THE CRIMINAL LIABILITY FOR ILLEGAL BANKING ACCESS WHICH HARMS STATE FINANCES

Ridho Syahputra Manurung
Universitas Pembinaan Masyarakat Indonesia, Medan, Indonesia
doktorridho80@gmail.com

Abstract

The misuse of developments in information technology has in fact given rise to a new mode of theft crime, namely the development of theft by certain parties who use electronic means. The purpose of this research is to know and analyze the Scope of Cyber Crime by accessing electronic banking systems that harm the Bank's finances, Legal Protection for Banks That Suffer Losses Due to Actors Accessing the Bank's Electronic System, Criminal Liability for Cyber Crime Actors By Accessing Electronic Banking Systems That Harm State Finances. The research method used is library research (library study), in legal research the normative juridical approach method or library law. This crime is often perceived as a crime committed in the cyber area. The mode of operation of this crime continues to develop, along with technological developments. Crimes that arise as a result of the misuse of technological advances are cyber crimes by accessing electronic systems. Cyber Crimeas a crime that uses computer technology as the main component which is very detrimental and disturbing to society is a form of crime found in the mass media, namely all kinds of use of computer networks. Electronic Information and Transactions in the form of cellphones, laptops, internet. Because of this, Cyber Crime is often a reported modes of operation also vary, ranging from fraudulent sales of goods, embezzlement, fraud through stock investment, hijacking customers' ATMs and so on.

Keywords: *Banking; Cyber; Crime; Illegal.*

A. INTRODUCTION

The development of the world towards globalization has encouraged the Indonesian state to adapt itself so that it can compete with countries on the international stage,[1] in order to face the development of the national economy which is always moving fast, competitive and integrated with increasingly complex challenges and an increasingly fast financial system. Therefore, policy adjustments in the economic sector, including banking, are needed. Current developments in the national economy show a direction that is increasingly integrated with the regional and international economy, which can both support and have less favorable impacts. Meanwhile, national economic development continues to move rapidly with increasingly complex challenges.[2]

1 Gomgom TP Siregar,. The Law Globalization In Cybercrime Prevention, *IJLR: International Journal of Law Recontruction*, Vol. 5, No. 2, September 2021, page. 211-228

2 Djoni S. Gazali and Rachmadi Usman., *Banking Law*, Jakarta, Sinar Grafa, 2012, page. 10

On the other hand, there is also the development of technological expertise and information which has implications for social change which creates a modern society. This is in accordance with the opinion of Satjipto Raharjo who states that in human life there are many factors that can be put forward as triggers for changes in society. The internet belongs to everyone in the world. Every person or institution can freely connect their computer to the internet.[3]However, in changes in the implementation of the results of modern technology today, many people are cited as one of the reasons for social change, technological sophistication is recognized as providing convenience, especially in helping human work. Apart from that, the development of computer technology has led to the emergence of new crimes, namely by utilizing computers as their mode of operation.[4]

One of the crimes that arises as a result of the misuse of technological advances is cyber crime by accessing electronic systems (without rights and against the law accessing electronic and computer systems) belonging to banks which is detrimental to the bank's finances. A bank is a financial institution that is a place for storing funds owned by individuals, state-owned enterprises and privately-owned enterprises, as well as other government institutions. Issues regarding banks in Indonesia are regulated in Law No. 7 of 1992 concerning Banking as amended by Law No. 10 of 1998 concerning Banking[5]From a legal perspective, the development of information technology and its use has its own consequences, namely the emergence of various deviations or actions that lead to criminal acts or new crimes.[6]

Cybercrime has developed into a transnational criminal act, a criminal act that does not recognize jurisdictional boundaries, in an effort to escape legal prosecution for criminal acts that have been committed. Cybercrime even results in legal problems between a country and another country, making it difficult to overcome and eradicate it without cooperation and harmonization of policies with other countries.[7]

The phenomenon of cyber crime must be watched out for. Considering that these crimes can be committed without recognizing territorial boundaries and there is no need for direct interaction between the perpetrator and the crime victim. The use of a global internet system means that cybercriminals in all countries can of course access the internet, so that all countries and the global community can potentially become victims of these crimes. Today's cyber crime levels of vulnerability and losses have exceeded the real world. The Interpol chief predicts that cybercrime will emerge as the biggest criminal threat and that the current problems show a

