www.bircu-journal.com/index.php/birci
Budapest International Research and Critics Institute-Journal (BIRCI-Journal)
Humanities and Social Sciences
ISSN 2615-3076 Online)
ISSN 2615-1715 (Print)
Budapest Institute

Cyber Crime Law Enforcement Against Illegal Access to Online Banking in Indonesia

Mohamad Yusuf[1], Tofik Yanuar Chandra[2], Ramlani Lina Sinaulan[3]
[1,2,3] *Faculty of Law, Jabaya University Jakarta, Indonesia*
ghumaisa.ihwan@gmail.com

Abstract

Cybercrime refers to the activity of a crime with a computer or computer network being a tool, target or place where a crime occurs. These include online auctions, cheque forgery, credit card fraud, identity fraud and child pornography and illegal internet access. The development of technology and its application has infiltrated and strongly influenced modern life, even a largeparagraph of business activities has entrusted to such technology, one of which is the banking industry. The purpose of the research in this paper is to analyze cyber crime law enforcement against illegal access to online banking in Indonesia and analyze the punishment of perpetrators of illegal access to online banking in Indonesia. The research uses a normative juridical approach that emphasizes literature research. In this study, what is used is the Statutory approach, the conceptual approach, the differential approach, the case approach, and the historical approach. The sources of Legal Materials used are primary, secondary and tertiary legal materials. The analysis of the legal materials used is qualitative. Based on research, it shows that the law enforcement used as the legal basis for cybercrime cases is Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE). With the ITE law, it is hoped that it can protect the public of information technology users in Indonesia. This is important considering the increasing number of internet technology users from year to year. The increasing use of the internet on the one hand provides many conveniences for humans in carrying out their activities, on the other hand making it easier for certain parties to commit criminal acts.

Keywords
law enforcement; cyber crime; illegal access; Indonesia

I. Introduction

In modern times today, humans are inseparable from the use of social media. Social media is a kind of media that is used for media that is free to express and explore the opinions we have continuously. On the other hand, a social network is a page where a person will create a web page (his social media account) personally, and will be connected and able to communicate with people he knows and new people he knows in cyberspace. Social networks that are often used by the community include Whatsapp, Telegram, Facebook, Twitter, and so on. Development is a systematic and continuous effort made to realize something that is aspired. Development is a change towards improvement. Changes towards improvement require the mobilization of all human resources and reason to realize what is aspired. In addition, development is also very dependent on the availability of natural resource wealth. The availability of natural resources is one of the keys to economic growth in an area. (Shah, M. et al. 2020)

DOI: *https://doi.org/10.33258/birci.v5i3.6619*

On the other hand, criminals, especially hackers who deliberately commit illegal acts to take personal data of individuals, especially for Online Banking users who are connected to their bank account's whatsapp number, of course, there have been many criminals who use this opportunity to break into someone's Online Banking account, lately it often happens on the grounds that the operator asks for an OTP (One-Time Password) code), as in the case, based on police findings, from 2017 until it was caught in 2020, the suspects had taken over as many as 3,070 accounts with a total loss suffered by the victim of 21 billion (compass).

This is a very big problem to overcome. Internet users, especially those who have Online Banking accounts connected to their social media accounts, will be able to hack their data to be taken by hackers. This is then to be used as an issue why you have to learn to use the internet properly and correctly, so that there is no breach of customer accounts by people who cannot be responsible. It is necessary to prevent the use of side effects from the use of unexpected and unwanted social media. The main problem is crimes in society related to the use of social media accounts. This is what the government must pay attention to with the use of legal infrastructure and its regulations so that the use of information technology is used safely to prevent misuse.

