Sibatik Journal
Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, dan Pendidikan
E-ISSN: 2809-8544

THE ROLE OF INVESTIGATORS OF THE CYBER DIRECTORATE OF THE REGIONAL POLICE NORTH SUMATERA IN HANDLING CRIMINAL ACTS IN THE FIELD OF BANKING THROUGH CYBER INTERMEDIARIES

Hendri Goklas Pasaribu[1]*, Alvi Syahrin[2], Robert[3]
University of North Sumatera, Indonesia
***Email Correspondence:** gloklas1983@gmail.com

Abstract
In line with the development of the times and the increasing development that is also inseparable from all aspects related to human life. Related to developments in people's lives for all existing problems, which are increasingly easy to solve or vice versa, there are also a small number of people who experience difficulties related to facing and meeting their needs. This has resulted in the rapid development of technology that is developing in society. Development at this level of technology will also have an impact on the impacts that occur in almost all aspects of human life, and will also change people's behavior, and human civilization, on the other hand, related developments in the field of technology have resulted in life in the world becoming limitless. Against the increasingly rapid technological advances, of course, it will have an impact in terms of positive or negative aspects. However, in line with the development of the times, the use of information technology has changed both in terms of people's behavior and those related to human civilization in general. With the advancement of technology, banking also follows technological developments, by creating applications that aim to provide convenience to customers so that in carrying out transactions in the form of checking and payments can be done using mobile banking and internet banking only by using a smartphone without having to come to the bank or to an ATM machine.

Keywords: Cyber Crime, Banking, Cyberspace.

INTRODUCTION

The development of information and communication technology has also created world relations that have no boundaries (borderless) and resulted in significant social, economic and cultural changes that will occur rapidly.

Along with the development of globalization, during the period of the fourth industrial revolution era, a new era has been created that is all digital and brings various complex implications in the life of the nation and state. The industrial revolution 4.0 is a self-upgrading phenomenon of globalization, seen from the rapid development of the digital world and the emergence of interdependence and the blurring of national boundaries (borderless). The definition of the industrial revolution 4.0 is an industry that unites automation with cyber. Through the development of technology, it can influence and have a major role in people's lives and have an influence on social, scientific, cultural, economic, political and legal developments.

Cyber crime is the term most often used by the entire society today. The word cyber is added to various terms to describe the form of society or new types of cyber-based crime, for example cyber society, cyber space, cyber attacks, cyber crime, cyber terrorism and others.

DOI: https://doi.org/10.54443/sibatik.v4i6.2788

The development of information technology or the internet has created a new world of cyber space, a computer-based communication world that offers a new reality, namely virtual reality. This is also called a term that produces a form of cyber space environment that gives birth to a new term, namely cyber crime. Before discussing further about the definition of cyber crime, it is necessary to combine opinions about what is meant by cyber crime. Can telematics crime be equated with computer crime or cyber crime and new types of crimes that are often known in technology and information literature. In the literature it is explained that what is called telematics crime is also called cyber crime. This is based on the argument that cyber crime is an activity that uses computers as a medium supported by a dial-up telecommunications system, using a telephone, or a wireless system using a wireless antenna.

Some experts argue that computer crime, cyber crime, and telematics crime are the same crime, only the names are different. The argument behind this is that initially computers were only used to collect and store data that could be used to commit conventional crimes, but in subsequent developments, computer crimes were also carried out via the internet such as Trojan horse hacking (Trojan horse virus), and data leakage (data leaks). The controversy over terminology does not create debate about the use of the terms used. Therefore, for reasons of consistency, the term often used is cyber crime.

Cybercrime is a form of virtual crime using a computer connected to the internet. Security holes in the operating system that cause weaknesses are exploited by hackers (skilled in using computers and internet networks), crackers (someone who is an expert at hacking), and script kiddies (amateur hackers) to infiltrate computers. According to Tavani, cybercrime is a crime in which criminal acts can only be carried out using cyber technology and occur in cyberspace.

Several experts have explained several types of digital crimes (Cyber Crime). According to Sunarto, there are five digital crimes (Cyber Crime) based on the type of activity, namely:

1. Unauthorized Access to Computer Systems and Services
   This crime is committed by illegally entering a computer network system without the owner's permission. The perpetrator's goal in doing this is to sabotage or steal important and confidential information.
2. Illegal Contents
   This crime is committed by entering incorrect, unethical, and illegal data or information into the internet. For example, hoax news, news that has the potential to disrupt public order and other types and invalid information.
3. Cyber Espionage
   This crime is aimed at spying on other parties by entering the system illegally.
4. Data Forgery
   This type is used by falsifying important data and documents stored as unscripted documents via the internet. This crime is aimed at online sales documents or e-commerce.
5. Cracking

DOI: https://doi.org/10.54443/sibatik.v4i6.2788

This type of crime is used to damage a computer system. The perpetrator commits theft or other acts when entering and gaining access to a computer system.

The development of increasingly sophisticated internet technology, especially in the field of information and electronics using computers and the internet. This progress is often accompanied by impacts that occur indirectly or directly. An example of the general negative impact of the development of information technology is the increasingly rampant expansion of information containing immoral acts of pornography, gambling, hoaxes, fraud, breaking into the banking system and so on, this is a serious threat from various groups, ranging from academics, law enforcement, Indonesian citizens, and the government. Cyber crime or often called digital crime in Indonesia itself has become a threat to the stability of public order and security with a fairly high escalation. This crime is not only committed in one area but several areas can even break through transnational and regional boundaries. To control, regulate and improve internet users, the government has passed Law Number 11 of 2008 concerning Information and Electronic Transactions. has been revised to Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions.

Cybercrime, leads to criminal activities by means of a computer system using the internet network as its main tool, the aim is to commit criminal acts. This is part of cybercrime which includes online auctions, check forgery, credit card fraud, illegal theft of customer data, fraud against someone's identity data and even breaking into banking data systems. The development of technology and its application has entered and strongly influenced modern life today, so that most of these business activities have entrusted modern technology, one of which is the banking industry.

