Jurnal Hukum Volkgeist
Volume 5 Issue 2, 2021
P-ISSN : 2528-360X, E-ISSN : 2621-6159

Responsiveness of Criminal Law to Skimming Crimes in The Era of Industrial Revolution 4.0 (Four Point Zero)

Ahmad Suryadi[1]

Abstract

This study aims to: 1)Analyze and understand the responsiveness of criminal law in entering the era of industrial revolution 4.0 (four point zero), 2)Enforcement of criminal law in cyber crime, criminal acts in cyber crime, criminal responsibility of cyber crime perpetrators. This research is normative-empirical research which is basically a merger between normative legal approach with the addition of empirical elements as the implementation of normative law in its action on every legal event that occurs in society. The results of this study show that cyber crime is a special crime. Cyber Crime has the intent as a crime in the realm of computer technology and internet networks as targets. The basis of law enforcement considerations in cyber crime is based on Law No. 11 of 2008 concerning Information and Electronic Transactions in the Act as amended into Law No. 19 of 2016 on Information and Electronic Transactions (ITE) on Information and Electronic Transactions. Criminal liability for perpetrators of cyber crime crimes always pay attention to the enactment of Law No. 11 of 2008 on Information and Electronic Transactions in as amended into Law No. 19 of 2016 on Information and Electronic Transactions (ITE) on Information and Electronic Transactions and pay attention to the methods of criminal law. In the process of law enforcement on cyber crime must always prioritize legal certainty as a form to provide protection and security in the process of transactions through the internet for the public at large.

Keywords: *Cyber Crime, Cyber Law, Enforcement Law.*

Author's Information:
[1]Faculty of Law, Hasanuddin University, Indonesia,

Email:
(ardisaucy12@gmail.com)

Article's Information:
DOI:
https://doi.org/10.35326/volkgeist.v5i2.845

1 Introduction

Without being misled, the state is obligated to offer protection to all its inhabitants. Because protection of citizens entails not just security but also protection from poverty, the state is also obligated to advance the general welfare (Salam, 2018) The development and advancement of information technology globally has a wide impact in the midst of national and international public life. Law in its development is not only used to regulate the behavior that already exists in society and maintain existing patterns of habits (Supriyanto, 2019)

These advances have not only created trade using electronic commerce, so as to indirectly obliterate the concept of conventional buying and selling, but also has raised public concerns and fears about the negative excesses of the technology, such as crimes against credit cards or Anjung Tunai Mandiri (ATM), data transactions and threats of information technology power in lieu of human power in the world of work is like the rise in online shopping.

In this case the government has responded by creating and establishing Law No. 11 of 2008 on Information and Electronic Transactions as amended to Law No. 19 of 2016 on Information and Electronic Transactions (ITE). The presence of this Law proves that the Government of Indonesia must follow the flow of globalization in all fields, including in electronic transactions that are clearly different from the legal actions in general. The enactment of this law also answers legal challenges in cyberspace or cyber law that have not been specifically regulated in Indonesia. In a good system there should be no opposition (Salam, 2020)

With the enactment of Law No. 11 of 2008 on Information and Electronic Transactions as amended into Law No. 19 of 2016 on Information and Electronic Transactions (ITE) brings logical consequences in the body of law enforcement institutions in Indonesia. Momentum is that the law should be enforced from the general public (Ilham, 2019)

This new law requires law enforcement who fully understand and master information technology comprehensively in carrying out tasks in the future. This is because the actions that used to be conventionally feel easy to solve, but the challenges of the tasks ahead must be faced with a legal action that can only be felt as a result without knowing who the perpetrator is and where the action is done. The legal action takes place in the cyber world. Law No. 19 of 2016 on Information And Electronic Transactions, n.d.)