3 Maskun, Cyber Crime., *Kencana Prenada Media Group*, Jakarta, 2013, page.17

4 Johannes Ibrahim., *Cross Default and Cross Collateral as Efforts to Settle Problem Loans,* Bandung, Refika Aditama, 2004, page. 1

5 Qamar., Nurul, *opage.cit*, page. 96-99.

6 Juan Maulana Alfedo., Elaboration Law Concept Pada Mutual Legal Assistance Sebagai Upaya Penanggulangan Cybercrime Transnational Industri 4.0, *Legislative*, Vol. 3, No. 1, December 2019, page. 32-55

7 Imam Nur Hakim Hasan., *Criminal Responsibility for Cyber Crime in the form of the spread of Viruses Which Cause Disruption To Electronic Systems*, Accessed on 1 November 2023

tendency to continue to get worse and get wilder. In the world of modern crime, theft is no longer just taking tangible goods/materials, but also includes taking data illegally[8]

Cases of cyber crime in the banking sector are relatively new crimes that seriously disrupt banking financial security[9] and even have the potential to harm a bank, because the perpetrators commit crimes using high-tech equipment by utilizing telecommunications networks.[10]

Research conducted by Chat Le Nguyen with title "National criminal jurisdiction over transnational financial crimes", This paper argues that when the jurisdictional concurrence occurs, the involved states should consult one another by taking into account a number of relevant factors and take the "centre of gravity" approach to deciding which state or forum should prosecute eventually. States less able to establish jurisdiction over the offences are often those which have a weak legal basis and/or insufficient resources.[11]

Research conducted by Gunsu Nurmansyah with the title Legal Protection For Corports Cybercrime Data Forgery In The Banking Sector Through The Internet (E-Banking). Analysis of Cybercrime Data Forgery in the banking sector through the Internet (e-banking), is carried out by starting with the theft of data - data from the Internet (e-banking). Internet (e-banking), carried out by starting with the theft of important data. The enactment of the Act is a written regulation that is imposed on cybercrime hackers, especially in cases of data forgery. Although the material elements have been fulfilled as in Criminal Code Article 263, but the perpetrator of data forgery. The perpetrators of data forgery are still caught by a more specific law in accordance with the Lex Specialist Darogat Lex Generalis principle. For example in the case of data forgery that can be subject to laws related to data falsification through electronic media, so that the perpetrators will be subject to the through electronic media, so the perpetrator will be subject to Article 35 jo Article 51 paragraph (1) of Law No. 19/2016 concerning ITE.[12]

The case of Cyber Crime by accessing electronic systems (without rights and against the law accessing electronic and computer systems) belonging to banks which is detrimental to the Bank's finances has occurred in the Medan City area, namely as a special criminal case in Decision Number: 1253/Pid.Sus/2020/ PN.Mdn, where Defendant I, Defendant II,

8 Desi Anggreini., *Accountability of Perpetrators of Cyber Crime Fishing*, Yogyakarta, UIN Sunan Kalijaga, 2009

9 Ilyas Sarbini., Legal Responsibility for Misuse of Government Credit Cards in State Financial Management, *Jurnal Ilmu Sosial dan Pendidikan (JISIP)*, Vol. 6, No. 2, Maret 2022, page.2637-2736

10 Awalia Meta Sari., *Judicial Study of Cyber Crime in Indonesia*, IAIN, Accessed 1 November , 2023

11 Le Nguyen, C., National Criminal Jurisdiction Over Transnational Financial Crimes, *Journal of Financial Crime*, Vol. 27, No. 4, 2020, page. 1361-1377

12 Gunsu Nurmansyah., Legal Protection For Corports Cybercrime Data Forgery In The Banking Sector Through The Internet (E-Banking), *Monograf Gagasan Pembaharuan Hukum Pidana Dan Perdata*, Vol. 5, 2020, page. 96

and Defendant III (hereinafter referred to as the Defendants) intentionally and without authorization (without permission from the Bank) accessed PT's electronic system. Bank Rakyat Indonesia, Tbk (BRI) used the BRI ATM machine to top up Link Aja in a way that did not work properly, in which case the BRI account balance used by the Defendants did not decrease, which resulted in losses for BRI Bank and also losses to the State.

The purpose of this research is to know and analyze the Scope of Cyber Crime by accessing electronic banking systems that harm the Bank's finances, Legal Protection for Banks That Suffer Losses Due to Actors Accessing the Bank's Electronic System, Criminal Liability for Cyber Crime Actors By Accessing Electronic Banking Systems That Harm State Finances.