With the advancement of technology, banking also follows technological developments, by creating applications that aim to provide convenience to customers so that in carrying out transactions in the form of checking and payments can be done using mobile banking and internet banking only by using a smartphone without having to come to the bank or to an ATM machine.

In this modern era, what is called a new legal regime called cyber law has emerged. Regarding the word cyber law, it is interpreted as an equivalent word derived from cyber law, which is currently used internationally as a legal term related to the use of information technology. Crimes in the field of cyberspace or commonly known as cyber crime basically lead to computer devices and technological tools that use systems connected to the internet as an element of their use. Advances in the field of information technology which are the origin of the emergence of cyber crime, will legally have both positive and negative impacts on the law itself. For cyber crime actions, due to the impact of the emergence of cyber crime, it will cause negative traits that will damage the field of modern life today, therefore advances in the field of computer technology will be one of the supporters of life in society of course. Developments in the field of technology and its application will enter and strongly influence the field of modern life today, even most business activities have used technology systems.

DOI: https://doi.org/10.54443/sibatik.v4i6.2788

The use of this internet network has created a new reality of life in terms of modern human civilization today. The internet has made distance and time no longer have limits. With the use of the internet medium, people can do various levels of activities that in real life would be difficult to do, due to differences in distance and time. A reality where at a distance of kilometers from where we are with people who are in distant places, with the use of the internet medium, the person will be able to appear in front of us. When the use of internet technology is growing rapidly, social media will also have an impact on rapid development.

In today's modern era, humans are inseparable from the use of social media. Social media is a type of media that is used for free media to express and explore the opinions we have continuously. On the other hand, social networks are pages where someone will create a web page (social media account) personally, and will be connected and can communicate with people they know or new people they know in cyberspace. Social networks used such as WhatsApp, Facebook, Twitter and so on. There are 2 (two) types of cybercrime, namely crimes where computers are targeted and crimes using computers and internet networks as a means, of the 2 (two) types of crimes that most often occur in banking, namely phishing, Skimming and malware.

Crimes using phishing, skimming and malware methods, which are crimes in the banking sector that result in financial losses to customer account holders, as explained that the definition of Phishing is a type of online fraud by tricking targets using fake website addresses with the intention of stealing target privacy data. Phishing comes from the English term Fishing, which means "fishing" here it is used to trap victims into providing information about the victim's personal banking data with a certain purpose. This can happen because some bank customers are less careful in providing personal data so that they experience phishing crimes which result in money from the customer's bank account being drained, this is an important concern for the government, banking and law enforcement officers in order to protect bank customers from cybercrime. Then another way the perpetrator commits fraud is by convincing the victim that the perpetrator is from the bank or another authorized party with the intention and purpose of being able to provide the customer's OTP code so that by obtaining the OTP code, the perpetrator freely takes money from the customer's account without the customer's permission or knowledge.

OTP or One Time Password is one of the security layers during online banking transactions. OTP has begun to be widely used in recent years along with the increasing popularity of digital banking and other digital financial transactions. The function of OTP itself strengthens the security layer of online financial transactions after PIN and password.

There are many ways that phishing criminals attempt to launch their crimes by committing online fraud using the OTP code mention mode which is generally common. The perpetrators randomly send broadcasts via WhatsApp, SMS, or email to potential victims with the mode of getting a prize draw or something else that attracts attention and makes the recipient of the message curious. This crime is termed phishing, the lack of knowledge of the victims regarding the importance of keeping personal data and OTP codes confidential from others, so that the perpetrators of the fraud can immediately use it to take

DOI: https://doi.org/10.54443/sibatik.v4i6.2788

over the victims' accounts or PINs. Then there are many more fraudulent methods carried out using the internet network and technology, one of which is the perpetrator pretending to be the owner of the goods advertised through the market place, then the perpetrator contacts and influences the owner of the goods to explain to the buyer of the goods that the perpetrator is the family of the owner of the goods where previously the perpetrator and the buyer of the goods had negotiated the price of the goods to be purchased and after the buyer of the goods met with the seller of the goods then because the price had been agreed upon with the fraudster then the buyer of the goods transferred money to the perpetrator's account without notifying the seller of the goods and after the transaction occurred when the buyer of the goods wanted to take the goods sold, it was stopped by the owner of the goods because the payment for the goods had not been received and when the buyer of the goods and the owner of the goods contacted the number of the fraudster it was no longer active, then this is also a crime in the banking sector using the internet network and electronic media involving banking.

Skimming crime is a method used by criminals in the banking sector to steal customer data contained in ATM cards, the mode is by attaching a skimmer tool to the slot/hole to insert the ATM card into the ATM machine where the perpetrator has placed a surveillance camera on the ATM machine to find out the PIN number of customers who are making transactions at the ATM machine, after the perpetrator obtains personal data or the customer's PIN number then the perpetrator uses a skimmer tool to duplicate the magnetic stripe data on the ATM card then clones it into a blank ATM card and after that the perpetrator is free to take money from the customer's account using the ATM that has been duplicated by the perpetrator.

In terms of banking crimes via computers and internet networks, the malware method is also very disturbing for internet banking users. In computer science terms, malware is a combination of 2 (two) English words, namely malicious and software, which means a program designed to disrupt computer operations, collect sensitive information or access computer systems without permission.

This malware method is carried out especially by hackers who intentionally carry out illegal actions to take someone's personal data, especially for Internet Banking users who are connected to the WhatsApp number belonging to their bank account, then the criminals use this opportunity to break into the customer's Internet Banking account.

One of the law enforcement officers authorized to conduct investigations and inquiries in relation to cybercrime is the Indonesian National Police. To conduct investigations into cybercrime, investigators in carrying out a series of actions are regulated according to the method in the Law which aims to seek and collect evidence with which the evidence sheds light on the crime that occurred and to find the suspect.

In addition to the role of the police in investigating cases of criminal acts of theft of money through cyberspace from customer accounts, of course the role of banking is also needed in terms of facilitating the investigation process, so that they can find out about customer data who are victims of criminal acts in the banking sector through cyberspace.