As contained in the ITE Law No. 11 of 2008, in Article:

a. Article 31 paragraph 1: Any person intentionally and without rights or unlawfully intercepts or intercepts electronic information and or electronic documents in a computer and or electronic system certainly belonging to another person.
b. Article 31 paragraph 2: Any person intentionally or without rights or unlawfully commits an interception or transmission of electronic documents that are not public from, to, and within a computer and or certain electronic system belonging to another person, whether that does not cause alteration, omission and or termination of electronic information and or electronic documents transmitted.
c. Article 47: Any person who fulfills the elements as referred to in Article 31 paragraph (1) or paragraph (2) shall be punished with a maximum imprisonment of 10 (ten) years and/or a maximum fine of IDR 800,000,000.00 (eight hundred million rupiah).

There are many modes and motives carried out by the perpetrator with the aim of taking advantage. One of them is by hijacking someone's WhatsApp account, then utilizing their personal data or digital account. This kind of action is known as a scam, where the act is a crime committed by the perpetrator deceiving the potential victim by providing a number code or information related to the person's personal data, so that the perpetrator can access the personal account of the potential victim. In reality, the perpetrators play online banking with money breakers belonging to customers and they carry out their actions using Internet media, of course, this makes it difficult for the police to uncover because the location of the perpetrators is difficult to detect.

By looking at the phenomenon and a number of opinions above, it is undeniable that cyber crime is increasingly demanding wider attention from law enforcement and lawmakers, so that the opportunity for losses caused by the improper use of information technology, requires regulatory and statutory tools that limit and punish the use of information technology for crimes, because cyber crime whatever form it is classified as a crime that must be punished, the question that is often asked is whether Indonesian legislation has regulated the problem?

Based on this fact, it is hoped that there will be a statutory provision that is able to reach the act. The preparation of a criminal law to overcome cyber crime, especially related to internet banking crimes, is not easy considering the continued development of

information technology, for this reason, a study through legal policy becomes relevant and important to do.

This opinion is reinforced by the fact that many criminal cases related to the cyber world in relation to internet crimes cannot be resolved by the judicial system completely because the authorities face difficulties in conducting investigations and looking for articles of law that can be used as a basis for prosecution in court. Some of the formulations of the problem are the following: How is the enforcement of cyber crime law against criminal acts of illegal access to online banking in Indonesia? and How is the punishment of perpetrators of criminal acts of illegal access to online banking in Indonesia?

II. Research Method

The type of research that the author uses in writing is the Normative Juridical Research Type, because in cyber crime crime will examine and study the relevant legal rules which based on the facts found, in making observations about the laws and regulations that apply legally in cyber crime in order to find answers regarding the enforcement of cyber crime laws in order to realize legal certainty.

In connection with the type of research used is normative juridical legal research, in this study the researcher uses three approaches (approaches), namely the statute approach, the conceptual approach (conceptual approach), the case approach (cases approach). The statute approach is an approach to normative juridical research methods that can be used as legal rules (Johnny Ibrahim, 2005). Meanwhile, the conceptual approach is usually used to decipher and analyze research problems that depart from the vacuum of norms. That is, in the current legal system, there are no or no norms of a law that can be applied to legal events or legal disputes (I Made Pasek Diantha, 2017).

In conclusion, normative legal research in the preparation of this dissertation all legal materials are tried by the method of mesistematics to recorded legal materials. Systematization requires grouping legal materials to make it easier for the analytical and architectural professions. The activity that is tried in the analysis of normative legal research information with the method of information obtained in an analysis in a qualitative descriptive way is the analysis of information that cannot be calculated. The legal material obtained next is tried to review, check and group into special Paragraphs to be processed into data information.

III. Result and Discussion

3.1 Cyber Crime Law Enforcement Against Illegal Access to Online Banking in Indonesia

Law enforcement in cyber crimes against illegal crimes is contained in the ITE Law. As contained in the ITE Law No. 11 of 2008, in Article:

a. Article 31 paragraph 1: Any person intentionally and without rights or unlawfully intercepts or intercepts electronic information and or electronic documents in a computer and or electronic system certainly belonging to another person.
b. Article 31 paragraph 2: Any person intentionally or without rights or unlawfully commits an interception or transmission of electronic documents that are not public from, to, and within a computer and or certain electronic system belonging to another person, whether that does not cause alteration, omission and or termination of electronic information and or electronic documents transmitted.

c. Article 47: Any person who fulfills the elements as referred to in Article 31 paragraph (1) or paragraph (2) shall be punished with a maximum imprisonment of 10 (ten) years and/or a maximum fine of IDR 800,000,000.00 (eight hundred million rupiah).