B. RESEARCH METHODS

The research method used is library research (library study), in legal research the normative juridical approach method or library law research which means an approach based on legal rules as a provision and also the basic law, tracing from related books and relevant to the discussion in this paper, apart from books about cyber crime, data is also sourced from related research journals, as well as from websites related to the title of this research.

C. RESULTS AND DISCUSSION

1. Scopeto *Cyber Crime*by accessing the banking electronic system which is detrimental to the Bank's finances

Along with the development of society's needs in the world, information technology plays an important role, both now and in the future.[13]Rapid developments in internet technology have caused new crimes in this field to emerge, for example crimes of data manipulation, espionage, sabotage, provocation, money laundering, hacking, software theft or hardware damage and various others.[14]Cyber crime is divided into 2 categories, namely cyber crime in the narrow sense and in the broad sense. Cyber crime in the narrow sense is crime against computer systems, while cyber crime in the broad sense includes crimes against computer systems or networks and crimes that use computer facilities.[15]

Intimidation also targets students and academics who hold scientific discussions. Critical voices at odds with the government are often attacked in the digital realm, not only promoting power that kills deliberative processes and public participation, this approach is also supported by state repression tools.[16]

Indonesia is a country of law, this is stated in article 1 paragraph

13 Agus Rahardjo., *Cybercrime-Understanding and Efforts to Prevent Technological Crime*, Bandung, Citra Aditya Bakti, 2012), page. 1

14 Barda Nawawi Arief., 2016, *Mayantara Crime and the Development of Cyber Crime Studies in Indonesia*, Jakarta, Rajawali Pers, page. 25

15 Akbar., Harmonization of the Cyber Crime Convention in National Law, *Jambi Legal Science Journal*, Vol.VI. No.3, 2014

16 Arief, B.N., *Law Enforcement Issues & Crime Prevention Policy*, Bandung, Citra Aditya Bakti, 2001

(3) of the 1945 Constitution of the Republic of Indonesia, so that law enforcement officers in carrying out their duties must comply with the laws that apply in Indonesia.[17]The consequence of Indonesia as a country of law, in the context of law enforcement in Indonesia, is that law enforcers in carrying out law enforcement, the Criminal Code has regulated theft, which is stated in Article 362 of the Criminal Code, namely "Whoever takes something, wholly or partially, belonging to someone with the intent to possess it unlawfully, is threatened, for theft, with imprisonment for a maximum of five years or a fine of a maximum of nine hundred rupiah."[18]The provisions of Article 362 of the Criminal Code regulate the crime of general theft or ordinary theft, however, along with the development of information and electronic transactions, it has created a new type of crime known as cyber crime.[19]including theft through cyberspace or electronic systems. Therefore, it is necessary to specifically regulate various crimes that occur within the scope of cyberspace, so that the development of information and electronic transactions in society is directly proportional to the increase in cybercrime.[20]which encouraged the government to establish Law No. 11 of 2008 concerning Electronic Information and Transactions which has been amended by Law No. 16 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Electronic Information and Transactions (hereinafter referred to as the ITE Law). The provisions of this law specifically regulate cybercrime, including theft using electronic systems[21]

2. The Legal Protection for Banks Who Suffer Lossescaused by Perpetrators Accessing the Bank's electronic system

With the rapid development of time and technology and the various forms of threats facing national security will change. Now threats can also occur in the world or better known as cyber crime. Several cases of cybercrime include crimes committed by bad actors through social media and the internet and have proven to be more or less disturbing national security. Internet banking is a banking service to customers or customers which aims to make it easier for customers to check balances and make payments for each banking transaction online. online Banks are becoming increasingly stronger in developing internet banking services because of the progress of the internet and its benefits, as well as the increasing number of internet users in the world.

17 Rofah, NR, & Priatnasari, Y., Internet Banking and Cyber Crime: A Case Study in National Banking, *Indonesian Journal of Accounting Education*, Vol. 18, No. 2, 2020, page.107-119.