DOI: https://doi.org/10.54443/sibatik.v4i6.2788

As in Law No. 10 of 1998 concerning Banking, what is meant by banking is a business entity that collects funds from the public in the form of savings and distributes them to the public in the form of credit and/or other forms in order to improve the standard of living of the people. As is known, banking strictly maintains the confidentiality of its customers' data as stated in Article 40 of Law No. 10 of 1998 concerning Banking which states that banks are prohibited from providing information recorded in the bank regarding the financial condition and other matters of their customers, so that with the existence of an article regulating the confidentiality of customer data, the banking party does not provide personal data if it does not comply with the requirements stated in Law No. 10 of 1998 concerning Banking.

As is known, crimes using phishing, skimming and malware methods with bank customer accounts as the object are criminal acts in the banking sector because they use computers, internet networks and electronic media, provisions regulating crimes using computers, internet networks and electronic media

Based on data obtained from the Cyber Directorate of the North Sumatra Regional Police in 2024 there were 224 cases of phishing crimes, therefore this study is important because of the rampant cyber crime because the perpetrators' actions cause losses to victims, and the perpetrators of this cyber crime are also difficult to find because of the fast access to eliminate all existing evidence, as with phishing crimes because the perpetrators' access is so fast to eliminate existing evidence and the existence of laws that explain that for the benefit of justice in criminal cases, the minister can give permission to the police, prosecutors or judges to obtain information from the bank about the financial condition of the suspect / defendant by making a written letter at the request of the Chief of Police of the Republic of Indonesia, the Attorney General or the Chief Justice of the Supreme Court. with the background above, the researcher is interested in conducting research in the form of a scientific thesis with the following title, "The role of investigators of the Cyber Directorate of the North Sumatra Regional Police in handling criminal acts in the banking sector through cyberspace intermediaries".

Based on the background above, several problem formulations can be taken as follows:

1. What are the legal provisions regarding criminal acts in the banking sector via cyberspace?
2. What is the role of police investigators in handling banking crimes through cyberspace?
3. What obstacles do Indonesian Police investigators experience in handling banking crimes through cyberspace?

METHOD

The research method used to support the process of making this research is legal research supported by empirical data, where this legal research places law as a system of norms. the normative system in question is about the principles, norms, rules of laws and doctrines (teachings) and the nature of this research is descriptive analysis that examines laws and regulations. The research is also based on data sources, namely primary data

DOI: https://doi.org/10.54443/sibatik.v4i6.2788

sources and secondary data sources, primary data sources are data obtained directly at the research site so that primary data is also called basic data or empirical data, namely obtained through interviews in the room of the Cyber Directorate Investigator of the North Sumatra Police named AKP HENDRIK PRIBADI SAPUTRA, SH Position Panit 1 Unit 1 Subdit 2, then secondary data sources are data obtained from legislative materials, libraries or literature that are related to the object of research. In normative legal research, a qualitative approach method is used, not a quantitative one, because it does not use statistical figures, the qualitative approach provides descriptions in words of the findings and therefore prioritizes quality over data and not quantity.

RESULTS AND DISCUSSION

Provisions on Criminal Offenses in the Banking Sector via Cyberspace

There are two terms that are often used interchangeably, although their meaning and scope can be different. The first is Banking Crime and the second is Banking Crime. The first is the definition of Banking Crime is a crime that is solely committed by a bank or bank personnel, while the definition of Banking Crime has a broad meaning, namely a crime related to banking committed by outsiders or bank insiders who are threatened with the Banking Law and regulated in other regulations such as the Money Laundering Law, the Corruption Law, the Information and Information Technology Law and other laws.

Banking crimes called banking fraud are crimes committed in relation to the banking industry, both banking institutions, devices and products that can involve the banking party or its customers as perpetrators of the crime, the article referred to as banking crimes is in accordance with Article 51 of Law Number 10 of 1998 concerning banking which contains "Criminal acts as referred to in Article 46, Article 47, Article 47A, Article 48 paragraph (1), Article 49, Article 50, and Article 50A of Law Number 10 of 1998 concerning banking, which includes 13 (thirteen) types of criminal acts, the thirteen types of banking crimes are summarized into four types of crimes, namely:

a. Criminal acts related to licensing.
b. Criminal acts related to bank secrecy.
c. Criminal acts related to supervision and guidance.
d. Criminal acts related to banking business.

Then one of the cybercrimes in the banking sector is phishing, skimming and malware, which are crimes carried out using deceptive or fraudulent techniques, embezzlement and theft using computers and internet networks, damaging security systems and so on, therefore the application of criminal law against perpetrators of cyber crimes in the banking sector with the type of phishing crime (fraud or deception), is regulated in Article 45A of Law Number 1 of 2024 concerningThe second amendment to Law Number 11 of 2008 concerning electronic information and transactions states, "Any person who intentionally distributes and/or transmits Electronic Information and/or Electronic Documents containing false notifications or misleading information that results in material losses for consumers in Electronic Transactions as referred to in Article 28 paragraph (1) shall be punished with imprisonment for a maximum of 6 (six) years and/or a maximum fine

DOI: https://doi.org/10.54443/sibatik.v4i6.2788

of IDR 1,000,000,000 (one billion rupiah)" while the crimeskimming (installing a device in the mouth to insert an ATM card) and malware (illegal access or entering the system illegally)regulated in Article 51 Jo Article 35 of Law Number 11 of 2008 concerning Information and Electronic Technology which states that Any Person who fulfills the elements as referred to in Article 35 shall be punished with imprisonment for a maximum of 12 (twelve) years and/or a maximum fine of Rp. 12,000,000,000.00 (twelve billion rupiah) jo Any Person who intentionally and without rights or against the law manipulates, creates, changes, removes, destroys Electronic Information and/or Electronic Documents with the aim that the Electronic Information and/or Electronic Documents are considered as if they were authentic data..

So the elements contained in Article 45A of Law Number 1 of 2024 concerning the second amendment to Law Number 11 of 2008 concerning the second amendment to Law Number 11 of 2008 concerning electronic information and transactions read: Any person who intentionally distributes and/or transmits Electronic Information and/or Electronic Documents containing false notifications or misleading information that results in material losses for consumers in Electronic Transactions as follows:

1) Elements of every person
   Every person referred to is a person as a legal subject who can be held responsible and legally competent based on legislation.
2) Deliberately
   The intention or deliberate and full awareness of a person in carrying out an unlawful act.
3) Distributing and/or transmitting Electronic Information and/or Electronic Documents containing false notices or misleading information that results in material losses.
4) Consumer.
   Based on Law Number 8 of 1999 concerning Consumer Protection, a Consumer is any person who uses goods and/or services available in society, whether for the benefit of themselves, their family, other people, or other living creatures and not for trading.

