THE LEGAL STRATEGY OF TREATING TELEMATICS CRIMES IN THE FIELD OF ELECTRONIC TRANSACTIONS IN GLOBAL TRADE

Dian Alan Setiawan
Universitas Islam Bandung
dian.alan@unisba.ac.id

Abdul Rohman
Universitas Islam Bandung
abdul.rohman@unisba.ac.id

Fabian Fadhly Jambak
Universitas Islam Bandung
fabianfadhly.j@unisba.ac.id

Alfiyan Umbara
Universitas Islam Bandung
alfiyanumbara01@gmail.com

Mia Oktafiani Mulia
Universitas Islam Bandung
miaoktafiani.momu@gmail.com

Abstract

Economic globalization that is sweeping the world today began with the development of transportation facilities and cross-border trade. One of the facilities in the internet world to support economic activity is Electronic Transactions. In Indonesia, problems that arise due to the use of transaction media through telematics technology continue without being followed by the existence of laws that regulate it (cyber law). This study aims to determine legal policies against crime in electronic transaction activities in various sources of positive criminal law in Indonesia and to determine strategies for overcoming telematics crimes in the field of electronic transactions in global trade. This research is a normative legal research that is finding a rule of law, legal principles, and legal doctrines in order to answer the legal issues faced. The results of this study explain the legal policy against crime in electronic transaction activities in various sources of positive criminal law in Indonesia carried out in two stages, namely the Applicative Stage and the Formulation Stage and explain the Legal Strategy for Combating Telematics Crime in the Field of Electronic Transactions in Global Trade which is carried out through the Penalty Policy and non-penal policy.

Keywords: *Crime; Electronic; Prevention; Telematics; Transactions.*

A. INTRODUCTION

The globalization of the economy that is sweeping the world at this time began with the development of transportation facilities and cross-border trade. However, the acceleration of development along with its influence and impact on the "severe" felt in the last decade, especially for developing countries. Many observers argue that the key aspects of globalization are investment, trade and monetary liberalization supported by advances in electronic technology.[1] Computer technology as the basis for the development and use of electronic media, has grown rapidly since Jack S. Kilby invented the microchip. The latest generation of computer technology development by combining information technology with telecommunications (telematics) has now entered the era of "virtual communication". One of the media created by telematics technology is the internet which is a means of communication, access, information, entertainment, and various purposes that have many business advantages compared to conventional media, including: faster, more practical, efficient, private and relatively cheaper.

One of the facilities provided on the internet to support economic activities, especially in the field of investment and monetary trade is "Electronic Transactions". The advantages of Electronic Transactions compared to conventional transaction media include: ease of payment, many choices, faster and more practical transaction processing, a very wide range of promotions, allowing for direct relationships between producers, distributors and consumers and others.[2]

The basic difference between transaction activities through electronic media in cyberspace and manual transactions in the real world can be seen in the following chart:[3]

Table 1. The difference between transaction activities through electronic media in the virtual world and manual transactions in the real world

Manual Transaction	Electronic Transaction
Paper Based	Paperless
Clear parties	The parties are not clear
The transaction path is recorded/recorded (there is proof of delivery, proof of order, proof of receipt, etc.)	The transaction path is difficult to trace
Validate with signature or initial or	Validate with digital signature or

1 Khor, Martin, *Globalisasi Perangkap Negara-Negara Selatan (Globalization and the South: Some Critical Issues, Alih Bahasa:* AB. Widyanta & Scholastika Siane), Cinderelas Pustaka Rakyat Cerdas, Yogyakarta, 2001, Page.12

2 Aria, Dion, *Bill E-Commerce Overview*, Bahan Seminar Sehari "Cyber Law 2000", Bandung, 2000,

3 A.l Wisnusubroto, *Strategi Penanggulangan Kejahatan Telematika*, Atmajaya Yogyakarta, Yogyakarta, 2010, page.111

stamp (Note: real signature functions as an acknowledgment and acceptance of the contents of the message/document)	even without validation (note: Digital Signature serves as message integrity)

Some of these basic differences raise serious problems related to the certainty of legal relationships and legal protection against the threat of computer misuse in cyberspace (cybercrime). In Indonesia, the problem is complex because of the rapid development of telematics, especially those relating to the use of transaction media through telematics technology, without being followed by the existence of laws that regulate and cover it (cyber law). Whereas the phenomenon of violations in electronic transaction activities is growing along with the increasing use of IT in Indonesia. Violations in technology are motivated by various purposes ranging from those with fad motives to those based on motivations that lead to criminal acts. The increasingly complex problems in the global economic system supported by technological advances (especially IT) must be balanced with adequate economic laws. Likewise, the development of the quantity and quality of crime due to irregularities in the activities of the economic system needs to be prevented by the existence of appropriate criminal laws in the economic field.

