered weak, it can still be used as evidence when needed. However, there are shortcomings that need to be considered by the borrower when entering into a contract agreement, namely the absence of witnesses who observe the contract process and signatures that can be misused.

Furthermore, when the borrower starts making *online* loans at the desired institution, the borrower will be faced with various conditions such as providing an Identity Card (KTP), Family Card (KK), NPWP, driving license, telephone number and bank account number (Iftah Putri Nurdiani, 2020: 4). then the file is uploaded on the link provided by the *online* borrower. Borrowers are also given convenience by offering repayment through the nearest Indomaret or Alfamart. This convenience is also the target and target of borrowers because borrowers do not need to spend a lot of energy preparing files manually. Then, in addition to providing a personal information data file, the borrower needs to do an analysis and prior approval. When the borrowed funds have begun to be disbursed, the borrower must immediately repay the loan in accordance with the mutually agreed upon agreement.

Borrowing *online* certainly not only offers convenience in transactions, but also has an impact that needs to be considered carefully by borrowers. Not all *online* loans are in legal status, many illegal *online* loans exist without government permission. Recently, there has been a lot of news circulating regarding the extortion experienced by *online* borrowers *.* The form of the crime committed is to force the borrower to pay off the loan immediately. For example, a mother in the Wonogiri area, Central Java, was unable to pay or pay off an *online* loan and ended up committing suicide (Sigit Kurniawan, 2021). Another victim also said that the money disbursed did not match the agreed loan. In fact, when the victim cannot pay off on the agreed schedule, 10% interest will be charged every day. it does not stop there, victims and their families will also be threatened and their personal data used for their benefit. This is a public concern at this time, especially during a pandemic, people really need some funds to carry out the lives of their family members. So, many illegal *online* loans have sprung up offering the convenience of *online* borrowing and ending up with *online* fraud *.*

Cases of illegal *online* loan crimes can be said to be part of cyber crime. This is assessed based on the practice of crimes committed through the internet network. This renewable technology is used by illegal *online* borrowers to seize victims under the pretext of ease of payment, cooperative savings and loans and the accuracy of the borrower's personal data security (Wening Novridatasati, Ridwan, dan Allyth Prakarsa: 262).

According to Setyo Budiantoro as a senior economic researcher from Perkumpulan Prakarsa, he stated that more and more illegal *online* loans were

found in Indonesia. This is due to the weakening of the regulatory system for *fintech* (Sigit Kurniawan, 2021). Another factor is the difficulty of accessing finance from formal institutions, such as banks. So, people are more interested in making *online* loans illegally. In addition, financial literacy is also considered very low among individuals and households. The borrower does not first examine the advantages and disadvantages that will be obtained after making an *online* loan.

In addition, Kisnu , who is a lecturer at the Department of Criminology, FISIP, University of Indonesia, once revealed that the increase in the use of *distributed computing* makes it increasingly difficult to control information systems, because when the number of *mobile computing* usage increases , there will be more opportunities to enter the network. so that the greater the opportunity for parties to steal or change information and the dramatic increase in internet and broadband usage which on the other hand is an exposure to information system security risks. Many victims of *cyber crime* do not realize that they have become victims because victims cannot easily identify if something happened to them is a crime, victims are reluctant to report, fear publicity or are seen as damaging to their reputation and apathy (fisip.ui.ac.id, 13 Agustus 2021).

In addition to the technical causes as described above, there are also various reasons from a criminological perspective that are factors that cause criminal acts during the pandemic, which are related to the problem of poverty, lack of access to education, increasing unemployment, population density, and weakening of the population. social control (Sahat Maruli Tua Situmeang, 2021). Likewise, at the point of social control, the ranks of the Indonesian government need to work together to eradicate various actions that are the root cause of problems and are detrimental to *cybercrime* victims . Therefore, it is hoped that there will be policies and legal rules that can firmly protect *online* loan victims and also monitor the performance of *online* loans .