Meanwhile, the elements stated in Article 51 Jo Article 35 of Law Number 11 of 2008 concerning Information and Electronic Technology which reads: Any Person who fulfills the elements as referred to in Article 35 shall be punished with imprisonment for a maximum of 12 (twelve) years and/or a maximum fine of Rp12,000,000,000.00 (twelve billion rupiah) jo Any Person who intentionally and without rights or against the law manipulates, creates, changes, removes, destroys Electronic Information and/or Electronic Documents with the aim that the Electronic Information and/or Electronic Documents are considered as if they were authentic Electronic data as follows:

1) Elements of every person
   Every person referred to is a person as a legal subject who can be held responsible and legally competent based on the Law.
2) Without rights or against the law
   The act was carried out without permission and the law has come into force which regulates prohibited acts.

DOI: https://doi.org/10.54443/sibatik.v4i6.2788

3) Manipulating, creating, changing, removing, destroying Electronic Information and/or Electronic Documents with the aim that the Electronic Information and/or Electronic Documents are considered as if they were authentic Electronic data. Acts of manipulating, creating, changing, removing, destroying information or security systems are aimed at seeking profit.
4) Authentic Electronic Data
   Creating data that is actually incorrect.

Thus, the positive legal provisions that regulate cyber crime in the form of phishing are stated in Law Number 01 of 2024, Article 45 A.1 of 2024 concerningthe second amendment to Law Number 11 of 2008 concerning electronic information and transactions, then the provisions of the laws and regulations for perpetrators of cyber crime in the form of skimming and malware are regulated in Article 51 Jo Article 35 of Law Number 11 of 2008 concerning Information and Electronic Technology and to fulfill the provisions in the laws and regulations must have 2 (two) pieces of evidence in accordance with Article 183 of Law Number 8 of 1981 concerning Criminal Procedure Law.

The role of directorate investigatorsNorth Sumatra Police Cyberin handling criminal acts in the banking sector through cyberspace.

The police are one of the government institutions that play an important role in the State, especially for a State based on law, in the law of the State the legal life is very much determined by the structural factor or legal institution. In line with this, Soejorno Soekanto argues that law and law enforcement are law enforcement factors that cannot be ignored, if ignored will cause the expected law enforcement not to be achieved.

Based on Article 5 paragraph (1) of Law Number 2 of 2002, Article 5 paragraph (1) concerning the Republic of Indonesia National Police, which states "The Republic of Indonesia National Police is a state apparatus that plays a role in maintaining public security and order, enforcing the law and providing protection, patronage and services to the public in the context of maintaining domestic security."

The police are one of the leading parties that have an important role in overcoming every occurrence of criminal acts, one of the police's efforts to maintain public security and order, enforce the law and provide protection, shelter and service to the community through preventive and repressive efforts. According to Barda Nawawi Arief, efforts to overcome through non-penal channels can be called efforts made through channels outside of criminal law. This effort can be done by implementingsocial assistance and education in order to develop social responsibility of community members; development of community mental health through moral, religious, and other education; increasing child and adolescent welfare efforts; and ongoing patrol and other surveillance activities by the police. Meanwhile, Repressive efforts, according to Barda Nawawi Arief, efforts to overcome through the penal path are called efforts carried out through criminal law, these efforts are actions taken after a crime has occurred by enforcing the law and imposing penalties for crimes that have been committed.

DOI: https://doi.org/10.54443/sibatik.v4i6.2788

The preventive efforts carried out by the North Sumatra Police cyber investigators related to criminal acts in the banking sector through cyberspace include providing socialization to the public, both face-to-face and through social media, so that they do not easily trust someone they do not know who then asks for an OTP code number, transfers money for buying and selling or other things that are considered to be profitable for the perpetrator.

Meanwhile, the repressive efforts carried out by cyber investigators of the North Sumatra Police regarding criminal acts in the banking sector through cyberspace based on legislation play a role in enforcing the law in accordance with Law Number 1 of 2024 concerning the second amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions Information and other applicable laws and regulations. The role of the North Sumatra Police Cyber Investigator is to seek or find the truth in a criminal act since the case process begins from the investigation and inquiry stage because this is the beginning of the process of finding and collecting facts for proof, the law enforcement process cannot be separated from the role of the North Sumatra Police Cyber Investigator to prove or collect as much evidence and evidence as possible with the aim of obtaining or finding suspects who have committed crimes in the banking sector through cyberspace which is in accordance with Article 183 of Law Number 8 of 1981 concerning Criminal Procedure Law which reads: A judge may not impose a sentence on a person unless with at least two valid pieces of evidence he obtains the conviction that a crime actually occurred and that the defendant is guilty of committing it, thus the role of the investigator must be able to collect as much evidence as possible to convince the judge that the person is the perpetrator of the crime.

In handling cyber crime in the banking sector, the North Sumatra Police Cyber Investigator has referred to positive laws and regulations, the role of the North Sumatra Police Cyber Directorate investigator has carried out stages, namely investigations to the investigation stage in accordance with laws and regulations, Investigators have the authority that has been regulated in the Criminal Procedure Code and Law Number 2 of 2002 concerning the Republic of Indonesia National Police, but in the investigation process that is carried out it cannot run easily and smoothly because of the laws and regulations governing permission to obtain customer data, the Police investigator must obtain approval from the Financial Services Authority after that coordinate again with the bank by attaching the permit granted by the Financial Services Authority, which can slow down the investigation process and can provide space for perpetrators of cyber crime in the banking sector to remove evidence or remove their identity without their whereabouts being known. So the role of the Police investigator who has the authority in law enforcement is essentially a process in the criminal justice system, therefore it is closely related to applicable laws and regulations and continues to comply with laws and regulations.