The increasingly complex problems in the global economic system supported by technological advances (especially IT) must be balanced with adequate laws in the economic field. Likewise, the development of the quantity and quality of crime due to irregularities in the activities of the global economic system needs to be prevented by the existence of appropriate criminal laws in the economic field. However, until now it is still a problem when the existence of criminal law in the economic field is increasingly difficult to reach deviations in economic activity in the era of global trade which has different characteristics from traditional economic systems and is complex. Meanwhile, regulatory policies in the field of economic criminal law, apart from running slowly, are also not based on clear concepts.

Globalization of technology in law and economics is seen as a result of the development of information technology, especially in the use of cyberspace as an electronic communication media to spread information throughout the world. This change causes anything that comes into contact with this information technology to be adjusted, so that globalization also demands changes in trade, investment, information technology, and so on policies that provide more flexibility for capital, technology, and labor to move easily between sovereignty country territory.[4]

Moving on from the background as described above, the basic problems in the legal field, especially economic criminal law in order to

4 Advento Jeronimo, The Globalization Affect of Law And Economic On Cybercrime, *Jurnal Pembaharuan Hukum FH Universitas Islam Sultan Agung*, Vol.6 No.3, 2019, page.394

overcome crime in electronic transaction activities can at least be formulated legal issues and problems, including how is the legal policy (penal policy) against violations/crime in transaction activities in various sources of positive criminal law in Indonesia (Criminal Law in the field of economics and the ITE Law) and What is the legal strategy for overcoming telematics crime in the field of electronic transactions in global trade

The purpose of this study is to examine the application of the law to violations/crime in activities electronic transactions contained in various sources of positive criminal law including criminal law in the economic field in Indonesia and the ITE Law which are considered inadequate as well as anticipatory efforts and strategies for overcoming telematics crimes in the field of electronic transactions in the era of global trade. In addition, the novelty of this research is to examine micro-crime prevention strategies in the field of electronic transactions in the era of global trade which has not been found in previous studies.

B. RESEARCH METHODS

The research method used in this study is a normative juridical research method, namely research that is focused on examining the application of rules or norms in positive law.[5] Normative juridical is legal research conducted by examining library materials or secondary data as the basic material to be investigated by conducting a search on regulations and literature related to the problem under study.[6] The author uses a statutory approach and a conceptual approach.[7] Meanwhile, the data collection method in this study was carried out through library research by conducting a search on legal principles, legislation and other documents related to the problem under study.[8]

C. RESULT AND DISCUSSION

In general, electronic transactions are legal relationships that are carried out and/or generated through an electronic system. The tangible forms of electronic transactions include "electronic commerce or better known as "Electronic Commerce" (e-commerce) and "Electronic Fund Transfer" or known as EFT. The definition of e-commerce is all forms of trade transactions/trade in goods or services (trade of goods and services) using electronic media.[9] In another source it is stated that "electronic commerce may be broadly defined as the automation of the commercial

5 Johny Ibrahim, *Teori dan Metodologi Penelitian Hukum Normatif*, Bayumedia Publishing, Malang, 2012, page.30

6 Soerjono Soekanto dan Sri Madmuji, *Penelitian Hukum Normatif*: Suatu Tinjauan Singkat. PT Raja Grafindo Persada, Jakarta, 2015, page.15