Criminal justice subsystems such as police, prosecutors, judiciary, correctional institutions and advocates must reposition themselves. Various efforts made by law enforcers With the existence of cases. (Herlina Sulaiman, 2019) Their professionalism is highly demanded in completing the difficult tasks in the field of law going forward. For in their hands is the legal certainty (legal certainty) can be realized for the seekers of justice on the earth (justice for all). In addition to repositioning rather than law enforcement in entering the industrial revolution 4.0 regulation and other legal institutions must also be renewed as an effort to answer the challenges of the times, the development of globalization forces us into the competition thegnology that consequently in criminal law is a matter of challenge locus delicti and tempos delicti. Locus delicti, which means location or place, in terms of the enactment of criminal law seen in terms of the location of the occurrence of criminal acts. Meanwhile, tempus delicti is the time of the crime (Prasetyo, 2017).

In addition, the determination of an act that is considered unlawful will have difficulty because it will be difficult to determine the act as a criminal act or an act as a business effort. actus reus (physical element) and mens rea (mental element). The actus reus element is the essence of the crime itself or the act committed, while the element mens rea is the mental attitude of the perpetrator at the time of doing the deed.

This will make it difficult for law enforcement to identify an act that is considered against the law if its regulation and legal structure do not lead to crimes in the tech world. In addition, existing legal norms cannot be considered to fully meet the dimensions of law enforcement related to the problem of technological crimes, it will make the handling and settlement of criminal acts sluggish and difficult. When faced with the problem of crime that occurs and causes losses due to the development of such technology. Then if law enforcement does not understand this, it can have an impact on an injustice in law enforcement. Therefore, preventive measures are needed that seek to enable law enforcement in the future to be able to understand the development of technology in the era of industrial revolution 4.0.

Not only until there are various crimes in criminal law committed by humans by using information technology systems wrongly. The tendency of people who use *e-commerce* is also vulnerable to the crime of *skimming*, therefore it is necessary to be careful in using electronic transaction tools so that we do not let our guard down and become victims of *skimming*, in this case exemplified the enforcement of tickets with electronic ticket system (e-ticket) in the aviation business globally is a clear example and provides convenience for consumers. Similarly, the determination of contracts by the parties is simply done through cyberspace by affixing an electronic signature, which is a signature consisting of electronic information attached, associated or related to other electronic information used as a means of verification and authentication.

In the end the era of disruption left a lot of homework for experts and law enforcement in Indonesia who demanded a high level of professionalism and reliable with the mastery of soft skills such as computers and English. Challenges or challenges are not something that must be avoided but must be faced in the right way and strategy, so that all get space in the science of law as implementative legal certainty.

2. Methods

2.1.Research Type

The type of research to be conducted using normative-empirical legal methods. Normative research is based on normative legal science in the Law, comparative laws, prevailing principles and theories that exist related to. While empirical based on facts and reality that occur (Dawn, 2010)

2.2 Types of Legal Materials

a. Primary Legal Materials

Primary legal materials that are authoritative or have authority consisting of legislation in Law No. 1 of 1946 concerning Criminal Law Regulations, Law No. 8 of 1981 on Criminal Procedural Law, Law No. 2 of 2002 concerning the State Police of the Republic of Indonesia, Law No. 16 of 2004 concerning The Attorney General of the Republic of Indonesia, Law No. 8 of 2004 on General Justice, Law No. 11 of 2008 has been amended to Law No. 19 of 2016 on Information and Electronic Transactions,, official records or treatises as well as the judge's decision on Decision No. 282/Pid.Sus/2020/PN. Mks.

b. Skunder Legal Materials

Secondary legal materials are derived from books, legal dictionaries, legal journals, dissertations, theses, articles, legal expert opinions and other documents that include secondary legal material by adding empirical elements in analyzingthem.

2.3 Legal Material

The technique of collecting legal materials in the writing of this thesis is through library research and legal documentation to obtain primary legal materials and secondary legal materials. Literature research is carried out by collecting, reading, and tracing a number of books, articles, legal journals, laws and regulations, judges' decisions or other literature by looking at the facts that occur as empirical elements relevant to the title of this thesis. Data collection techniques used in this study is to use interview techniques, namely conducted direct interviews with respondents who are expected to provide input and explanation on the issue properly andcorrectly (Salam, 2017)

Legal materials obtained normatively-empirically through research activities both primary legal materials and secondary legal materials or facts and events that occur in society are analyzed qualitatively. Quality data analysis is descriptive data management that starts from the basics of general knowledge and then examines things of a special nature. Then from the analysis process is drawn an analysis and conclusions. Then presented in a way that explains and describes according to the problems associated with writing this thesis.