Obstacles experienced by Indonesian Police investigators in handling banking crimes through cyberspace

A. Substantial Barriers

1. Bank Confidentiality

DOI: https://doi.org/10.54443/sibatik.v4i6.2788

Bank financial institutions are known for their very strict confidentiality principles, this is regulated in article 1 paragraph 28 of Law Number 10 of 1998 concerning banking which states "Bank secrecy is everything related to information about deposit customers and their savings" this article expressly regulates bank secrecy, namely everything related to financial information or customer identity. The development of the era and technological advances have increased criminal acts, especially in the banking sector, including cyber crime in the form of phishing, skimming and malware, the involvement of law enforcement officers such as the Police is needed to uncover criminal acts in the banking sector with crimes in the form of investigations, this is emphasized as in Law Number 8 of 1981 concerning Criminal Procedure Law which is described in detail in article 1 paragraph 2 that investigation is a legal process carried out by investigators by collecting evidence to indicate ongoing criminal acts and to reveal the perpetrators.

The investigation process carried out at the Cyber Directorate of the North Sumatra Police in terms of collecting evidence and finding suspects is often not in line with or is hampered by the existence of bank confidentiality regulations, these obstacles include difficulties in obtaining information regarding customer personal data or complete identities of customers registered with banks and customer transactions that have been carried out by someone who is related to criminal acts in the banking sector through cyberspace with phishing, scimming and malware crimes. To obtain permission regarding customer data, the North Sumatra Police Cyber Investigator is required to receive a permit to open customer data from the Central Financial Services Authority, this is in accordance with Law Number 4 of 2023 Chapter IV Article 42 concerning the Development and Strengthening of the Financial System which reads:

a) In the interests of the trial in criminal cases as referred to in Article 40A paragraph (1) letter b, the Financial Services Authority has the authority to grant permission to the police, prosecutors, judges or other investigators who are authorized under the Law to obtain information from banks regarding the savings of suspects, defendants, convicts or other parties related to suspects, defendants or convicts.
b) The permit as referred to in paragraph (1) is given in writing upon written request from:
    1) The Chief of the Indonesian National Police, the Chief of the Criminal Investigation Agency of the Indonesian National Police, or the Chief of the Regional Police in the case of a request submitted by an investigator from the Indonesian National Police.
    2) Attorney General, Deputy Attorney General, or Head of the High Prosecutor's Office in the case of a request submitted by an investigating prosecutor and/or public prosecutor.
    3) Chief Justice of the Supreme Court, Chief Justice of the High Court or Chief Justice of the District Court.

DOI: https://doi.org/10.54443/sibatik.v4i6.2788

4) The head of an agency who is authorized to conduct investigations or a position one level below the head of an agency who is authorized to conduct investigations.

In order to fulfill mutual assistance in criminal matters as referred to in Article 40A paragraph (1) letter g, the Financial Services Authority may grant permission to the police or prosecutors to obtain information from the Bank based on the Law regarding reciprocity in criminal matters.

The permit as referred to in paragraph (3) is given in writing upon request from the Chief of the Republic of Indonesia National Police or the Attorney General or an appointed official at his/her agency.

The request as referred to in paragraph (4) must state:

a. Name and position of police or prosecutor
b. The name of the relevant party requested and
c. A description that the request for assistance relates to an investigation, prosecution and examination in a court of law in the requesting State and his status as a suspect or witness as referred to in the Law on mutual assistance in criminal matters.

After the North Sumatra Police Cyber Investigator received a letter of permission to receive customer personal data from the Central Financial Services Authority, the North Sumatra Police Cyber Investigator then wrote a letter to the bank that owns the customer's account regarding a request for permission for customer personal data and customer transactions by attaching a letter of approval from the Central Financial Services Authority.

Bank secrecy policies are considered rigid and limited, which can hinder obtaining customer data or transactions related to criminal acts. The Financial and Development Supervisory Agency's view is that "Bank secrecy is a rule that makes it difficult to reveal information about a person's bank account, this can be an obstacle in efforts to stop crime, some even say that bank secrecy can be a 'shield' used to hide money from crime by perpetrators of criminal acts."

2. Lack of specific regulations regarding criminal acts in the banking sector via cyberspace.

Indonesia as stated in Article 1 paragraph 3 of the 1945 Constitution of the Republic of Indonesia firmly states that "The State of Indonesia is a State of Law", so that by implementing laws in the midst of society in a country, it becomes easier to achieve the goals of life for the community itself, namely living safely and peacefully.

To handle cybercrime in the form of phishing, the North Sumatra Police Cyber Investigator applies Article 45A of the Republic of Indonesia Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions which reads "Any person who intentionally distributes and/or transmits Electronic Information and/or Electronic Documents containing false notifications or misleading information that results in material losses

DOI: https://doi.org/10.54443/sibatik.v4i6.2788

for consumers in Electronic Transactions as referred to in Article 28 paragraph (1) shall be punished with imprisonment for a maximum of 6 (six) years and/or a maximum fine of IDR 1,000,000,000 (one billion rupiah), but in Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions there is no article that gives authority to Law Enforcement Apparatus in this case the Republic of Indonesia National Police to explicitly be able to easily receive customer data information from banks in the region without having to go through the procedures that have been regulated in Law Number 4 of 2023 Chapter IV concerning the Development and Strengthening of the Financial System.

Then, because the development of information technology has other impacts such as the emergence of new crimes known as cyber crime, the definition of cyber crime is more of a general crime that has characteristics carried out by parties who master the use of information technology such as computers, mobile phones and the internet, one of the crimes that utilizes online media is the type of phishing crime which is the same as fraud.

Cybercrime of phishing type handled by North Sumatra Police Cyber Investigator; the perpetrators often use mobile phones to communicate with victims. Mobile technology in Indonesia has evolved several times so that currently at the level of fourth generation mobile technology (4G), which is able to provide customers with high data speeds than before so that it can provide communication services based on voice, images, text and internet-based services. Not inferior to the development of mobile technology and mobile phone devices, the growth in the number of mobile customers in Indonesia is also increasing.