7 Peter Mahmud Marzuki, *Penelitian Hukum,* Cet. 6, Kencana Prenada Media Group, Jakarta, 2010. page.21

8 Marzuki, *Penelitian Hukum,* page.21

9 Arrianto Mukti Wibowo et.al., *Kerangka Hukum Digital Signature Dalam Electronic Commerce, Hasil penelitian yang dilaksanakan oleh Grup Riset Digital Security dan Electronic Commerce*, FIKOM UI, Jakarta, 1993, page.3

transactions through the use of computers and telecommunications to exchange and process information, transactional documents and forms of payment".[10] While what is meant by EFT is a series of activities in carrying out orders from the original sender which aims to transfer a certain amount of funds to the recipient mentioned in the transfer order, all of which are carried out by electronic media. Because electronic transactions are a legal relationship, to ensure their security, a set of norms is needed to regulate the parties involved in transactions. Likewise, if there is a disturbance in the security of the implementation of electronic transactions as a result of irregularities that lead to criminal acts.

1. Threats of Hackers and Cyber Crime in Electronic Transactions

Technological crimes in electronic transaction activities are part of various forms of modus operandi in cybercrime whose perpetrators are commonly referred to as Hackers. Therefore, the discussion of telematics-based technological crimes as a medium for electronic transactions cannot be separated from the discussion of the problem of the existence of hackers in cybercrime.

Hacker or a more precise term is Cracker,[11] is the most feared term in the internet world. In the literature Hacking is defined as a connection by adding a new computer terminal to a computer network system against the law (illegal) or without the permission of the rightful owner of the computer network.[12] In other sources, this act is known as: Computer Trespass as for example in Article 9A (new) Victoria Crimes Act it is determined that: "Computer trespass: .... Access to, or enter, a computer system or part of a computer system without legal authority to do so… "[13]. So actually at first the actions of these hackers were just a fad act which was generally based on a challenge or adventure motivation.[14] In America, it is known as a legendary hacker named Kevin Mitnick who with his expertise managed to penetrate the data defense system of the NORAD computer center (North American Defense Command)[15]. In Germany, known as "Maskerade" for password crackers, one of the initial modes carried out by hackers before carrying out further actions such as stealing and duplicating credit card numbers,

10 Abu Bakar Munir dan Siti Hajar Hj Mohd Yasin, Legal Issues in Cyberspace Contracting, *The Malayan Law Journal*, 1997, page. 185

11 Suheimi, *Kejahatan Komputer,* Penerbit Andi Offset, Yogyakarta, 1995, page. 104-106

12 Andi Hamzah, *Aspek-aspek Pidana di Bidang Komputer*, Sinar Grafika, Jakarta, 1987, page.136

13 Al. Wisnusubroto, *Kebijakan Hukum Pidana Dalam Penanggulangan Penyalahgunaan Komputer***,** Penerbit Universitas Atma Jaya Yogyakarta, 1999, page.34

14 Anita Rosenz, New York, 2000, page.24

15 U.S Department of Justice Report, May 9 2010 (*http//www.cybercrime.gov*) accessed on March 25 2021

copying and selling computer software via the internet illegally or hijacking people's phone numbers (hacker phone)[16].

Recently, the actions of these hackers/crackers have become increasingly reckless and lead to criminal acts based on the motivation of stealing, damaging, threatening, disrupting and other criminal acts. Another way to break into a site or system on a computer network is known by various technical terms such as: Probe, Scan, Account Compromize, Root Compromize, Sniffer, Denial of Service (DoS), Malicious Code. Whether it's a fad or especially one that leads to criminal acts, the actions of hackers/crackers are very disturbing and very detrimental to both network owners, site owners and other users so that efforts to overcome them need to be considered.

Technically, countermeasures have been taken by improving an adequate computer security system. The usual form of security is to use a password or password to be able to access a computer network system. This fact demands a legal approach to overcome the actions of hackers, namely by imposing criminal sanctions for criminals in cyberspace.

2. Modus Operandi of Crime in Electronic Transactions

Electronic and digital systems emerge from the creative minds of their creators through logic gates in computer technology. In its development, these logic gates open up opportunities to be used in a deviant way so that new crimes arise. Along with the development of banking technology, various banking service facilities have emerged that help make the transaction process facilitated by the Bank easier, faster and more accurate. However, the use of high technology and online systems in the banking system has also opened up opportunities for abuse in the form of unauthorized transfers of funds. The modus operandi can vary, from breaking into an ATM machine to various cracking variations in the Internet Banking system.