In this regard, in the next sub-chapter the author will systematically describe the efforts made by the state or government in overcoming these problems.

c. Human Rights: Privacy Right Violation of Illegal Online Loans Victims

Privacy right is a right inherent in human beings which is very important to be respected. Therefore, the debate on privacy rights itself has long been discussed by world legal practitioners, as according to a note in a study it was stated that, for the first time the issue of privacy rights was discussed and considered important in court decisions in the UK, which was then followed by America. In addition, regarding the conceptualization of privacy rights, Samuel Warren and Louis Brandeis discussed in the Harvard Law Review on December 15, 1890. The implications of this idea resulted in an acknowledgment of the need to protect the right to privacy (Wahyudi Djafar, 1890).

Privacy right is basically a representation of how humans should keep the information attached to themselves confidential, with no acts of discrimination against a person, such as stalking (W. A. Parent, 1983: 305-338). Theft and exposing someone's personal data and so on. In line with that, the protection of one's personal information as a form of privacy right needs to be respected, because if not, it can have implications for criminal acts that can be carried out by irresponsible parties,

the explanation of this point has been described in previous sub-chapter.

With regard to the provisions on the protection of privacy rights, it has been implicitly described in Article 28 G Paragraph (1) of the 1945 Constitution, which reads "Everyone has the right to the protection of his personal, family, honor, dignity, and property under his control. , and has the right to a sense of security and protection from the threat of fear to do or not do something which is a human right". In addition, there are also special rules relating to human rights, namely Law Number 39 of 1999 which clearly guarantees the protection of the right to privacy (privacy right). Not only that, Indonesia as one of the countries involved in the International Covenant on Civil and Political Rights (ICCPR), which is mandatory for every government in Indonesia to protect the privacy and personal data of its citizens (UU RI Nomor 12 Tahun 2005). Although the ICCPR is an institution of the United Nations Human Rights Committee, until 2018, the ICCPR has not taken special steps regarding the handling of digital privacy rights in a systematic and comprehensive manner (Human Rights Council Adopted Resolution, April 2018).

Based on the description above, it is about how the protection of privacy rights needs to be protected, respected and not discriminated against, however, acts of violating privacy rights along with the development of information technology have also developed various motives for crimes that occur in the field. In line with that, these human rights violations can occur because of the complexity between the lack of public knowledge about online loan mechanisms and there is no special regulation that regulates Financial Technology including protection against misuse of personal data which is an administrative mechanism in conducting Financial Technology transactions (*Rodes Ober Adi Guna Pardosi, Yuliana Primawardani, 2020).* In other studies, it is also stated that the implementation of legal policies related to the protection of personal data is currently not running effectively (Sahat Maruli Tua Situmeang, 2021).

Meanwhile, regarding the causes of various violations of privacy rights at this time, the International Covenant on Civil and Political Rights (ICCPR) states that violations of privacy rights can arise due to data collection activities carried out in people's daily lives to access various services, such as banking, telephone mobile, online shopping and other essential services. The level of sensitivity to data is caused by being collected without proper control and supervision (Human Rights Council Adopted Resolution, April 2018).

Among several cases that have been highlighted by the author is the vulnerability of human rights violations committed by illegal online lenders by committing cyber gender violence. The stereotype of women as weak creatures has in fact led to more severe discrimination than men. As according to the complaint data from online application users, 72.08% of them are women and 22% of them admit to experiencing Cyber Gender-Based Violence or abbreviated as KGSB. The forms of KBGS usually target female victims with various threats, such as threats to kill their children, telling the victim to sell herself, disseminating loan information to all of the victim's colleagues and superiors so that the victim can be laid off, and also disseminating personal data. and a photo of the victim's face (Metro.Tempo.Co, 10 September 2021).

In line with the case above, basically the protection of personal data is very

urgent to do in ensuring the peace of human life, because everyone has the right to respect their personal and family life (Dmytro Gadomsky & Tykhin Alekseienko, 2013). The description of the actions taken by the online lender is a very serious threat, thus making the victim feel ashamed because her privacy right has been disturbed and intimidated, so there are cases where the victim finally decides to commit suicide.