18 Tatulangi, CH., Cyber Crime in Banking Activities, *Lex Privatum*, Vol. 9, No. 5, 2021

19 Agus Setia Wahyudi., Obstacles to Criminal Accountability for Perpetrators of Money Theft at Banks via the Internet Based on Law Number 11 of 2008 concerning Information and Electronic Transactions, *Journal of Legal Sciences, Mimbar Justice* July-November 2015, page. 135-149

20 Rahardjo, Agus., *Cybercrime Understanding and Efforts to Prevent Technological Crime*, Citra Aditya Bakti, Bandung, 2012;

21 Isemadi, HS, & Shaleh, AI., Banking Credit Restructuring Policy Amid COVID-19 Pandemic in Indonesia, *Journal of Economic Innovation*, Vol. 5, No. 02, 2020

Therefore, the potential that currently exists is good for banks to develop internet-based services.[22]

The following are the types of security systems used in internet banking according to Lewis and Thygerson. The system has the function of recognizing a customer and protecting all of the customer's financial information. This system functions to do.[23]

Prevention of parties who do not have permission from entering protected or protected areas in a company's work center unit. The firewall system cannot prevent viruses and this is purely an internal organizational problem.[24]

There are several aspects of computer security that must be considered and have several important scopes, which according to Lewis and Thygerson, this aspect emphasizes efforts to maintain the confidentiality of data and information and that other parties must not access it. Meanwhile, privacy places more emphasis on private data, for example data about banking customers. prioritize the security of data or information so that it cannot be accessed other than without the owner's permission. Aspects that emphasize the originality of data or information, including that the party providing the data or accessing it is the party who has access permission or is the legal owner.[25]

Availability Aspects related to the availability of information when needed, computer security includes several aspects including[26]: Authentication, so that the recipient of the information can ensure the authenticity of the message coming from the person requested for the information.[27]Integrity, the authenticity of messages sent over a network and it can be ensured that the information sent has not been modified by those entitled to travel the information.[28].Non-repudiation, Non-repudiation is a matter that concerns the sender. The sender cannot deny that he was the one who sent the information.[29]*Authority,* Information on the network system cannot be modified by parties who do not have the right to access it. Confidentiality is an effort to protect information from people who do not have the right to access it. Privacy, Privacy refers more to data that is personal in nature. Availability: The availability aspect relates to the availability of information when

22 Remy Syahdeni, Sutan., *Crime and Computer Crime*, Pustaka Utama Grafiti, Jakarta, 2016

23 Suhariyanto, Budi., *Information Technology Crime (Cybercrime),* Raja Graffindo Persada, Jakarta, 2012

24 Muhamad Djumain., *Principles of Banking Law in Indonesia*, Citra Aditya Bakti, Bandung, 2005

25 Faridi, Muhammad Khairul., Cyber Crime in the Banking Sector, *Cyber Security and Digital Forensics*, Vol. 1, No. 2, 2018

26 Juniawan, Komang., Legal Protection for Customers Victims of ATM Card Duplication Crimes at National Private Banks in Denpasar, *Udayana Master of Law Journal*, Vol. 2, No. 2, 2013

27 Maskun., *Cybercrime An Introduction*, Kencana, Prenata Media Group, Jakarta, 2013

28 Safitri Indra., Crime in the Cyber World, Insider, *Legai Journal from Indonesian Capital and Investment Market*, accessed hhtp://business.fortunecity.com on 27 October 2020.

29 T Arifianto., Application of Fingerprint Recognition Using the Learning Vector Quantization (LVO) Method in an Automatic Teller Machine (ATM), *Jumal SPIRIT*, 2018

needed.[30]*Access control*, This aspect relates to the way access to information is regulated.

According to Budi Rahardjo, he said that the security aspects that must be maintained in internet banking are:[31]*Confidentiality*, The confidentiality aspect provides a guarantee that data cannot be intercepted by unauthorized parties.[32]Integrity: The integrity aspect guarantees data integrity, where data must not be changed or changed by unauthorized parties.[33]Authentication, Authentication is used to convince people who access the service and also the (web) server that provides the service[34]Non-repudiation, The non-repudiation aspect guarantees that if a customer makes a transaction then he cannot deny having made the transaction[35]. Availability: The availability aspect focuses on service availability. [36]

It is explained that protection is all efforts to fulfill rights and provide assistance to provide a sense of security to witnesses and/or victims which must be implemented by (LPSK) or other institutions in accordance with the provisions of this Law.[37].Based on Article 1 Number 8 of Law of the Republic of Indonesia Number 31 of 2014 concerning Amendments to Law No. 13 of 2006 concerning Protection of Witnesses and Victims, it explains that protection is all efforts to fulfill rights and provide assistance to provide a sense of security to witnesses and/or victims which must be carried out by the Witness and Victim Protection Agency or other institutions in accordance with the provisions of this Law.[38]

This article explains that witnesses and/or victims have the right to provide assistance and protection. Thus, in cases of data theft against bank customers, customers who are victims have the right to receive legal protection and assistance as victims of criminal acts.[39]Most of the victims of banking crime are those who usually have direct interaction with various banking activities.