Recently, what is becoming a trend in the issue of electronic transactions is the misuse of the internet in electronic commerce (e-commerce) which is most often done by hackers in Indonesia is shopping for free through online shop sites. This method is done by using someone else's credit card after the perpetrator has succeeded in breaking into that person's e-account or creating a fictitious account to obscure tracking. How to sabotage other people's credit cards can be done semi-manually, for example, starting with peeking at the pin numbers on other people's credit cards at the hotel reception or at cashiers of large supermarkets that accept credit card payments. The latest development of hackers has found a new pattern after being fed up with randomizing "online stores" and looking to penetrate "online banks" is still a high risk. Now they start by accessing fixed gambling

16 Richard Benda, *Kriminalitat im Internet,* IPA Austria, (http://www.ipa.at/inetcrime.htm), 1998, accessed on April 10 2021

games with credit card abuse mode, where if the perpetrator loses, the payment of the bet is charged to someone else's account, but if the player wins the result is automatically transferred to his personal account. Another mode is to break into the system of cellular phone providers such as Telkomsel, Xl, Axis, Smartfren etc. The hackers then top up their cellular phone credits that have run out or flood the credits on the beautiful numbers that are being marketed beyond capacity so that the beautiful numbers cannot be used and become unsold.

It turns out that the potential for misuse of e-commerce does not only come from hackers but it is also possible for providers of goods/services to be carried out on the internet. This may happen because in e-commerce, consumers practically cannot see directly who the seller is, how the condition of the shop is intended and how the condition of the goods to be purchased is. What if after the account on the consumer's credit card was debited to the seller's account, but it turned out that the goods did not arrive because the shop was fictitious or the goods received by the consumer did not match what was offered on the online shop site. The modus operandi of criminality in electronic transactions as described above is expected to continue to grow, especially with the opening of the import-export system through EDI (Electronic Data Interchange). It appears that in various modes these are not only disturbing but more than that, they are very detrimental to other people or other corporations who are victims, even at a certain level can damage the image of a country. Worse yet, if the hacker's actions are not immediately addressed, it will damage the existing values in Indonesia which will trigger more and more hackers to commit criminal acts because they consider actions using computers on the internet system as legal acts because there are no rules. the law or even though there is now an ITE Law, law enforcement officials still have very limited capabilities in enforcing it.

3. Analysis of Legal Policy Against Violations/Crime in Electronic Transaction Activities in Various Positive Criminal Law Sources in Indonesia (Criminal Law in the Economic Sector and the ITE Law)

a. Penal Policy at the Applicative Stage: Operational Strategy for Various Sources of Criminal Law in the Economic Sector

An urgent problem to think about in order to find a solution is what about cybercrime cases that have started to occur in Indonesia, especially after the e-commerce "boom" since 2000, while in Indonesia until now even though it has an ITE Law which is often claimed as a cyber law. first, but it is considered not perfect, especially because it often causes problems in its application in solving criminal cases in e-commerce activities. In accordance with the legal system that underlies the practice of Indonesian (criminal) justice which relies on a codification system, law enforcement officers

are required to operationalize the provisions contained in positive criminal law against criminal cases that arise with an interpretive approach.

The sources of positive criminal law in the Indonesian economy from the general to the specific can be classified into four sources, namely:

1) The provisions contained in the codification system, namely the Criminal Code in general, are articles related to offenses against assets, for example articles on theft, fraud, embezzlement;
2) Provisions contained in the Act that amend or add to the provisions contained in the Criminal Code, for example Act No. 1 of 1960 which contains aggravating criminal threats for articles 359, 369 and 188 of the Criminal Code, Act No. 7 of 1974 concerning Gambling Control, Act No. 4 of 1976 concerning Aviation Crimes;
3) Provisions contained in the Special Crimes Act, for example Act No. 31 of 1999 concerning the eradication of corruption in conjunction with Act No. 20 of 2001 concerning amendments to Act No. 31 of 1999;
4) Provisions contained in the administrative law legislation that contain criminal sanctions. For example, criminal provisions in the Banking Law, criminal provisions in the Copyright Law;
5) The provisions contained in the laws and regulations that most specifically regulate the issue of Electronic Transactions such as Act No. 19 of 2016 concerning Amendments to Act No. 11 of 2008 concerning Information and Electronic Transactions