Harassment and discrimination against women are also carried out in cases where the person who makes the online loan is a man, in this case a man who is married and has not paid off his debt on an illegal online loan will be forced so that the victim is willing to sacrifice his wife to have sexual relations with the organizer of the illegal loan, with a guarantee that if he agrees to it then all his debts to the related party will be considered paid off. From the examples of these cases, the author considers this an act of harassment against women as well as a violation of human rights, especially privacy rights and the right to a sense of security as mandated by the Constitution.

Based on the author's analysis, various violations committed by illegal online loan actors not only harm and discriminate against the victims involved, but the very complex problems make other parties also disadvantaged because online lenders can access the data and phone numbers of the parties. who is the partner of the main victim. This happens because in carrying out their actions, these illegal online lenders do not hesitate to terrorize other people who have nothing to do with the online loan, just because he is a friend of the borrower or his name is in the borrower's contact is enough to make the contact enter. in the terror list of online loan providers (CNN Indonesia, 27 Agustus 2021).

d. Legal Rules and Countermeasures for Illegal Online Loans

Given that there have been many previous studies that have reviewed the legal rule for cybercrime, in this study, the author will only present a general summary. However, what is new here is the description related to the latest policies taken by high state institutions in addressing the problem of illegal online loans. OJK as an online loan supervisory agency in Indonesia, has issued a POJK regarding the implementation of online loans (P2P leading), in which information technology-based lending and borrowing services are regulated in the Financial Services Authority Regulation Number 77/POJK.01/2016 Year 2016 concerning Lending and Borrowing Services. Information Technology-Based Money ("POJK 77/2016"). Article 1 point 3 of POJK 77/2016 explains that information technology-based lending and borrowing services is the provision of financial services to bring together lenders and loan recipients in order to enter into lending and borrowing agreements in rupiah currency directly through an electronic system using the internet network (Ayu Dian Ningtias, Suisno, Dan Dhevi Nayasari, Jurnal Independent Fakultas Hukum, Vol. 8, No.2).

Although there are regulations in the POJK regarding the implementation of legal online lending, it cannot be denied that these rules are still very weak, so it is not surprising that the practice of online lending remains fertile. The existence of illegal online lending practices in Indonesia is very well known for its unethical, intimidating, inhumane, and against the law actions, which have an impact on victims

and their families, such as psychological disorders, physically threatened, or even victims who end their lives.

There is a case where the victim does not get their rights like the victim in criminal acts in general (Wening Novridasati, Ridwan, Allyth Prakarsa, 2020), these facts represent how weak the law in Indonesia is. In addition, related to the discussion in the previous sub-chapter regarding various cases of threats and harassment that were made to victims of illegal online loans, these actions can be categorized as a violation of Article 27 paragraph (1) of the ITE Law, which reads "any person who intentionally and without the right to distribute and/or transmit and/or make accessible Electronic Information and/or Electronic Documents that have contents that violate decency". With the regulation of the Act, at least it can be a legal rule for victims of cybercrime.

In addition to the ITE Law above, there are also other legal rules that control online loan actions that are proven to have violated the law. For example, there are cases related to fintech or illegal online loans that violate the form of distributing personal data, this can be subject to Article 32 in conjunction with Article 48 of Law no. 11 of 2008 in conjunction with Law no. 19 of 2016 concerning Information and Electronic Transactions (ITE). Then, the threat of fintech companies to customers can be charged with Article 368 of the Criminal Code (KUHP) and Article 29 in conjunction with Article 45B of the ITE Law. The "rogue" fintech company can also be charged with Article 55 of the Criminal Code for being involved in a criminal act. If the crime takes the form of physical violence, the taking of goods may be subject to sanctions in accordance with Article 170, Article 351, Article 368 Paragraph 1, Article 335 Paragraph 1 after the decision of the Constitutional Court (Dhevi Nayasari Sastradinata, 2020).