Departing from the above principle to the real thing when it comes to Cyber crime, with the enactment of Law No. 11 of 2008 is a crime. In the legal way to decide the cyber crime actor as the perpetrator of the crime until the convincing factor with the power of factual equipment becomes a very meaningful matter. In the law of criminal activities of the Criminal Procedure Code, the determination of a decent amount of fact is a problem that is not subjugated to be suspected in terms of the factor of error and the existence of crimes. This means that the evidentiary case in the way of Cyber crime litigation, is an important factor in deciding the defendant as the perpetrator of the Cyber crime act.

Law No. 11 of 2008 concerning Data and Electronic Business is under the regulatory law regarding errors in data technology spoken of by Cyber crime. Cyber crime is a type of error related to the exploitation of a data and communication technology without restrictions, and has a solid character with a technological engineering that entrusts a large level of security, from a data that is informed and accessed by internet consumers (P.H, 2010).

In Article 35 of Law No. 11 of 2008 concerning ITE, it has been explained that" Every Person with a planned and without rights or against the law carries out falsehood, invention, replacement, disappearance, destruction of Electronic Data and or or Electronic Deeds with the aim that Electronic Data and or or Electronic Deeds are mistaken for as if the information is genuine" (Electronic Transaction Law Number 11 of 2008, 2008).

Cyber activities even though they are virtual can be categorized as actions and clear legal actions in business and applications. In a juridical way in terms of cyber space, it has been out of place to categorize something with dimensions in conventional legal qualifications to be used as objects and actions, because if this method is taken, there are very many difficulties and circumstances that pass the legal net. Illegal access activities are virtual activities that have very clear repercussions, even though the evidence is electronic. That way, the subject of the perpetrator must also be qualified as a person who has carried out legal actions in a clear way.

The use of cybercrime laws in organizing citizens, through criminal legislation, is essentially the article of a policy stage. Next, to ensure that a logical stage of effort in carrying out wisdom cannot be separated from the purpose of the wisdom of development itself in an integral way. That way in an effort to ensure that any policy (listed as the wisdom of the law of crime) is always linked and inseparable from the goals of national development itself; is how to create salvation for the citizens.

The law in principle must estimate the speed of advances in data technology and the internet. Indonesia has no skew that aims at protecting or deterrence, but rather efforts to resolve it after the legal impact is established. Nevertheless, the way the law progresses is underway, it is obligatory to explore a very distant way, and arguably, after the country suffered a considerable loss, the law was passed. Legal arrangements in the aspect of technology must be able to explore the speed of advances in technological developments, instead wanting to urge the apparent current crimes in citizens that cannot be ensnared by using the old law. Meanwhile, the country has been vulnerable to huge losses, but there has been little action from lawmakers in Indonesia to tackle the problem. It was this pedestal that underlies his birth.

The crime of using the pc and the internet Cybercrimes in the small intentions (computer crimes) is tried with various modes of error in Cyber crime such as Underhand access (illegal access). The action of illegal access online bangking above is listed the

action of accessing pc and or data systems belonging to others with the underhand method with the meaning of quoting by underhand the data of individuals in the PC and or data system. The action is contained in the act of data collection and electoral business that prevents any person in a planned manner and without rights or against the law from accessing pc and or electronic system by any method with the aim of obtaining electronic data and or electronic deeds as well as regulated in Article 30 Paragraph 2 Law No. 19 of 2016 concerning the replacement of Law no. 11 of 2008 concerning Electronic Data and Business or known as the ITE Law.