In accordance with the principle of *lex specials derogate legi generalis*, the method of its application to concrete cases must be traced from the most specific sources of criminal law to the most general. In criminal law, there are various methods of interpretation, ranging from grammatical interpretation to analogous interpretation. In connection with the principle of legality (*nullum delictum*) which is the main joint in criminal law, efforts are made to avoid analogous interpretations. To be able to ensnare cybercrime for which there are no rules in the sources of criminal law in Indonesia, it must first be observed the legal events by looking at the elements, nature and motivations as well as the ultimate goal or consequences/impact of the actions of the hackers/crackers. The next step is to look for the provisions contained in positive criminal law sources with the most relevant elements to be then applied with interpretive methods known in legal science and the last step is to apply them to concrete cases.

An example of an act carried out by a Carder (carding actor: shopping for a number of items with someone else's credit card number through e-commerce facilities), then there are two steps of

interpreting the provisions in the Criminal Code that can be applied to the perpetrator).

1) The act of snooping on someone else's credit card pin number, either for direct use or duplicating, can be interpreted as theft which can be described as follows:
   a) By knowing the credit card number, the right to use the credit card passes to the perpetrator, this can be interpreted as an element of "taking"
   b) The value of a credit card lies in the number, so the interpretation of the element of "something" is not limited to the card but also the number;
   c) The credit card number clearly does not belong to the defendant
2) The act of the perpetrator manipulating the credit card number to take money or goods through e-commerce access, can be interpreted as an act of "fraud" (article 378 of the Criminal Code), another possibility is to apply more specific provisions such as Act No. Article 40 in conjunction with Article 56) and (Article 22 in conjunction with Article 50)

The two examples of the application of the law as described above show that through a progressive legal interpretation strategy, crime cases in the field of electronic transactions (in this case carding) can be resolved by the Criminal Code and the Telecommunications Law. Now Indonesia has a special law on electronic transactions, namely Act No. 11 of 2008 concerning Information and Electronic Transactions (UU ITE) which also regulates violations, criminal provisions and sanctions. Even though there is no single article that specifically regulates carding matters, through contextual interpretation, several provisions in the ITE Law that can be applied are:

1) If the method of "peeking" the credit card number is done by tapping the transaction activity between the card owner and the online shop via internet (e-commerce) then the perpetrator can be subject to Article 31 paragraph (1) or (2) which regulates the issue of "illegal interception "In conjunction with Article 47 of the ITE Law which regulates the sanctions"
2) The act of using another person's credit card number to outsmart the online store so that the perpetrator can shop for a number of items without paying, can be subject to Article 35 of the ITE Law which regulates "computer-related forgery" problems in conjunction with Article 51 paragraph (1) which regulates the sanctions read textually, the articles in the ITE Law are indeed only related to electronic information/documents, but with reference to the notion that Electronic Transactions are legal acts carried out using computers, computer networks and/or other

electronic media, the meaning of violations related to electronic information/documents also includes electronic transaction activities which are legal actions with electronic media.

As part of the crime prevention strategy in electronic transactions, the penal policy in applying the relevant positive criminal law in several carding cases that have occurred in Indonesia does not appear to be a problem. Even though it is not correct because there are no provisions that specifically regulate crimes in the field of electronic transactions and perhaps also because of the limited knowledge of law enforcement officials regarding the ins and outs of IT, the efforts and courage to interpret various sources of positive criminal law are deemed relevant and need to be rewarded to continue developed. Even if in the investigation/proofing process other special elements are found, it is possible to apply provisions from various other sources of criminal law. For example: if there is a motivation to enrich oneself illegally and cause state financial losses, the provisions in the Corruption Eradication Law can be applied if the intrusion is followed by an act of illegally copying programs or important copyrighted data contained in the hacked site, then it can Copyright Law is applied.