The need for regulations to regulate and require customers to register customer data when activating cellular services on prepaid SIM cards has been implemented in 2005, in accordance with the Regulation of the Minister of Communication and Information Number 23 of 2005, however, this regulation has not been able to reduce and stop criminal acts through cellular services because the obligation to register personal data listed in the civil registry office has not been implemented because every kiosk or package card provider has accepted it without the need for prior registration so that the use of the package card is registered using other people's personal data.

The development of cellular technology has two sides, namely being used for positive things and being used for negative things, in 2024 the Cyber Directorate of the North Sumatra Police has received 224 cases of fraud using cellular phones, so that the Cyber Investigators of the North Sumatra Police have difficulty determining the actual owner of the number used in phishing crimes, because the personal data stored on the operator does not match the user data.

Therefore, due to the rampant criminal acts of phishing using mobile phones and package cards which are considered disturbing and have claimed many victims with varying amounts of losses, a new regulation is needed, namely the

DOI: https://doi.org/10.54443/sibatik.v4i6.2788

implementation of validation and verification of the use of package cards by filling in the personal data of each user using the Population Identification Number registered with the Civil Registry Office which aims to make it easier to find perpetrators of cybercrime in the form of phishing.

B. Structural Barriers

1. Limitations of Forensic Tools

The Indonesian National Police, especially the North Sumatra Regional Police, in receiving reports from the public about cybercrime in the form of phishing where the perpetrators and victims often communicate using the WhatsApp application because WhatsApp is one of the most popular communication platforms among the global community and this application offers to carry out the investigation and investigation process, especially handling cybercrime in the form of phishing using mobile phones or what is commonly known as cellphones still use equipment with various features such as text, voice calls, video calls and chat groups that make it easier to interact between users, misuse of WhatsApp in digital crimes often involves efforts by perpetrators to delete traces of their communication, features such as (Disappering Message) and single-view media allow messages and media to disappear automatically after being viewed for a certain period of time, although this feature is designed to improve user privacy, perpetrators can take advantage of this feature to eliminate traces of digital evidence that aims to complicate the investigation or investigation process carried out by Law Enforcement Officers.

Starting from the perpetrator who communicated with the victim using WhatsApp messenger activating the temporary message feature and sending photos. However, within a certain period of time without the need to delete the conversation message will be deleted automatically, in the limited conditions of the Law Enforcement Apparatus devices in this case the Indonesian National Police using the National Institute of Standards and Technology (NIST) method, which provides a systematic framework in the digital forensics process. So with this approach investigators can ensure that the procedures carried out are in accordance with standards and procedures so that the evidence obtained has legal validity and can be used in the trial process and the NIST method also allows optimization of data acquisition techniques and can trace digital traces to support the effectiveness of the investigation.

In the process of investigating the victim's cell phone, confiscation is usually carried out with the aim of being able to examine data related to the reported crime, so that cellular evidence is investigated using the NIST method. The NIST method has 4 stages, namely the Collection stage, the Examination stage, the Analysis stage and the Reporting stage.

The next stage is the report obtained with digital evidence to be used as evidence supported by the authenticity of the evidence. However, the digital forensic tools discussed above are still minimal in the North Sumatra Regional Police, with

DOI: https://doi.org/10.54443/sibatik.v4i6.2788

the rampant cyber crime in the form of phishing, skimming or malware, the government should be able to provide the most advanced forensic analysis tools such as data tracking software and digital deleted data recovery tools to help collect evidence related to phishing crimes aimed at proving the trial stage.

2. Human Resource Limitations

Cybercrime has become one of the most complex and dynamic forms of crime in Indonesia, especially in today's digital era, philosophically, cybercrime tests the principle of substantive justice in law, demanding the legal system to protect individual rights while ensuring the stability of society in an ever-evolving digital order. From a legal perspective, although Law Number 1 of 2024 concerning the second amendment to Law Number 11 of 2008 concerning electronic information and transactions has provided a legal basis for dealing with cybercrime, the limitations of human resources in the evidence process are not the same as conventional crimes.

Cyber Investigators of the North Sumatra Police face various technical obstacles that can hinder the effectiveness of the law enforcement process, including limited human resources, namely not having special expertise in the field of digital forensics. There are still many investigators who are not equipped with sufficient knowledge or training to handle digital evidence, such as activity log analysis, IP address tracking or encrypted data decryption because in the law enforcement process, evidence that has been regulated by law is needed, so investigators need expertise to dismantle the complex system used by cyber perpetrators.

C. Cultural Barriers

1. Changes in crime mode

Internet technology has been used in various aspects of life and one of them is the banking world with internet banking technology is a form of internet media utilization by banks to promote and at the same time conduct online transactions both from conventional and the latest products. Internet banking facilities that provide many benefits of convenience for customers such as cost reduction, market expansion and increased service speed, give rise to new types of crimes both traditional organized crimes and cyber security violations using computer and internet media. Where these crimes are known as cyber crimes. According to Fuady, there are various versions of cybercrime such as hackers, people who are experts and master computers, like to study the ins and outs of computer systems and experiment with them to then infiltrate the communication network of an institution in cyberspace, Crackers are the dark side actions of a hacker who illegally infiltrates and destroys sites, websites, and internet network security systems to gain pleasure and profit, Cardera is a person who cracks credit cards to steal other people's card numbers and use them for personal gain, Deface is an act of infiltrating a site and then changing the appearance of the site page with a specific purpose, Phreaker is a

DOI: https://doi.org/10.54443/sibatik.v4i6.2788

person who cracks the telephone network, so that they can make free calls to any area they want.

With the advancement of technology today, especially the perpetrators of cybercrime who have the ability to do evil either by committing fraud, surveillance or even breaking into the system that has been created with the aim of benefiting themselves. Although law enforcement officers have attempted to prevent perpetrators of cybercrime, cybercrime perpetrators continue to try to change the method or form so that it can be difficult for law enforcement officers to prove it, this can be said because there are still complaints received at the police station in each region regarding cybercrime.

2. Lack of public trust

Information and communication technology continues to experience very rapid development, with information and communication technology actions that occur in the real world can now easily occur. Cyber crime is a crime using technology such as computers and internet networks, many cyber crimes that occur have harmed many people.