More fully, Article 30 Paragraph 2 of the ITE Law reads, "Everyone with a planned and without rights or against the law accesses the Pc and or or Electronic System by any method also with the aim of obtaining Electronic Data and or or Electronic Deeds".

Each action can be punished if it meets the factors of the crime contained in the alleged Article 30 Paragraph 2 of the ITE Law above, it can be known if the criminal elements are listed, as follows: 1. The Fallacy Factor is Planned; 2. Unlawful Factors constitute Without Rights or Against the Law; 3. The Action Factor is Accessing by Any Method; 4. Object Factors include Electronic Systems; and 5. The purpose is with the aim of obtaining electronic data and or electronic deeds.

Because illegal access errors are listed in the cyber crime area where the character of this error is multi-format, not limited in space and duration to countermeasures must be tried in a comprehensive and prolonged way along with the growth of data and communication technology.

Cyber crime is located in an area of electronics and cyberspace that is difficult to identify in a way, on the contrary, the basis of conventional validity departs from riel action and legal clarity. Cyber crime is closely related to the latest technological advances that are very quickly replaced by the opposite the basis of conventional validity departs from the static basis of official law. Cyber crime crosses the boundaries of the country, on the contrary, the legislation of a country is basically or generally only legal in its own territorial area.

3.2 Conviction of perpetrators of Illegal Access Online Banking in Indonesia

In the use of internet banking, threats to service providers and their users are inevitably will occur, so banks as service providers must pay attention to aspects of protection. The things that can be done by banks in ensuring the security of internet banking applications, one of which is the creation of standardization in internet banking applications. For example, a form about internet banking that is easy to understand by service users who in the future service users can take steps in taking action and providing a manual if they find problems in using internet anking services. Several important things that must be applied by banks to protect their customers if they experience losses by providing legal assistance, both in litigation and non-litigation which aims to be a form of punishment for online bangking criminals (Estradiyanto, 2012).

The punishment of criminals is directed to provide a deterrent effect and guarantee all the security of internet banking application users, namely those contained in theparagraph of the terms and conditions, because in these terms and conditions contain all the rights and obligations of the parties, especially banks and customers. However, in the explanation of these terms and conditions, it is a standard agreement made in writing by the business actor / bank, so that the bank prioritizes the obligations of the customer and the rights of the bank over the rights of the customer and the obligations of the bank itself. So that in the future there will no longer be mistakes, either mistakes or omissions made by customers, from the bank and other threats, it is important to discuss customer protection

for further study, especially legal protection obtained as a customer's right to use internet banking if they experience cybercrime threats.

In every device that uses Information Technology must include a security system so as not to be misused by responsible parties. Online Bangking as one of the banking equipment (devices) that use information technology must also be accompanied by a sufficient security system from unlawful actions by other parties. The case of illegal online access bangking is one of the data leaks caused by the weak security system of a bank.

As is already known that illegal access is already regulated in the ITE Law. The provisions of Article 30 paragraph (3) of the ITE Law stipulate that "Everyone intentionally and without rights or unlawfully accesses Computers and/or Electronic Systems in any way by violating, breaking through, exceeding, or breaking into the security system". Illegal access to mobile banking accounts certainly does not stop only being limited to access to mobile banking accounts, but will also control accounts containing a certain amount of funds in the mobile banking account. Thus, it can be ascertained that the perpetrator will transfer the funds in the mobile banking account he controls.it can be understood that the perpetrator transferred the funds in the mobile banking account including through a fund transfer order to transfer a certain amount of funds to the perpetrator's own account. This kind of deed has also been regulated in the Fund Transfer Law. The provisions of Article 81 of the Fund Transfer Law stipulate that "Any person who unlawfully quotes or transfers some or all of the Budget belonging to another person through an illegal Budget Transfer Order is convicted of a very long sentence of crime of 5 years or compensation of very much IDR 5,000. 000. 000, 00 (5 billion rupiah)".