3. The criminal responsibility for cyber crime perpetrators by accessing banking electronic systems that harm state finances

Viewed from the point of view of the occurrence of a prohibited

30 Wahid Abdul and Moh, Labib., *Mayantara Crime (Cyber Crime),* Refika Aditama, Jakarta, 2005

31 Widyopramono Hadi Widjojo., Cybercrimes and their Prevention, *Technology Law Journal, Faculty of Law, University of Indonesia*, Jakarta, 2005

32 William Wiebe., Crime Through Computers, Seminar, Makassar, 2000.

33 Marwandianto and Helmi Ardani Nasution., *Op, Cit,* page. 2

34 Widodo., *Criminal Law in the Field of Information Technology; Cybercrime Law: Theoretical Study and Case Analysis*, Yogyakarta, Aswaja Pressindo, 2011

35 Wisnubroto Aloysius., *Criminal Law Policy in Combating Computer Abuse,* Yogaykarta, Atmajaya University, 1999

36 Widyopramono., *Crime in the Computer Sector*, Sinar Harapan Library, 1994.

37 Ferdinand Wisnu., *Definition, Types and Functions of Banks*, accessed 20 July 2023

38 William Wiebe., *Crime Through Computers*, Seminar, Makassar, 2000.

39 Sinta Dewi Rosadi., *(Cyber Law) Aspects of Data Privacy According to International, Regional and National Law*, Bandung, PT. Refika Aditama, 2015

action, a person will be held criminally responsible for these actions if the action is unlawful and there is no elimination of the unlawful nature or justification for it.[40]Viewed from the perspective of capacity for responsibility, only someone who is capable of responsibility can be held criminally accountable. The development of criminal law means that parties who can be held accountable or held criminally responsible are not only people as legal subjects (as regulated in the Criminal Code), but also legal entities (corporation, as regulated in the Environmental Management and Protection Law).[41]With regard to the criminal liability of perpetrators of theft through electronic systems, the thing that needs to be taken into account is that the act committed is against the law, where the act fulfills the criminal elements of a criminal act that have been formulated in the criminal law regulations.[42]

Criminal acts or in Latin called actus reus are defined as acts that violate criminal law. Actus reus is an unlawful act that includes elements of an act that are in accordance with the formulation of the law[43]. According to Herman Kantorowics, a criminal act (actus reus) means that the defendant can be expected to do something other than the act that has been committed which constitutes deik.[44]The perpetrator of a criminal act can be held criminally liable, in this case it means that the perpetrator must fulfill the requirements to be held accountable. Based on the "principle of no criminal liability without fault", the maker can be held responsible if he makes a mistake. Meanwhile, the measure of whether there is a mistake in the maker, can be seen from the maker's normal mental attitude or his or her intellect, which can differentiate between actions that are permissible and not permissible to do. In relation to the criminal liability of perpetrators of theft via electronic systems, this act has been determined as a criminal act as regulated in Articles 30 to 36 of the ITE Law.[45]

The application of sanctions against perpetrators of cyber crime in theft is through the criminal justice system as part of criminal law policy to enforce the law, with the initial process of the police to conduct investigations and apply pasa, then to the prosecutor's office to complete the formal and material, and then to the court, namely to impose sanctions from the judge to the perpetrators of criminal acts. And the researchers found that the sanctions against the perpetrators of cyber crime are very light and ineffective because of the crimes committed by the perpetrators of cyber crime that cause enormous losses to other

40 Dian Ekawati Ismail., Cyber Crime in Indonesia, *Faculty of Social Sciences, Gorontalo State University,* Vol. 6, No. 3, 2009.