Although the Law on Information and Electronic Technology is a regulation that regulates cybercrime, law enforcement officers who have the authority to prove the perpetrators of cybercrime and continue to the prosecution stage still experience many obstacles, such as the existence of a law that regulates the granting of bank customer data permits which takes a long time in the process, then the limitations of the latest digital tools owned by the police, especially the Cyber Directorate of the North Sumatra Police and knowledge of using digital tools which are very useful for evidence in the investigation process that has validity in accordance with laws and regulations, resulting in public distrust of the police in the investigation process.

CLOSING

Conclusion

1. The legal provisions for criminal acts in the banking sector through cyberspace intermediaries in Indonesia, especially phishing crimes, are regulated in Law Number 01 of 2024, Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions, Article 45A, which reads "Any person who intentionally distributes and/or transmits Electronic Information and/or Electronic Documents containing false notifications or misleading information that results in material losses for consumers in Electronic Transactions as referred to in Article 28 paragraph (1) shall be punished with imprisonment for a maximum of 6 (six) years and/or a maximum fine of IDR 1,000,000,000 (one billion rupiah).
2. Investigation is part of the Criminal Justice System or is a process of enforcing criminal law, therefore it is closely related to applicable laws, the criminal justice system is a system in a society to deal with crime problems, the institutions in a criminal justice system are the Police, Prosecutors, Judges and correctional institutions, in terms of the

DOI: https://doi.org/10.54443/sibatik.v4i6.2788

Police who have the authority as investigators to conduct investigations into all criminal cases. The role of the Cyber Directorate Investigator of the North Sumatra Police in handling criminal acts in the banking sector through cyberspace after receiving a police report which then conducts an investigation aimed at finding out whether the incident is a criminal act or not a criminal act, then the Cyber Directorate investigator of the North Sumatra Police conducts an investigation aimed at collecting evidence, collecting evidence and finding the perpetrators of the crime, but the efforts made are considered hampered by the existence of Law Number 4 of 2023 Article 42 Chapter IV concerning the Development and Strengthening of the Financial System because investigators are required to wait for permission from the Financial Services Authority and banking later.

3. The obstacles faced by the North Sumatra Police Cyber Directorate Investigators in handling cyber crime in the banking sector are broadly divided into 3 (three), namely:
   a) Substantial Obstacles, namely bank confidentiality, are everything related to customers, both personal data and customer accounts, the bank's obligation to keep its customer data confidential is regulated in the Banking Law and the regulation on obtaining customer data related to criminal acts, National Police investigators are required to obtain permission from the Financial Services Authority as regulated in Article 42 Chapter IV of Law Number 4 of 2023 concerning the Development and Strengthening of the Financial System, then obstacles due to the lack of specific regulations regarding criminal acts in the banking sector through cyberspace, namely because there are no regulations governing the activation of internet cards because as is known, to activate an internet card, consumers do not need to register first because the internet card can be used directly because it has been registered with other people's personal data.
   b) One of the structural obstacles is the limited forensic tools owned by the Cyber Directorate of the North Sumatra Regional Police, even down to the Polsek level because digital tools are an important part of revealing or clarifying a criminal event. Then, the obstacle of limited human resources is also something experienced in the Cyber Directorate of the North Sumatra Regional Police, even down to the Polsek level because of the limited digital forensic tools owned, so that knowledge to use digital forensic tools is very limited and there is a lack of understanding regarding forensic data in relation to digital evidence that can be submitted to court.
   c) Cultural Barriers, one of which is the change in crime modes that are difficult to anticipate, is also one of the obstacles experienced, because the perpetrators of these crimes always change their crime methods, either from words that can convince or send data in the form of invitations or website addresses that resemble institutions or institutions, while the obstacle of lack of public trust is due to several factors, namely the length of time to handle criminal acts due to obtaining permits from the Financial Services Authority and obtaining permits from banks, then other causal factors due to the lack of digital tools owned so that the handling of criminal acts in the banking sector through cyberspace is not optimal.

DOI: https://doi.org/10.54443/sibatik.v4i6.2788

Suggestion

1. In terms of cyber crime in the form of phishing and malware has been regulated in Law Number 1 of 2024 concerning the second amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions, it is recommended to the government that the Information and Electronic Transactions legislation has an article that regulates the authority of the Indonesian National Police to be able to receive or obtain personal data information of customers directly from banks in each region. Then to reduce cyber crime in the form of phishing, the government through the Ministry of Communication and Digital is advised to regulate the use of package cards or cards used for the internet which are currently sold freely because without having to register first to activate the package card, the Ministry of Communication and Digital makes new regulations regarding the activation of package cards that must be filled in using the personal data of each registered user which aims to make it easier to find out the user's package card number.
2. Investigators have the authority to conduct investigations and inquiries in handling criminal acts including cybercrimes. Investigation is a process in the criminal justice system that aims to shed light on criminal events, so it is recommended that investigators be given the convenience of obtaining customer data without having to follow the laws governing the granting of customer data permits.
3. In connection with the law enforcement process, the Police must be able to prove the perpetrators of cyber crimes, namely by collecting evidence and digital evidence forensically, it is proposed to the government to procure advanced/sophisticated forensic equipment in large quantities for the purpose of being used in the investigation process at the Cyber Directorate of the North Sumatra Police to the Polsek level.

REFERENCES

Adytama, Ryan, “Penegakan Hukum Cyber Crime Pada Tindak Pidana Pencurian Uang Nasabah Dengan Cara Pembajakan Akun Internet Banking Lewat Media Sosial”, Jurnal Vol 5 Nomor 1 Tahun 2021.

Ahmad M. Ramli, 2008, Tinjauan Cyber Law serta terkait dengan Haki, Bandung, Sinar Grafika.

Alamsah D. Nandang H, dkk, Teori dan praktek kewenangan pemerintahan, (Penerbit Pandiva buku, November 2017) hal 4.

Agus Sallam dkk, 2022, Tindak Pidana Kejahatan UU ITE, Jakarta: Guepedia.

Arief, Barda Nawawi, 2010, Penanggulangan Terhadap Tindak Pidana Pada Kejahatan DiBidang Telematika Dan Informatika, Jakarta, Budi Utama.