Various cybercrime actions carried out by illegal online loan providers as described in the previous sub-chapter, can be classified in the form of acts of digital thuggery. Therefore, serious preventive and repressive actions need to be mobilized by various government officials, either in the form of regulations and policies, or direct actions that synergize with each other to eradicate various actions that are the source or root of the cybercrime action. In addition, various binding laws and government policies are needed to protect the public from various acts of digital thuggery carried out by illegal online loan providers.

With regard to efforts to protect various cybercrime acts, considering that the nature of criminal activities in cyberspace is different from traditional criminal acts, legal resistance cannot be pursued through traditional means (Dmytro Gadomsky & Tykhin Alekseienko, 2013). In Indonesia itself, until the end of 2021, there have been many preventive and repressive measures taken by various levels of government in tackling the problem of illegal online loans. As was done by Kominfo with its strategy of illegal loan screening through internet raids, this effort has been carried out from 2018 to October 26, 2021, and has captured as many as 4,096 illegal online loan content located on various sites, google play store, file sharing sites and media. social media, and has been blocked because it is an act of violating the applicable laws and regulations. In addition, through the Cekrekening.id platform, Kominfo has received 5,327 reports about accounts used for fraudulent actions related to illegal online lending activities, which will then be compiled and collected in a blacklist database

by Kominfo (Novina Putri Bestari, 29 Oktober 2021).

In addition, the government has also carried out various socializations about the movement of online loans and the negative implications for the community. Not only that, the government is also in the stage of fighting these illegal acts by closing illegal online loans and taking action against the owners of capital or related online loan investors. In addition, the complexity of the problems caused by online loans has prompted the Coordinating Minister for Political, Legal and Security Affairs, Mahfud MD, to issue a statement so that illegal online loan customers do not pay their debt installments again, they must be billed (Kompas.com, 21 Oktober 2021). Actions like this are an effort to make illegal online loan providers become a deterrent and no longer practice illegal borrowing.

In line with the statement above, the ranks of high state institutions have delivered their press release with No. 295/HM/Kominfo/08/2021, this press release was carried out as an effort to eradicate illegal online lending practices. These high state institutions consist of the Financial Services Authority, Bank Indonesia, the Indonesian People's Police, the Ministry of Communication and Information of the Republic of Indonesia, and the Ministry of Cooperatives and Small and Medium Enterprises of the Republic of Indonesia which synergize to issue a joint statement according to their respective authorities in protecting the public. .

The joint statement discussed in the press release relates to several preventions, handling public complaints, and law enforcement. There are several prevention efforts that have been mutually agreed upon, including, first, strengthening financial literacy and conducting an active and comprehensive communication program to increase public awareness of illegal online loan offers. Second, strengthening education programs for the public to increase prudence in making online loans and safeguarding personal data. Third, strengthen cooperation between authorities and application developers to prevent the spread of illegal online loans through applications and cellular phone service providers to disseminate information on public awareness of illegal online loan offers. Fourth, prohibit banks, non-bank Payment Service Providers (PJP), aggregators, and cooperatives from collaborating or facilitating illegal online loans, and must comply with the principle of recognizing service users (Know Your Customer) in accordance with applicable laws and regulations.

Meanwhile, efforts to handle public complaints according to the mutual agreement are carried out by opening access to public complaints at each relevant institution or ministry and taking follow-up actions on public complaints in accordance with the authority of each Ministry/Agency and/or reporting to the Indonesian National Police for legal process is carried out. In law enforcement efforts, these state institutions also seek to take legal action against the perpetrators of illegal online loans in accordance with the authority of each Ministry/Agency and conduct international cooperation in the context of eradicating illegal online loan operations across countries. After that, following up on the Joint Statements from several state institutions or ministries, the relevant institutions make it happen in a Cooperation Agreement (PKS) which discusses the Eradication of Illegal Online Loans which will contain steps from each Ministry/Institution that coordinated within the Investment Alert Task Force (Kominfo.go.id, 20 Agustus 2021).