41 Hardianto Djanggih., Criminal Law Policy in Overcoming Cyber Crime, *Legal Media Journal*, Vol. 1, and 2, 2013.

42 Abdul Wahid and Mohammad Labib., *Mayantara Crime*, Bandung, Refika Aditama, 2010.

43 Agus Rahardjo., Cybercrime: *Understanding and Efforts to Prevent Technological Crime*, Bandung, PT Citra Aditya Bakti, 2002

44 Teguh Prasetyo., *Opage.cit*., page. 8.

45 Josua Sitompul., 2014, *Cyberspace, Cybercrimes, Cyberlaw*, Jakarta, Tatanusa, page.147-148

people and banks.

The act is formulated as a formal offense, so that the act is considered complete if the act has been carried out, even though the goal the perpetrator wanted to achieve has not been realized. Apart from criminal acts (*actus reus*), criminal liability must also pay attention to the mental attitude (mens rea) of the perpetrator. Mens rea includes the element of the perpetrator or perpetrator of the offense, which includes the inner attitude or psychological state of the perpetrator. The inner attitude of the perpetrator is closely related to the ability to take responsibility.[46]

D. CONCLUSION

The scope of cybercrime is regulated in Law No. 36 of 1999 concerning Telecommunications which regulates several articles containing prohibited acts, including cybercrime crimes. Law No. 36 of 1999 concerning Telecommunications was enacted to accommodate punishment for cybercrime crimes, before the enactment of Law No. 11 of 2008 concerning Information and Electronic Transactions. However, Law No. 36 of 1999 concerning Telecommunications only regulates several criminal acts including cybercrime which are still general and broad in nature, and only relate to telecommunications, so it cannot accommodate criminal acts related to computers. Law enforcement against perpetrators is carried out through a criminal responsibility process for Cyber crimes carried out by perpetrators using computers and the internet. Criminal liability by the perpetrator is carried out in accordance with the procedures of the Criminal Code (KUHP) and Law No. 11 of 2008 concerning Electronic Transactions. Law enforcement procedures are carried out according to the Criminal Procedure Code in accordance with Law No. 8 of 1981 because Cybercrime violations will be prosecuted formally in the Criminal Procedure Code as a form of law enforcement for perpetrators to be held accountable for Cybercrime criminal acts.

BIBLIOGRAPHY

Journals:

Agus Setia Wahyudi., Obstacles to Criminal Accountability for Perpetrators of Money Theft at Banks via the Internet Based on Law No. 11 of 2008 concerning Information and Electronic Transactions, *Journal of Legal Sciences, Mimbar Justice*, July-November 2015;

Akbar., Harmonization of the Cyber Crime Convention in National Law. *Jambi Legal Science Journal*, Vol. VI, No. 3, 2014;

Dian Ekawati Ismail., Cyber Crime in Indonesia, *Faculty of Social Sciences, Gorontalo State University,* Vol. 6, No. 3, Gorontalo, 2009;

46 Chairul Huda., *From No Crime Without Fault To No Criminal Responsibility Without Fault,* Jakarta, Prenada Kencana Media Group, 2014, page. 68.

Faridi, Muhammad Khairul., Cyber Crime in the Banking Sector, *Cyber Security and Digital Forensics*, Vol. 1, No. 2, 2018.

Gomgom TP Siregar., The Law Globalization In Cybercrime Prevention, *IJLR: International Journal of Law Recontruction*, Vol. 5, No. 2, September 2021;

Gunsu Nurmansyah., Legal Protection For Corports Cybercrime Data Forgery In The Banking Sector Through The Internet (E-Banking), *Monograf Gagasan Pembaharuan Hukum Pidana Dan Perdata*, Vol. 5, 2020;

Hardianto Djanggih., *Criminal Law Policy in Overcoming Cyber Crime*, *Legal Media Journal*, Vol. 1 and 2, 2013;

Ilyas Sarbini., Legal Responsibility for Misuse of Government Credit Cards in State Financial Management, *Jurnal Ilmu Sosial dan Pendidikan (JISIP)*, Vol. 6, No. 2 Maret 2022,

Isemadi, HS, & Shaleh, AI., Banking Credit Restructuring Policy Amid COVID-19 Pandemic in Indonesia, *Journal of Economic Innovation*, Vol. 5, No. 02, 2020;

Juan Maulana Alfedo., Elaboration Law Concept Pada Mutual Legal Assistance Sebagai Upaya Penanggulangan Cybercrime Transnational Industri 4.0, *legislative*, Vol. 3, No. 1, December 2019;