3. Result

3.1 Material Criminal Law Enforcement Against *Skimming* Crimes In *Cyber Crime* In the Era of Industrial *Revolution 4.0 (Four Point Zero)*

Cyber crime or cybercrime a term that refers to criminal activity with a computer or computer network being a tool, target or place of occurrence of a crime. These include online auction fraud, cheque fraud, credit carding fraud, confidence fraud, identity fraud, child pornography, skimming, and others (Sodiki, n.d.)

Regulation *of Cyber Crime* to bring legal certainty to achieve the interests of the legal objectives itself. The purpose of the law is the direction or objective to be realized by using the law as a tool in realizing that goal in the order of governing society. The purpose of law in general or the purpose of law universally, can be seen from three conventional traditions (Ali, 2008) :

a) Ethical Flow

The purpose of the law is solely to achieve justice determined by ethical beliefs about fair and unjust. The law aims to neutralize or realize justice.

b) Utilistic Flow

The purpose of the law is solely to create the greatest benefit or happiness for people and citizens in the largest number (practical moral teachings).

c) Dogmatic Juridical Tradition

The purpose of the law is solely to create legal certainty, because with the certainty of the law, the function of the law can run and be able to maintain order. Legal certainty is an absolute requirement of every rule, the issue of justice and the usefulness of the law is not the principal reason of the purpose of the law but the important thing is legal certainty.

On the fact that there has been a positive law that applies to Indonesia responds to this by making a special rule to limit the possibilities of crimes that can occur in cyberspace by enacting Law No. 11 of 2008 on information and electronic transactions which is then in amendment to Law No. 19 of 2016 on information and electronic transactions with the basic application of theology of legal certainty . Structurally in this Law there are 9 acts that are prohibited starting from article 27 to article 35 of Law No. 19 of 2016 on information and electronic transactions with the following primary norms (Law No. 19 of 2016 on Information And Electronic Transactions, n.d.) :

1) Article 27: Prohibition of distributing, transmitting, making accessible electronic information and/or electronic documents.
2) Article 28: Fake news
3) Article 29: Threats of violence or scaremongering

4) Article 30: Accessing the electronic systems of others
5) Article 31: Interception or wiretapping
6) Article 32: Prohibition of changes in electronic information and/or electronic documents
7) Article 33: Interfering with electronic systems
8) Article 34: Prohibition of facilitating electronic software and/or passwords
9) Article 35: Falsification of electronic documents

In part of the research results in a criminal act contained in the ITE Law specifically question the crime of skimming. Skimming is theft of bank data with the aim of harming the owner of bank or bank data. The culprit is called a skimmer. skimming is one of the crimes in cyber crime. This crime is committed through a network of computer systems, both local and global, by utilizing technology, by illegally copying the information contained in the magnetic stripe of atm cards to have control over the victim's account. These cyber crime actors have a high capability background in their field making it difficult to track and eradicate them completely. Skimming is the activity of doubling the information contained in magnetic stripes contained on credit cards and ATMs / debits illegally. This means that skimming is an activity related to the perpetrator's attempt to illegally steal data from the magnetic tape of an ATM/debit card to have control over the victim's account.

Several cases of skimming crimes that occurred in Indonesia such as skimming crimes that occurred in the jurisdiction of Mapolda Metro Jaya Jakarta in 2018 that arrested a bank break-in plot with suspects named Caitanovici Andrean Stepen, Raul Kalai, Lonel Robert Lupu and Ferenc Hugyec each from Hungary, Bulgaria, Romania by carrying out their crimes in almost 64 countries in a row and arrested in crimes in the region Indonesian law. The perpetrators of skimming crimes are entangled with article 263 of the Criminal Code, 363 of the Criminal Code and Article 46 of Law No. 19 of 2016 and article 3, 4, 5 of Law No. 8 of 2010 concerning Money Laundering Crimes all of his crimes using the same mode by pairing chips or cameras and skimmers on ATM machines, according to the police statement of this conspiracy to rake in billions of rupiah from skimming crimes.