C. CONCLUSION

Online loan crimes are often found in various parts of the country, one of which is in Indonesia. This crime has harmed many victims, especially during the pandemic. People really need funds that will be used to maintain the survival of their family members. Online loans are the choice of some people because the procedure is very easy to do than the procedures applied by banks or other official institutions. This ease of transactions is used as a tool for online loan providers to attract many targets. At first online loans seem easy and fast, but there are various risks that must be faced by borrowers. Between the borrower and the party providing the loan will enter into a mutual agreement through a contract agreement. Borrowers will be subject to a review schedule and a predetermined amount of funds and interest. If the borrower does not succeed in paying off the loan, it will be subject to an increase every day.

Seeing this process, borrowers often get criminal acts, such as acts of terror against themselves and their families, exploiting borrowers' personal data and being considered as online fraudsters. In addition, borrowers also often get criminal actions from online loan providers, such as not being notified when the repayment period will be made. Then, the party carries out its crime by taking out a loan on another day that is not in accordance with the agreement and automatically the increase in collection will multiply and is beyond the control of the borrower. This case not only affects the borrower physically, but also psychologically.

Therefore, countermeasures from the government are highly expected so that online loan crimes no longer operate. In addition, there is a need for government firmness in maintaining and protecting people who will make online loans. So far, the government's efforts in tackling crime in cyberspace and online loans have been fairly good. The government has issued various regulations such as the ITE Law and POJK as well as other legal rules that will protect victims. However, the government also needs to pay attention to the human rights and privacy rights of victims of online lending crimes wisely. Thus, matters relating to cybercrime will soon be resolved.

REFERENCES

Akhmad Yani Surachman, "Media Massa beserta Ideologi nya Dalam Proses Hegemoni", Media Nusantara Vol. XVIII, No. 1 (2021): 72.

Anggraini Dila Pitaloka, "Pertanggungjawaban Pidana Pelaku Pinjaman Online yang Berimplikasi Tindak Pidana", Jurist-Diction, Vol. 3, No. 5 (2020): 1597.

Ani Mardatila, " 12 Jenis-jenis Cyber Crime atau Kejahatan Dunia Maya yang Perlu Diwaspadai", Merdeka.com (2020).

Ayu Dian Ningtias, Suisno, Dan Dhevi Nayasari "Aspek Hukum Terhadap Perusahaan Pinjaman Online Ilegal Menurut System Hukum Di Indonesia" Jurnal Independent Fakultas Hukum, Vol. 8, No.2. Https://Jurnalhukum.Unisla.

Ac.Id/Index.Php/Independent/Article/View/122/Pdf

Cnn Indonesia "Pakar Sebut Pinjol Ilegal Bentuk Baru Premanisme Digital", 27 Agustus 2021.Https://Www.Cnnindonesia.Com/Teknologi/20210827113036-185-686223/Pakar-Sebut-Pinjol-Ilegal-Bentuk-Baru-Premanisme-Digital

Deutsche Welle "Kejahatan Dunia Maya Berkembang Pesat Di Masa Pandemi Covid-19", 14 May 2021. Https://Republika.Co.Id/Berita/Internasional/Deutsche-Welle/Qt021d3915000/Kejahatan-Dunia-Maya-Berkembang-Pesat-Di-Masa-Pandemi-Covid19

Dhevi Nayasari Sastradinata "Aspek Hukum Lembaga Pinjaman Online Ilegal Di Indonesia" Jurnal Independent Fakultas Hukum, Vol. 8, No. 1 (2020). Http://Jurnalhukum.Unisla.Ac.Id/Index.Php/Independent/Article/View/115/Pdf

Dista Amalia Arifa, "Kasus *Cybercrime* di Indonesia", Jurnal Bisnis dan Ekonomi (JBE), Vol 18, No. 2 (2011): 187.