Atmasasmita, Romli, 1996, Sistem Peradilan Pidana (Criminal Justice Sistem) Perspektif Eksistensialisme Dan Abolisionalisme, Jakarta, Penerbit Bina Cipta.

Atmasasmita, Romli, 2013, “Sistem Peradilan Pidana Kontemporer”, Jakarta, Kencana.

Ayu Anggriani dan Ridwan Arifin, “Tindak Pidana Kesusilaan Dalam Kaitannya Dengan Kejahatan Mayantara Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik Di Indonesia”, Jurnal Trisakti.

Chazawi, Adami, 2015, Prija Djatmika, dan Ardi Ferdian, Tindak Pidana Pers: Penyerangan Terhadap Kepentingan Hukum Yang dilindungi Dengan Mempublikasikan Tulisan, Bandung, Mandar Maju.

Dara Sawitri, Revolusi Industri 4.0: Big menjawab tantangan Revolusi 4.0, Jurnal Ilmiah Maksitek vol. 4 No 3, hal. 2.

Dista Amalia Arifah, "Kasus Cybercrime di Indonesia (Indonesia's Cybercrime Case)", Jurnal Bisnis dan Ekonomi (JBE), Vol. 18, No. 2, 2011.

Ediwarman, 2016, Monograf Metode Penelitian Hukum Panduan Skripsi, Tesis dan Disertasi, Yogyakarta, Genta Publishing.

Edy Prabowo, membuka rahasia bank sebagai tindak pidana dan implikasinya terhadap berlakunya perppu Nomor 1 tahun 2017 tentang akses informasi keuangan untuk kepentingan perpajakan, Lex Crimen, Vol VIII, 2018. Hal 13.

Eka Pradnyaswari, Ida Ayu, I Ketut Westra, "Upaya Perlindungan Hukum Bagi Konsumen Dalam Transaksi Jual Beli Menggunakan Jasa E-Commerce", Jurnal Kertha Semaya Fakultas Hukum Universitas Udayana, Vol. 5 No. 8 (2020).

Fadly Adrianto, Kepastian Hukum dalam Politik Hukum Indonesia, Jurnal Administrasi Low & Governance, Vol 3, 1 Maret 2020. hal 1.

Friedman, Lawrence M, 1975, The Legal System: A Social Science Perspective. New York: Russel Sage Foundation.

Fuady Munir, Teori – Teori besar (grand Theory) dalam hukum, (Penerbit Kencana Prenadamedia Group, Agustus 2014) hal. 92.

Hasan Ichsan Nurul, Jakarta, 2014, Pengantar Perbankan, Referensi (Gaung Persada Press Group).

Hanah Faridah, jenis-jenis tindak pidana perbankan dan perbandingan Undang-Undang perbankan, Jurnal hukum fositum, vol 3, 2018, hal 111.

H. Salim HS., Erlies Septiana Nurbani, Penerapan Teori Hukum pada Panelitian Tesis dan Disertasi, (Penerbit PT RajaGrafindo Persada, Agustus 2022), hal. 183.

Ika Dwi Purwaningsih dkk, Tinjauan tentang prinsip kerahasiaan Bank untuk melindungi nasabah berdasarkan hukum positif di Indonesia (Jurnal Yustisiabel, Vol 5, 2021) hal 163.

Isharyanto, 2016. Teori Hukum Suatu Pengantar Dengan Pendekatan Tematik, Jakarta, WR Penerbit.

Kitab Undang-Undang Hukum Pidana.

Marnia Rani, perlindungan otoritas jasa keuangan terhadap kerahasiaan dan keamanan data pribadi nasabah bank, Jurnal Selat, Vol 2, 2014, hal 174.

Maskun dkk, 2020, Korelasi Kejahatan Siber dan Kejahatan Agresi dalam Perkembangan Hukum Internasional, Makassar: Nas Media Pustaka.

Moljatno, Asas-Asas Hukum Pidana, 2008, Jakarta, Rineka Cipta.

Muhammad Khairul Faridi, kejahatan siber dalam bidang perbankan, jurnal Vol. 1, No. 2, November 2018, hal. 58.

Murio Julyanto, dkk, Pemahaman terhadap Asas Kepastian Hukum melalui Konstruksi Penalaran Positivisme Hukum, Jurnal Crepido, Vol 01, 01 Juli 2019, hal. 13.

DOI: https://doi.org/10.54443/sibatik.v4i6.2788

Nasution, Bahder Johan, 2008, Metode Penelitian Ilmu Hukum, Bandung, Mandar Maju.

Raodia, Pengaruh perkembangan teknologi terhadap terjadinya kejahatan mayantara, jurisprudentie, vol 6, 2019, hal 233.

Saleh, Roselan, 1981, perbuatan pidana dan pertanggungjawaban pidana: Dua Pengertian Dasar Dalam Hukum Pidana, Jakarta, Aksara Baru.

Sahat Maruli Tua Situmeang, 2020, Sistem Hukum Indonesia Komponen Substansi Hukum & Kelembagaan Peradilan Pidana, Bandung, Logoz Publishing.

Sugiarto R, 2012, Sistem Peradilan Pidana Indonesia dan Sekilas Sistem Peradilan Pidana di beberapa Negara, Semarang, UNISSULA PRESS.

Soekanto, Soerjono, 2014, Pengantar Penelitian Hukum, Universitas Indonesia, UI- Press.

Sri Wulandari, kebijakan hukum pidana dalam penanggulangan tindak pidana di bidang perbankan, Jurnal hukum dan dinamika masyarakat Vol 19, 2021, hal 171.

Sukendar, dkk, Teori Hukum suatu pengantar, (Banguntapan Bantul, Penerbit Pustakabarupress, 2022) hal 118.

Yanuar, Afdal Muh, Jakarta 2023, Kencana, Kerahasiaan Bank dan Anti-Tipping Off.

Yuli Purwanti dkk, Upaya Penanggulangan Tindak Pidana Penipuan Dengan Metode Phising Oleh Kepolisian Lampung, Jurnal, Vol. 2. Nomor 1, Tahun 2023.