To be able to use the interpretation method (interpretation) optimally in order to find and apply the law in solving cybercrime cases, especially in electronic transaction activities by means of criminal law, the following steps and supporting factors are needed:[17]

1) Improving the quality of human resources for law enforcement officers (Judges, Prosecutors, Police, Lawyers) especially their knowledge in the fields of legal science and computer/cybermedia technology.[18] To support the improvement of the quality of human resources for law enforcement officers, it is necessary to support the availability of jurisprudence relating to cases of misuse of computers, literature and experts in the field of multimedia;
2) In dissecting cases of cybercrime in general and criminality in electronic transactions in particular, law enforcement officers need to refer to the reference results of studies and anticipation of the modus operandi of various computer abuse cases, both real cases and simulation results. This surgery is needed to clearly reveal the legal events;
3) In exploring positive criminal law legislation in order to find provisions relevant to the cybercrime case being handled, law enforcement officers need to be supported by the availability of adequate and easily accessible legal documentation and information system;

17 Wisnusubroto, *Strategi Penanggulangan Kejahatan Telematika,* page.127
18 Benda, *Kriminalitat im Internet* , page.3

4) Furthermore, the results of the search for statutory provisions and the results of surgery on cybercrime cases are analyzed and examined for the relationship or equivalence of the elements through the interpretation method in order to find the law to be applied to the inconcreto case. In carrying out this interpretation one should abandon the legal-formalistic mindset;
5) The results of the discovery and application of the law are used as study material for models or references in the settlement and handling of cybercrime cases in general and crime in electronic transactions in particular.

b. Penal Policy at the Formulation Stage: Future Cyber Crime Law Regulatory Strategy

From the previous discussion that by optimizing the interpretation method, several provisions in various sources of criminal law that exist in Indonesia at this time can be applied to criminal cases in electronic transactions, but it must be acknowledged that in many cases this application has limitations, including the ineffectiveness of interpretation that is too broad and inadequate criminal sanctions compared to the impact of cybercrime. The presence of the ITE Law does not appear to have been able to answer the problem in overcoming the development of crime in the field of Electronic Transactions.

Compared to several other countries such as the USA with the Illinois Electronic Commerce Security Act 1998, Singapore which already has The Electronic Transaction Act 1998 or even Malaysia has Cyber Laws consisting of the Digital Signature Act 1997 (Act 562) and Regulation 1998, Computer Crimes Act 1997 (Act 563) and Telemedicine Act 1997 (Act 564), so in terms of Cyber Law regulation, Indonesia is one that is lagging behind because it only had the ITE Law in 2008. In relation to crime in the era of Global Transformation, currently the source of positive criminal law in Indonesia is only one UU ITE which regulates actions that generally include cybercrime, so that the formulative or legislative stage occupies an important role in realizing legal certainty in overcoming cybercrime through criminal law means. With regard to new forms of crime in this globalization era, such as computer abuse or especially cybercrime, the first thing that must be determined is the form of regulation. There are several options in managing the problem of irregularities in electronic Transaction activities, namely:

1) Become part of the regulations in the field of Cyberlaw. For example, by regulating in the form of criminal provisions in the Electronic Transaction Law. It seems that this model was then (temporarily) chosen in Indonesia, namely with the ratification of Act No. 11 of 2008 concerning Information and Electronic Transactions;

2) Specially regulated by means of regulated in a special Law on Computer Misuse/Cybercrime or regulated in a special chapter in the Criminal Code. This model is also an alternative for Indonesia's cybercrime law regulations in the future;
3) Integrated into the codification system (KUHP) by adding/updating articles in the Criminal Code. This model also appears to have been adopted in the RKUHP (2019 draft)

To determine the choice, conceptually must consider the legal system (criminal) in Indonesia. Even though Rene David once said that the legal system in Indonesia is a "mixed system law", in the field of public law, especially criminal law, the continental legal tradition appears to be more prominent in the practice and development of legal science. Therefore, if after reviewing it turns out that there is no fundamental difference between the nature of the actions committed in cyberspace and actions in the real world, then the development of regulations regarding cybercrime issues. However, if a fundamental difference is found regarding actions in cyberspace with actions in the real world, then it is possible that the regulatory model will lead to the second option (specifically/separately regulated) or the first choice (becoming part of cyberlaw) if the situation and needs are deemed very urgent.