Dmytro Gadomsky & Tykhin Alekseienko, "Right To Privacy And Cybercrime Investigation", Int. J. Intellectual Property Management, Vol. 6, No. 1/2 (2013). Doi:10.1504/Ijipm.2013.053453

Fakultas Ilmu Sosial Dan Ilmu Politik Universitas Indonesia, "Mencegah Dan Membatasi Cyber Crime Di Masa Pandemi", 13 Agustus 2021. Https://Fisip.Ui.Ac.Id/Mencegah-Dan-Membatasi-Cyber-Crime-Di-Masa-Pandemi/

Hardianto Djanggih dan Nurul Qamar, "Penerapan Teori-teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime)", Pandecta, Vol. 13, No. 1 (2018): 13.

Human Rights Council Adopted Resolution "The Right To Privacy In The Digital Age", April 2018. Https://Www.Ohchr.Org/Documents/Issues/Digitalage/Reportprivacyindigitalage/Inclo.Pdf

Iftah Putri Nurdiani, "Pencurian Identitas Digital sebagai Bentuk Cyber Related Crime", Jurnal Kriminologi Indonesia, Vol. 16, No. 2 (2020): 4.

Istiqamah, "Analisis Pinjaman Online Oleh Fintech Dalam Kajian Hukum Perdata", Jurisprudentie, Vol. 6, No. 2 (2019): 291.

Kimberly Pavlik "Cybercrime, Hacking, And Legislation" Journal Of Cybersecurity Research, Vol. 1, No. 1 (2017). Https://Clutejournals.Com/Index.Php/Jcr/Article/Download/9966/10067/37046

Kominfo.Go.Id "Pernyataan Bersama Ojk, Bank Indonesia, Kepolisian Ri, Kominfo Dan Kemenkop Ukm Dalam Pemberantasan Pinjaman Online Ilegal" 20 Agustus 2021. Https://Www.Kominfo.Go.Id/Content/Detail/36494/Siaran-Pers-No-No-295hmkominfo082021-Tentang-Pernyataan-Bersama-Ojk-Bank-Indonesia-Kepolisian-Ri-Kominfo-Dan-Kemenkop-Ukm-Dalam-

Pemberantasan-Pinjaman-Online-Ilegal/0/Siaranpers

Kompas.Com «Jumlah Aduan Pinjol Ilegal Ke Ojk Tegal Naik 100 Persen Selama 2021" 21 Oktober 2021. Https://Regional.Kompas.Com/Read/2021/10/21/204453178/Jumlah-Aduan-Pinjol-Ilegal-Ke-Ojk-Tegal-Naik-100-Persen-Selama-2021?Page=All.

Machsun Rifauddin dan Arfin Nurma Halida, "Waspada Cybercrime dan Informasi Hoax Pada Media Sosial Facebook", Khizanah Al-Hikmah, Vol. 6, No. 2 (2018): 101.

Metro.Tempo.Co "Lbh Jakarta: Wanita Pengguna Pinjol Rentan Kekerasan Gender Siber, Sebab", 10 September 2021. Https://Metro.Tempo.Co/Read/1504714/Lbh-Jakarta-Wanita-Pengguna-Pinjol-Rentan-Kekerasan-Gender-Siber-Sebab/Full&View=Ok

Novina Putri Bestari "Kominfo Razia Internet, 4.096 Pinjol Ilegal Diblokir", 29 Oktober 2021. Https://Www.Cnbcindonesia.Com/Tech/20211029183059-37-287653/Kominfo-Razia-Internet-4096-Pinjol-Ilegal-Diblokir

Rayyan Sugangga dan Erwin Hari Sentoso, "Perlindungan Hukum Terhadap Pengguna Pinjaman *Online* (Pinjol) Ilegal", PAJOUL (Pakuan Justice Journal of Law), Vol. 1, No. 1 (2020): 58.