a. Skimming Crimes

In the Criminal Code does not regulate the crime of *skimming*. However, delik in *skimming* crimes can be qualified in Article 362 and Article 263 of the Penal Code as theft and forgery of letters. However, with the existence of Information and Electronic Transactions and considering the principle of *lex specialis derogate legi generalis* then against the perpetrators of *skimming* crimes can be imposed under Law No. 11 of 2008 which has been amended Law No. 19 of 2016 on Electronic Transactions and Information. Skimming criminals are ensnared by Article 30 paragraph 1 (Law No. 19 of 2016 on Information And Electronic Transactions, n.d.), paragraph 2 and paragraph 3 of the ITE Law, Article 31 paragraph 1 and Article 32 of the Electronic Transactions and Information Act and based on Law No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering Crimes for which skimming criminals are entangled with Article 3, Article 4, and Article 5. In addition, the act of accessing the perpetrators of *skimming* crimes can be said to have interacted with computer systems and/or electronic systems belonging to the Bank issuing debit/credit cards in which they store electronic data belonging to customers of a personal nature in any way. The definition of personal data in Article 1 number 27 of Government Regulation 82 of 2012 concerning the Implementation of Electronic Systems and Transactions is certain individual data that

is stored, maintained, and maintained to the truth and protected by confidentiality. (Pratiwi, 2019)

b. Responsibility for *Skimming* Crimes

The elements that must be fulfilled in the accountability of criminal acts are, namely, the ability to distinguish between good and bad deeds that are in accordance with the law and those that are against the law and the ability to determine their will according to the intuition of good and bad deeds. The element is deliberately attached to the element against the law that can be qualified as an error because the act of accessing information or documents contained in the debit/credit card is a banking secret to protect the cardholder as referred to in Government Regulation No. 82 of 2012 concerning Implementation of Electronic Systems and Transactions as well as Bank Indonesia Regulation Number 14/2/PBI/2012 concerning amendments to Bank Indonesia Regulation No. 11/11/PBI/2009 concerning The Implementation of Payment Instrument Activities by Card. Elements of unlawful nature are an absolute element in criminal acts. The existence of such elements can be known from certain behaviors, certain circumstances, or certain consequences that are prohibited or required. (Pratiwi, 2019)

The concept of deliberate and unlawful skimming is important in legal practice regarding the application of Article 30 paragraph (2), Article 31 paragraph (1) and Article 32 paragraph (1), paragraph (2) of the Information and Electronic Transactions Act. Deliberately according to the Indonesian Penal Code means a conscious will intended to commit certain crimes. The phrase requires it to be known or to know that the act can cause consequences as intended by the perpetrator. The act of accessing by the perpetrator of skimming crimes can be said to have interacted with computer systems and/or electronic systems belonging to the Bank issuing debit/credit cards in which they store electronic data belonging to customers of a personal nature in any way. The definition of personal data in Article 1 number 27 of Government Regulation 82 of 2012 concerning the Implementation of Electronic Systems and Transactions is certain individual data that is stored, maintained, and maintained to the truth and protected by confidentiality.

The way that the perpetrator uses a skimmer to copy electronic data on the card is included in the element of Article 30 paragraph (3) because it has tried to break through the security system at the ATM machine. Provisions based on Article 30, Article 31 or Article 32 contain the meaning of the law, that the data or information that is the result of accessing is given to the rightful, then it can not be prosecuted criminal liability because it is not qualified as a delik, even if the data or information accessed belongs to others. Note the meaning of the word in Article 32 paragraph (1) specifically on how to "change, add, reduce, transmit, damage, eliminate, transfer, conceal an electronic information and/or electronic document. It should be understood that the elements contained in the Article are alternative, so that it can be proven one element or part or all of the elements.