Juniawan, Komang., Legal Protection for Customers Victims of ATM Card Duplication Crimes at National Private Banks in Denpasar, *Udayana Master of Law Journal*, Vol. 2, No. 2, 2013;

Le Nguyen, C., National Criminal Jurisdiction Over Transnational Financial Crimes, *Journal of Financial Crime*, Vol. 27, No. 4, 2020;

Rofah, NR, & Priatnasari, Y., Internet Banking and Cyber Crime: A Case Study in National Banking*. Indonesian Journal of Accounting Education*, Vol. 18, No. 2, 2020;

T Arifianto, Application of Fingerprint Recognition Using the Learning Vector Quantization (LVO) Method in an Automatic Teller Machine (ATM), *Jumal SPIRIT*, 2018;

Tatulangi, CH., Cyber Crime in Banking Activities. *Lex Privatum*, Vol. 9, No. 5, 2021;

Books:

Abdul Wahid and Mohammad Labib., 2010, *Mayantara Crime*, Refika Aditama, Bandung;

Agus Rahardjo., 2002, *Cybercrime: Understanding and Efforts to Prevent Technological Crime*, PT Citra Aditya Bakti, Bandung;

Agus Rahardjo., 2012, *Cybercrime-Understanding and Efforts to Prevent Technological Crime*, Citra Aditya Bakti, Bandung;

AwaliaMeta Sari., 2023, *Judicial Study of Cyber Crime in Indonesia*., IAIN;

Desi Anggreini., 2023, *Accountability of Perpetrators of Cyber Crime Fishing*, UIN Sunan;

Arief, B.N., 2001, *Law Enforcement Issues & Crime Prevention Policy,* Citra Aditya Bakti, Bandung;

Barda Nawawi Arief., 2016, *Mayantara Crime and the Development of Cyber Crime Studies in Indonesia*, Rajawali Pers, Jakarta;

Djoni S. Gazali and Rachmadi Usman., 2012, *Banking Law*, Sinar Grafa, Jakarta;

Ferdinand Wisnu, Definition., 2023, *Types and Functions of Banks*, accessed 20 July;

Imam Nur Hakim Hasan., 2009, *Criminal Responsibility for Cyber Crime in The Form of The Spread of Viruses Which Disrupt Electronic Systems*, Accessed on 1 November 202 Kalijaga, Yogyakarta;

Johannes Ibrahim., 2004, *Cross Default and Cross Collateral as Efforts to Settle Problem Loans*, Refika Aditama, Bandung;

Maskun., 2013, *Cyber Crime*, Kencana Prenada Media Group, Jakarta;

Maskun., 2013, *Cybercrime An Introduction*, Kencana, Prenata Media Group, Jakarta;

Muhamad Djumain., 2005, *Principles of Banking Law in Indonesia*, Citra Aditya Bakti, Bandung;

Rahardjo, Agus., 2012, *Cybercrime Understanding and Efforts to Prevent Technological Crime,* Citra Aditya Bakti, Bandung;

Remy Syahdeni, Sutan., 2016, *Crime and Computer Crime*, Pustaka Utama Grafiti, Jakarta;

Safitri Indra., *Crime in the Cyber World, Insider, Legai Journal From Indonesian Capital and Investment Market*, accessed hhtp://business.fortunecity.com on 27 October 2020;

Sinta Dewi Rosadi., 2015, (*Cyber Law) Aspects of Data Privacy According to International, Regional and National Law*, PT. Refika Aditama, Bandung;

Suhariyanto, Budi., 2012, *Information Technology Crime (Cybercrime),* Raja Graffindo Persada, Jakarta;

Wahid Abdul and Moh, Labib., 2005, *Mayantara Crime (Cyber Crime),* Refika Aditama, Jakarta;

Widodo., 2011, *Criminal Law in the Field of Information Technology; Cybercrime Law: Theoretical Study and Case Analysis*, Aswaja Pressindo, Yogyakarta;

Widyopramono Hadi Widjojo., 2005, Cybercrimes and their Prevention, *Technology Law Journal, Faculty of Law, University of Indonesia*, Jakarta;

Widyopramono., 1994, *Crime in the Computer Sector*, Sinar Harapan Library;

William Wiebe., 2000, *Crime Through Computers*, Seminar, Makassar;

Wisnubroto Aloysius., 1999, *Criminal Law Policy in Combating Computer Abuse*, Atmajaya University, Yogaykarta.