Richard Apau & Felix Nti Koranteng "Impact Of Cybercrime And Trust On The Use Of E-Commerce Technologies: An Application Of The Theory Of Planned Behavior", Journal Of Cyber Criminology (Diamond Open Access Journal, Vol. 13, No. 2 (2019). Doi: 10.5281/Zenodo.3697886

*Rodes Ober Adi Guna Pardosi, Yuliana Primawardani "*Perlindungan Hak Pengguna Layanan Pinjaman Online Dalam Perspektif Hak Asasi Manusia", Jurnal Ham, Vol. 11, No. 3 (2020). Https://Ejournal.Balitbangham.Go.Id/Index.Php/Ham/Article/View/1400/Pdf

Sahat Maruli Tua Situmeang, "Fenomena Kejahatan Di Masa Pandemi Covid-19: Perspektif Kriminologi", Bidang Hukum: Majalah Ilmiah Unikom, Vol. 19, No. 1, 2021.

Sahat Maruli Tua Situmeang, "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Sibe", Jurnal Sasi: Fakultas Hukum Universitas Pattimura, Vol. 27, No. 1 (2021).

Sara Norden, *Thesis*, "How The Internet Has Changed The Face Of Crime" Florida Gulf Coast University, United States. Lihat Https://Fgcu.Digital.Flvc.Org/Islandora/Object/Fgcu%3a21423/Datastream/Obj/Download/How_The_Internet_Has_Changed_The_Face_Of_Crime_.Pdf

Sejarah Cyber Crime, Https://Danrayusuma.Weebly.Com/Sejarah-Cybercrime.Html

Steven Millward, "Perkembangan Internet Mobile Paling Besar di Dunia Ada di Asia",

id.techinasia.com,, 2014.

Tempo.Co "Bos Ojk Sebut Pinjol Sudah Salurkan Pinjaman Rp 27,48 T, Melonjak 116,2 Persen", 27 Oktober 2021. Https://Bisnis.Tempo.Co/Read/1521946/Bos-Ojk-Sebut-Pinjol-Sudah-Salurkan-Pinjaman-Rp-2748-T-Melonjak-1162-Persen/Full&View=Ok

Thomas HA Gregory, "Ketenaran Cybercrime di Indonesia", Makalah STIMIK Perbanas 2005.

Undang-Undang Republik Indonesia Nomor 12 Tahun 2005: Pengesahan International Covenant On Civil And Political Rights (Kovenan Internasional Tentang Hak-Hak Sipil Dan Politik), Http://Www.Dpr.Go.Id/Doksetjen/Dokumen/-Regulasi-Uu-No.-12-Tahun-2005-Tentang-Pengesahan-Kovenan-Internasional-Tentang-Hak-Hak-Sipil-Dan-Politik-1552380410.Pdf

Virdita Ratriani "Kenali, Ini 3 Modus Pinjol Ilegal Jerat Korbannya", 23 Oktober 2021. Https://Keuangan.Kontan.Co.Id/News/Kenali-Ini-3-Modus-Pinjol-Ilegal-Jerat-Korbannya

W. A. Parent, "A New Definition Of Privacy For The Law", Law And Philosophy, Vol. 2, No. 3 (1983), Hal. 305-338. Http://Www.Jstor.Org/Stable/3504563

Wahyudi Djafar "Hukum Perlindungan Data Pribadi Di Indonesia: Lanskap, Urgensi, Dan Kebutuhan Pembaruan", Https://Law.Ugm.Ac.Id/Wp-Content/Uploads/Sites/1043/2019/08/Hukum-Perlindungan-Data-Pribadi-Di-Indonesia-Wahyudi-Djafar.Pdf, Lihat : Samuel Warren Dan Louis Brandeis, The Right To Privacy, Dalam Harvard Law Review Vol. Iv No. 5, 15 Desember 1890, Http://Faculty.Uml.Edu/Sgallagher/Brandeisprivacy.Htm.

Wening Novridasati, Ridwan, Allyth Prakarsa "Pertanggungjawaban Pidana Desk Collector Fintech Ilegal Serta Perlindungan Terhadap Korban", Jurnal Litigasi, Vol. 21, No. 2 (2020). Doi: Http://Dx.Doi.Org/10.23969/Litigasi.V21i2.3103