If it is associated with the crime of skimming then the way used is to transmit, and move. While in Article 32 paragraph 2 using the meaning of transferring or transferring electronic information and /or electronic documents, The explanation in Article 32 has said quite clearly, while the Institution of criminal responsibility teaches must be clear and the perpetrator understands the allegations brought against him. The act of accessing the offender with the purpose of obtaining data or electronic documents and transferring electronic information and/or electronic documents to his or her electronic system and or others by sending the transmission to an unauthorized person, then transferring or transferring into another blank card / bodong and used to conduct electronic transactions, with the utilization carried out by the plegen, and or doen plegen or medeplegen. losses

to the cardholder/customer and the Bank. Perpetrators of skimming crimes in the formulation of Article 30 paragraph (1), paragraph (2), paragraph (3), Article 31 paragraph (1) and Article 32 due to the act of accessing are subject to criminal sanctions as stipulated in Article 46 paragraph (1), paragraph (2), and paragraph (3) of the ITE Law.

If the objective and subjective elements in Article 30, Article 31 or 32 of the ITE Law can be proven that the perpetrator committed a mistake or caused harm, then it will be penalized as stipulated in Article 46 if it is proven to violate Article 30, Article 47 if it is proven to violate Article 31 or Article 48 if it violates Article 32 and the imposition of this criminal sanction is a criminal liability for the perpetrators of skimming crimes. In the LAW ITE does not clearly regulate anyone who can be said to be the perpetrator, so that the understanding of a person is considered as an offender in order to be punished following the regulation in Article 55 paragraph (1) 1e of the Criminal Code, namely the person who commits a criminal event including the person who did, who ordered to do, or participated in the act.(Soerodibroto, n.d.)

c. Crimes Against *Skimming* Criminals

The regulation on criminal offences for skimming crimes can be reviewed from several laws, namely the Criminal Code, Law No. 11 of 2008 as amended to Law No. 19 of 2016 on Information and Electronic Transactions (ITE). In the Criminal Code of prosecution against the type of acts committed by a person is regulated in Article 10 of the Criminal Code, namely:

Criminal Consists of:

1. Principal Criminal

   a. Death Penalty
   b. Prison Sentence
   c. Confinement
   d. Fines

2.Additional Criminal

   a. Revocation of Certain Rights
   b. Confiscation of Certain Items
   c. Announcement of Judge's Decision

Law No. 11 of 2008 as amended into Law No. 19 of 2016 on Information and Electronic Transactions (ITE) on Information and Electronic Transactions of skimming crimes is qualified to enter into:

Article 30 of the ITE Law, namely:

1) Any Person knowingly and without right or against the law accesses another Person's Computer and/or Electronic System in any way.
2) Any Person willfully and without right or against the law accesses a Computer and/or Electronic System in any way for the purpose of obtaining Electronic Information and/or Electronic Documents.
3) Any Person knowingly and without right or against the law accesses a Computer and/or Electronic System in any way by breaching, breaking through, exceeding, or breaching the security system.

Article 31 of the ITE Law is: Any person willfully and without right or against the law interception or interception of electronic information and/or electronic documents in a particular computer and/or electronic system belonging to another person.

Article 32 of the ITE Law is:

1) Any Person willfully and without right or against the law in any way alters, adds, reduces, transmits, damages, removes, transfers, conceals any Electronic Information and/or Electronic Documents belonging to others or public property.
2) Any Person willfully and without right or against the law in any way transfer or transfer Electronic Information and/or Electronic Documents to another Person's Electronic System that is not entitled to
3) The act as referred to in paragraph 1 which results in the opening of an electronic information and/or electronic documents that are confidential becomes accessible to the public with improper data integrity.

The three articles governing the crime of skimming, namely Article 30, Article 31 and Article 32 are prohibited acts under the ITE Law. The criminal provisions governing skimming crimes, namely Article 46 regulates the provisions of criminal acts stipulated in Article 30 paragraph 1, paragraph 2 and paragraph 3, Article 47 regulates the criminal provisions against acts stipulated in Article 31 paragraph 1, Article 48 regulates the criminal provisions against acts regulated in Article 32 paragraph 1 , paragraph 2 and paragraph 3 of Law No. 19 of 2016 on Information and Electronic Transactions (ITE) on Electronic Information and Transactions.