With the reality of the legal system that underlies the development of criminal law in Indonesia, the integration of various types of modus operandi of new criminal acts into the codification system is based on the idea that the regulation of criminal acts is patterned, systematic, guaranteed certainty, flexible and makes it easier to operate, but if forced to be integrated into codification it turns out that it will damage the system in it, so it should be arranged separately. Furthermore, the two central problems in penal policy are determining and formulating what actions should be made into criminal acts and what sanctions should be used or imposed on the violator.[19]

The step to determine the act that should be made a criminal act must go through the process of criminalizing the act. In various literatures, various considerations of criminalization/decriminalization of actions have been put forward by various experts.[20] In relation to cybercrime problems in general, there are three points that need to be considered in criminalizing the actions of hackers/crackers, namely:[21]

1) Actions that are truly harmful and can cause serious excesses (selective and limitative principles) should be chosen so that the

19 Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, Citra Aditya Bakti, Bandung, 1996, page.32
20 Sudarto, *Hukum dan Hukum Pidana*, Alumni, Bandung, 1977, page.44-48
21 Wisnusubroto, *Strategi Penanggulangan Kejahatan Telematika*, page.132

regulation of acts categorized as cybercrime is not overcriminalization so that it will have a counterproductive impact on the development of computer technology in the multimedia field, which is very much needed by the state. Indonesia in facing the era of globalization;

2) It should be considered whether the costs that must be incurred to draw up provisions governing computer offenses categorized as complex and complex cybercrimes, the costs of supervising and enforcing these provisions that require high-tech facilities or means and the burden that must be hit by the victim will be balanced with the result is a situation of law and order in the cyber world (cost and benefit principle);
3) The capacity or working capacity of law enforcement agencies in Indonesia should be considered which will later be tasked with enforcing the provisions governing computer offenses categorized as cybercrime, so that there is no overblasting task load so that many regulations/stipulations are made in fact in practice in the field cannot be enforced.

In connection with the considerations above, it is necessary to determine actions that are categorized as cybercrime, besides of course having to pay attention to the fundamental values of society which will be safeguarded by the social, cultural, political and economic situation and condition of the Indonesian state, especially those related to the complexity of law enforcement issues in Indonesia. Indonesia also cannot be ruled out that the results of the criminalization of such acts should be formulated in a provision that is flexible and too technical, and it is equally important to pay attention to synchronization and harmonization with existing similar regulations.

Violations of the law with information technology instruments are often difficult to solve, because in addition to illegal acts, they are committed by subjects who use advanced technology and are difficult to trace. These activities are often carried out from outside the territory of Indonesia or vice versa where the subject is in Indonesia, but the modus operandi and lex locus delicti are outside Indonesia, this causes the proof to be more difficult than ordinary acts against the law.[22] The steps for determining criminal sanctions for violators are seen as being able to follow a general pattern. This means that until now there has been no specific form of sanctions against criminal behavior in the internet world. In determining the severity of the sanctions, it is necessary to consider the image that appears as a result of the perpetrator's actions, in addition, it is also necessary to consider the appropriate form of treatment for perpetrators whose

22 Asep Ahmad Fauzi, Penerapan Prinsip UNCITRAL Model Law Dalam Pembuktian Kasus Transaksi Elektronik di Indonesia, *Jurnal Hukum UBELAJ FH Universitas Bengkulu*, Vol. 02 No.1 Tahun 2017. page.93

actions are motivated by mere fad, challenge or adventure motives. Determining the form of action to be criminalized, formulating actions and determining sanctions to support law enforcement, it is necessary to have supporting instruments such as ratification of extradition treaties and diplomatic relations between countries considering that cybercrime acts are generally transnational in nature which is very difficult to reach solely with national law.

Cybercrime as an impact of globalization that causes a lot of losses in various fields, the handling must be maximized, given the perpetrators of violations often become difficult to be snared because the law and the court does not have jurisdiction against perpetrators and legal actions that occur, given the violation of the law is transnational but the result actually has implications law in the country.[23] Various models of cyberlaw regulations from various countries that already have them should be used as comparisons in preparing cyberlaw in Indonesia, at least global signs such as the UNCITRAL Model Law on Electronic Commerce (adapted December 16, 1996), UNCITRAL Draft Rules on Electronic Signature (July 10, 1996). 1998) and the Uniform Electronic Transaction Act (September 1998 draft), as well as the EU Convention on Cybercrime (ratified in Budapest, 23 November 2001), need to be considered by taking into account and adapting to special conditions in Indonesia.