The determination of Crime that can be used to attract Cyber Crime actors is up to date to the Laws and Regulations of the Crime Law Book (Criminal Code) and Law Number. 11 2008 Regarding Data and Electronic Business. Other determinations, if any, are strewn about various laws and regulations and are not of special habit. On the contrary, America already has several laws and regulations that clearly regulate Cyber Crime, namely Title 18 U. S. Code 1030 which regulates Fraud and related activities in connection with computers, regulates Bank Fraud and Title 18 U. S. Code 2252B which regulates misleading areas name on the internet. Not only that, America is also the body of the Convention on Cyber Crime (Budapest Convention 2001) is a body that plans to protect citizens from mistakes in the world (Shahrullah, R, 2014).

The body is capable of knowing all the transgressions that lie upon all the earth. Indonesia, which is not the body of the conflagration, is very burdened because the agreement creates a very efficient law as a form of protection for cyber crime attitudes. As a result, in terms of cracking down on Cyber Crime when compared to America, Indonesia is inefficient (Arofah, N. R., & Priatnasari, 2020).

This matter is influenced by aparagraph of aspects, among others, due to laws and regulations that do not regulate in detail to the actors who have violated the regulations and the non-optimal application of enforcement measures tried by law enforcement. The Kepri Regional Police, specifically in the Sub-Directorate of the Ditreskrimsus Ayat of cybercrime violations that have been made in March 2020, which has the right to carry out enforcement against cybercrime violations, reports that cybercrime violations are a type of violation that is not easy to handle, this is because the way the actors live and the factual objects of violations are not easy (Disemadi, H. S., & Prananingtyas, 2019).

For the police, cases that have not ended are difficult to handle because they face obstacles, including in calculating the factual equipment of violations which because the digital disposition of violations requires interrogators to also have equipment with

advanced technology in order to create the equipment of the facts, the interrogator squad that is lacking, the way of detention for cybercrime violators located outside the jurisdiction of the Indonesian state which due to the absence of cooperation between The Indonesian state and other countries. However, it is sourced from the data that the author can, to freeze the actors of cybercrime violations, even though they are facing many obstacles and difficulties.

That doesn't make the police run out of ideas and methods, the police are having other ways to find facts or actors located outside the country. The forms of action that have been tried by the police include bonding and collaborating with other state police as a result of being able to help how to detain cybercrime actors in their hiding areas. Mistakes in the banking aspect are also said to be any mistakes related to banking, the illustration is illegal access to online bangking. On the contrary, banking errors are a form of action that has been born by banking law which is a taboo and imperative, for example, the taboo of establishing a black bank and exposing bank secrets. The comparison of isitlah gives rise to or influences the enforcement of the law. Banking errors are to be acted upon through the determination of crimes regulated in banking law, on the contrary, errors in the banking aspect are acted upon through laws outside the banking law (Yulia, 2010).

Law Number 10 of 1998 does not formulate an interpretation of banking crimes. The Act merely categorizes the seThe act clause is listed as an error and on the one hand it can be categorized as an offence. However, there is also an interpretation of banking crimes with crimes in the banking aspect.

Criminal acts in the banking aspect are all types of unlawful actions related to activities in carrying out bank efforts, either the bank as a target or as a tool, on the contrary, banking crimes are crimes tried by banks (Yulia, 2010). There is also a character in the act of banking crime is that the bank can be as a victim or as a whistleblower. Banks as victims, for example, in matters of lying, manipulation of bank letters, and banks as actors such as window dressing actions, deciding on missed interest, distributing unnatural installment cards, carrying out bank efforts in banks, carrying out bank efforts without permission and carrying out efforts that match banks. Illegal Access online bangking is also said as one of the latest forms or formats of errors in the current era that get special attention in the Global world (Arief, 2001).