Article 46 is:

1) Every person who fulfills the elements as referred to in Article 30 paragraph (1) shall be penalized with a maximum imprisonment of 6 (six) years and/or a maximum fine of Rp600,000,000.00 (six hundred million rupiahs).
2) Every person who fulfills the elements as referred to in Article 30 paragraph (2) shall be penalized with a maximum imprisonment of 7 (seven) years and/or a maximum fine of Rp700,000,000.00 (seven hundred million rupiahs).
3) Every person who fulfills the elements as referred to in Article 30 paragraph (3) shall be penalized with a maximum imprisonment of 8 (eight) years and/or a maximum fine of Rp800,000,000.00 (eight hundred million rupiahs).

Article 47 is:

1) Every person who fulfills the elements as referred to in Article 31 paragraph (1) or paragraph (2) shall be penalized with a maximum imprisonment of 10 (ten) years and/or a maximum fine of Rp800,000,000.00 (eight hundred million rupiahs).
2) Article 48 is:
3) Every person who fulfills the elements as referred to in Article 32 paragraph (1) shall be penalized with a maximum imprisonment of 8 (eight) years and/or a maximum fine of Rp2,000,000,000.00 (two billion rupiahs).
4) Every person who fulfills the elements as referred to in Article 32 paragraph (2) shall be sentenced to a maximum imprisonment of 9 (nine) years and/or a maximum fine of Rp3,000,000,000.00 (three billion rupiahs).

5) Every person who fulfills the elements as referred to in Article 32 paragraph (3) shall be penalized with a maximum imprisonment of 10 (ten) years and/or a maximum fine of Rp5,000,000,000.00 (five billion rupiah).

3.2 Criminal Law Responsiveness As *Ius Constituendum* Against *Skimming* Crimes In *Cyber Crime* In the Era of Industrial *Revolution 4.0 (Four Point Zero)*

The era of globalization and information technology has an influence on the emergence of various forms of crime that are new*(cybercrime),*is a phenomenon that requires rapid and accurate countermeasures. Changes to some provisions contained in the Criminal Code is one of the ways that can be used to overcome a new type of crime*(cybercrime)* (Maskun, 2013)

Based on the description above so that in the efforts to responsiveness of criminal law as ius constituendum against skimming crimes in cyber crime in the era of industrial revolution 4.0 (fourt point zero) which is basically about criminal material law that substantively has obtained the legal basis of Law No. 11 of 2008 as amended into Law No. 19 of 2016 on Information and Electronic Transactions (ITE) on Information and Transactions electronic. In other efforts regarding the responsiveness of criminal law as ius constituendum against skimming crimes in cyber crime in the era of industrial revolution 4.0 (fourt point zero) divides on the main part:

a. Criminal Conduct

In this perspective the term criminal conduct is stated in the Budapest Convention, the Cybercrime Convention held for European countries in 2001. In this case criminal conduct is included in the penal policy which is a science as well as an art that ultimately has a practical purpose to enable positive legal regulations to be formulated better and to provide guidelines not only to lawmakers, but also to courts that apply the Law and also to the organizers or executors of court decisions. Therefore, in other words "crime prevention policy with criminal law" can be called criminalization policy, where in this process (criminalization) using criminal means. With regard to the policy of criminalization of cyber crime in the context of the upcoming criminal law (Ius Constituendum), then first of all, the form of regulation must be determined. There are several options in regulating or approaching the criminalization of cyber crime, namely:

1) Integrated into the codification (Criminal Code) by: adding, silicating or meruba or updating the articles in the Criminal Code.

2) Special Law, a special arrangement is required if cyber crime is considered a new category of crime that requires a new and comprehensive legal framework to address the special nature of emerging technologies and new challenges that do not exist in ordinary crimes, and therefore need to be regulated separately outside the Criminal Code. In the field of public law, especially the criminal tradition of continental law seems more prominent in the practice and development of legal science. Therefore, the development of arrangements on the issue of cyber crime crimes is more appropriate when using integrative approaches with arrangements in the Criminal Code either through security or comprehensive changes in the CriminalCode.

The policy of criminalization against cyber crime has been pursued in the concept of a new Criminal Code Bill (concept of September 2019), the Draft Law on Information and Electronic Transactions and Criminal Acts in the Field of Information Technology. In the Draft Law of the Criminal Code regulates regulations that support the policy of criminalization of cyber crime. This is seen in several conditions (Design Criminal) :

Draft Law of the Criminal Code in Book I

a. Article 158. The definition of a term, electronic information is a set or set of electronic data, including but not limited to writing, sound, images, maps, designs, photographs, exchanging data electronically, telegrams, remote copying or the like, letters, signs, numbers, access codes, symbols, or perforations that have meaning or can be understood by people who are able to understand it.
b. Article 164. The definition of a term, a computer is a tool for processing electronic, magnetic, optical, or system data that performs logical, arithmetic, and storage functions
c. Article 171. The definition of the term, login is including accessing the computer or logging into the computer system.

Draft Law of the Criminal Code in Book II

1. Article 336. Any Person who uses or accesses a Computer or electronic system in any way without the right with a view to obtaining, altering, damaging, or omitting information in a Computer or electronic system shall be sentenced to a maximum imprisonment of 4 (four) years or a maximum fine of category V

2. Article 337. Sentenced to a maximum imprisonment of 7 (seven) years or a maximum fine of category VI, any Person who:

a) Without the right to use, access a Computer, or electronic system in any way, with the intention of obtaining, altering, damaging, or omitting national defense information or international relations that may cause interference or harm to the country or its relationship with the subject of international law
b) Without the right to take action that causes the transmission of programs, information, codes or commands of state-protected Computers or electronic systems to be corrupted
c) Without the right or exceed its authority to use or access Computers or electronic systems, both from within and outside the country to obtain information from Computers or electronic systems protected by the state
d) Without the right to use or access government-owned Computers or electronic systems
e) Without the right or exceeding its authority to use or access state-protected Computers or electronic systems, resulting in such Computers or electronic systems becoming corrupted
f) Without the right or exceed its authority to use or access computers or electronic systems protected by the public, resulting in such Computers or electronic systems becoming corrupted
g) Affect or cause disruption of computers or electronic systems used by the government
h) Disseminate, trade, or utilize access codes or information similar to it, which may be used to breach a Computer or electronic system for the purpose of abusing a Computer or electronic system used or protected by the government
i) Commit acts in the framework of international relations with the intention of damaging computers or other electronic systems that are state protected and located in the jurisdiction of Indonesia and addressed to anyone; or

j) Commit acts in the framework of international relations with the intention of damaging computers or other electronic systems that are state protected and located in the jurisdiction of Indonesia and addressed to anyone.

3. Article 338. Sentenced to a maximum imprisonment of 10 (ten) years or a maximum fine of category VI, Any Person who:

a) Without the right or exceed its authority to use or access computers or electronic systems with the intention of obtaining profits or obtaining financial information from central banks, banking institutions or financial institutions, credit card issuers, or payment cards or containing data on their customer statements

b) Without the right to use data or access in any way another person's credit card or payment card in electronic transactions to gain profit

c) Without the right or exceed its authority to use or access the Computers or electronic systems of central banks, banking institutions or financial institutions protected, with the intention of abusing, or to benefit from it; or

d) Disseminate, trade, or utilize access codes or information similar to those that may be used to breach computers or electronic systems with the intent of abusing which could consequently affect the electronic systems of central banks, banking institutions or financial institutions, as well as businesses at home and abroad.

4. Article 339. Any Person without the right to use or access a Computer or electronic system in any way, with the intention of obtaining, altering, damaging, or omitting government-owned information that due to its status must be kept secret or protected shall be sentenced to a maximum imprisonment of 12 (twelve) years or a maximum fine of category VII.

b. International Codperation

If you pay attention to the pace of development of the times followed by crimes that can occur at any time in cyberspace without knowing locus and tempus a criminal incident ksusnya skimming with internet use it is necessary to feel positive laws that apply in Indonesia take an international role in the efforts to respond to criminal law in entering the era 4.0. It considers the development of arrangements made in the Convention for Cyber Crime signed by 30 Countries of the Council of Europe in November 2001 in Budapest Hunggaria which formulated the category of cyber crime delik into a wider scope:

1) Deliberations on the confidentiality, integrity, and availability of data and computer systems including: accessing computer systems without rights, without the right to capture / hear the transmission and transmission, without the right to damage data, without the right to interfere with the system, misuse equipment.