Thus, concrete steps are needed in preventing illegal access to online bangking. the countermeasures of criminal acts in online crime are more emphasized to the repressive efforts of law enforcement that are preceded by the availability of laws. It is the duty of the police, prosecutors, judges, and of course Bank Indonesia in terms of administrative violations.

There are also criminal arrangements for cybercrime in Indonesia that can also be observed in big intentions and small intentions. In a big way, cybercrime is all criminal acts that use tools or with the encouragement of Electronic Systems. It can be known not only to regulate material cybercrime acts, the ITE Law regulates the acts of cybercrime, especially in the aspect of investigation. Article 42 of the ITE Law stipulates that investigations into crimes in the ITE Law are tried to be based on the determination in Law Number. 8 Of 1981 concerning the Criminal Procedure Code) and determination in the ITE Law. That is, the determination of investigations in the Criminal Procedure Code is always legal as long as it is not regulated otherwise in the ITE Law. Not only the ITE Law, the regulations above in cracking down on cybercrime problems in Indonesia are the regulations of the ITE Law and also technical regulations in investigations in each investigating agency.

IV. Conclusion

Law enforcement that is used as the legal basis for cybercrime cases is Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE) as amended by Law Number 19 of 2016 concerning amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions. With the ite law, it is hoped that it can protect the public of information technology users in Indonesia, this is important considering the increasing number of internet technology users from year to year. The increasing use of the internet on the one hand provides many conveniences for humans in carrying out their activities, on the other hand making it easier for certain parties to commit criminal acts, this technological advance also affects the lifestyle and mindset of humans, the fact is that there are currently many crimes using information technology. This rapidly developing phenomenon of cybercrime that knows no territorial boundaries should indeed be watched out for because this crime is somewhat different from other crimes in general.

The punishment carried out by law enforcement for illegal crimes of online banking access according to the author has not been effective, because the legal system in Indonesia requires criminals to go through a long process from investigation to punishment. This requires a legal breakthrough to prevent people from becoming perpetrators of online banking crimes or becoming people who help the perpetrators by providing Bank accounts to hold money from crimes as examples of cases have been described by the author. These precautions can be taken by related parties, from banking industry players to law enforcement itself.

References

Arief, B. N. (2001). Law Enforcement Issues & Crime Countermeasures Policies. Image of Aditya Bakti.

Arofah, N. R., & Priatnasari, Y. (2020). Internet Banking And Cyber Crime: A Case Study In National Banking. Indonesian Journal of Accounting Education, 18(2), 107–119.

Disemadi, H. S., & Prananingtyas, P. (2019). Legal protection for banking customers who use CRM (Cash Recycling Machine). Udayana Master's Journal of Law (Udayana Master Law Journal), 8(3), 286–402.

Electronic Transaction Law Number 11 of 2008, (2008).

Estradiyanto, N. (2012). "Protection for Bank Customers in the Use of Internet Banking Facilities for Cyber Crime in Indonesia." 4.

I Made Pasek Diantha. (2017). Normative Legal Research Methodology In Justification of Legal Theory (2nd ed.). Prenada Media Group.

Johnny Ibrahim. (2005). Normative Legal Research Theory and Methods. Stone Media.

Kompas. (, April). The source was accessed on April 5, 2021 at 21.00 WIB. 2021. https://nasional.kompas.com/read/2020/10/05/18440581/bareskrim-tangkap-10-tersangka-kasus-dugaanpengambilalihan-rekening-lewat

P.H, A. T. (2010). Cyber Crime in Criminal Law Perspectives. UMS.

Shah, M. et al. (2020). The Development Impact of PT. Medco E & P Malaka on Economic Aspects in East Aceh Regency. Budapest International Research and Critics Institute-Journal (BIRCI-Journal). P. 276-286.

Shahrullah, R, S. (2014). Juridical Review of Cybercrime Handling in the Indonesian and American Banking Sectors. Journal of Judicial Review, XVI(2).

Yulia, R. (2010). Victimology of Legal Protection of Victims of Crime. Graha Science.