2) Computer-related delik-delik (falsification and fraud with computers

3) Delik-delik containing child pornography

Based on the description above, then seen from the point of criminal law policy (penal policy), criminalization policy is not just a policy of settling / formulating / formulating / formulating what actions can be criminalized (including criminal sanctions), but also covering the issue of how the policy formulation / legislation was prepared in a unified criminal law system (legislative policy) that is harmonious and

integrated. In addition, there is a system that can recognize, detect, protect, revive, and there must be a measure of how far the responsiveness of criminal law in the era of globalization. So the science, first, crime with the application or cybersecurity and resilience that will produce its information security.

4. Conclusion

In part of the research results in a criminal act contained in the ITE Law specifically question the crime of skimming. This crime is committed through a network of computer systems, both local and global, by utilizing technology, by illegally copying the information contained in the magnetic stripe of atm cards to have control over the victim's account. This means that skimming is an activity related to the perpetrator's attempt to illegally steal data from the magnetic tape of an ATM/debit card to have control over the victim's account.

Several cases of skimming crimes that occurred in Indonesia such as skimming crimes that occurred in the jurisdiction of Mapolda Metro Jaya Jakarta in 2018 that arrested a bank break-in plot with suspects named Caitanovici Andrean Stepen, Raul Kalai, Lonel Robert Lupu and Ferenc Hugyec each from Hungary, Bulgaria, Romania by carrying out their crimes in almost 64 countries in a row and arrested in crimes in the region Indonesian law. era of globalization and information technology has influenced the emergence of variousa new form of crime, is a phenomenon that requires rapid and accurate countermeasures.

Based on the explanation above so that in the efforts to responsiveness of criminal law as ius constituendum against skimming crimes in cyber crime in the era of industrial revolution 4.0

References

Ali, A. (2008). *Uncovering Legal Theory And Judicial Theory*. Prenadamedia Group.

Dawn, M. (2010). *Dualism Normative & Empirical Law Research*. Celeben Timur.

Herlina Sulaiman, M. R. L. (2019). Law Enforcement and Eradication of Criminal Action of Narcotics in Pohuwato District Area. *Jurnal Hukum Volkgeist*, *4*(1), 17–25.

Ilham. (2019). Criminal Law Policy about KPK Authorities In The Perspective of Criminal Action In Corruption In Indonesia. *Jurnal Hukum Volkgeist*, *4*(1), 17–25.

Law No. 19 of 2016 on Information And Electronic Transactions.

Maskun. (2013). *Cyber Crime, An Introduction*. Prenada Media Group.

Prasetyo, F. (2017). *Criminal Law*. Raja Grafindo Persada.

Pratiwi, D. F. (2019). Criminal Code Bill. *Juris-Diction*, *2*(4).

Salam, S. (2017). Analysis of Cooperation Agreements and Comparison Patterns of Out-of-Court Dispute Resolution. *Jurnal Hukum Volkgeist*, *2*(1), 71–81.

Salam, S. (2018). Legal Political Perspective on The Protection and Development of Foreign Workers in Indonesia. *Jurnal Hukum Volkgeist*, *3*(1), 89–103.

Salam, S. (2020). Reconstruction of the Paradigm of Philosophy of Science: Critical Study of Law as a Science. *Ekspose: Jurnal Penelitian Hukum Dan Pendidikan*,

18(2), 885–896. https://doi.org/10.30863/ekspose.v18i2.511

Sodiki, A. (n.d.). *Mayantara Crime*. Refika Aditama.

Soerodibroto, S. (n.d.). *Criminal Law Book*. Grafindo Persada.

Supriyanto, H. (2019). The Nature Of Corporate Crime In Law Enforcement Of The Criminal Justice System In Indonesia. *Jurnal Hukum Volkgeist*, *4*(1), 17–25.