4. Analysis of Legal Strategy for Combating Telematics Crime in the Field of Electronic Transactions in Global Trade

One of the products of the globalization of crime, namely cybercrime, where crimes are committed are not only limited to space and time. The acceleration of modern transportation, communication and information gave birth to the globalization of technology that affects the globalization of crime (globalization of crime).[24] The criminal law policy (criminal policy) in overcoming this is *warmaking* criminology or harm creating on crime which is hostile (adversarialism) as a repressive approach and combined with a preventive approach of mutualism or togetherness on the basis of peacemaking criminology.[25]

In tackling cybercrime, comprehensive efforts are needed both through criminal law and through criminal law channels. Crime prevention and control is carried out with an integral approach between penal policies and non-penal policies. The penal policy has several limitations and weaknesses, namely it is pragmatic, individualistic (offender oriented), more repressive and must be supported by infrastructure that requires high costs. Thus, crime prevention is better

23 Jeronimo, *Law And Economic On Cybercrime*, page.387

24 Muladi dan Diah Sulistyani R.S., *Kompleksitas Perkembangan Tindak Pidana dan Kebijakan Kriminal*, Alumni, Bandung, 2016, page.24

25 Muladi dan Diah, *Kebijakan Kriminal*, page.24

done by using non-penal policies that are preventive in nature.[26] Policies in overcoming cybercrime can be carried out in two ways, namely:

a. Penal Policy

Policies related to the use of criminal sanctions in the settlement of crime cases in cyberspace. Penalty policy can be done in the following ways:

1) Criminalizing actions in the law so that these actions include crimes in cyberspace/telematics

The rule of law basically determines that the rule of law guarantees state order and public order.[27] Indonesia is a state of law, so the imposition of legal sanctions must be preceded by criminalizing an act so that it can be classified as a criminal act. Criminalization can occur because of the development of society which is supported by advances in science and technology.[28] Criminalization needs to be carried out taking into account the legal interests that are protected so that over-criminalization does not occur. Criminalization does allow chaos in the legal structure of telematics. Strictly Jonathan Mayer said as follows:[29]

The structure of cybercrime law generates the potential for two different types of redundancy. First, a cybercrime offense might be internally redundant, overlapping with other cybercrime offenses within the same statutory scheme. Second, a cybercrime offense might be externally redundant, overlapping with non-cybercrime civil claims or criminal charges.

In formulating an action that needs to be classified as a criminal act or not, legislators need a line between personal protection on the one hand and freedom of expression on the other. Zubair Kasuri, Flare said "Civil and human rights activists contend that the law would put unnecessary curbs on freedom of expression on the internet. According to them, it will give undeterred powers to the law-enforcement and investigation authorities to harass innocent people in the name of national security.[30] " Civil and human rights activists argue that the law will prohibit restrictions on freedom of expression on the internet. According to them, it would give law enforcement and investigative authorities unfounded powers to harass innocent people in the name of national security. Indonesia to date only has a draft law on personal data protection (not yet ratified).

26 Hatta, *Kebijakan Politik Kriminal; Penegakan Hukum dalam Rangka Penanggulan Kejahatan*, Pustaka Pelajar, Yogyakarta, 2010, page.39

27 Sri Widoyati Wiratmo Soekito, *Anak dan Wanita dalam Hukum*, LP3ES, Jakarta, 1983, page.85

28 Andi Hamzah, *Aspek-aspek Pidana di Bidang Komputer*, page.28

29 Jonathan Mayer, Cybercrime Litigation, *University of Pennsylvania Law Review*, Vol. 164, 2016, page.1485-1486

30 Zubair Kasuri, Karachi Flare, Cybercrime Prevention Law Takes Effect, *Karachi*, Vol. 12 No.11, Aug 2016, page.28

Provisions regarding personal data have indeed been regulated in Article 26 of Act No. 19 of 2016 concerning Amendments to Act No. 11 of 2008 concerning Information and Electronic Transactions, but it is deemed not sufficient to protect the spread of personal data that is vulnerable to occur in cyberspace. In addition, the issue of child pornography has not yet become an independent legal rule so that this crime is only threatened with an aggravated punishment compared to when it involves adults.

2) Harmonization of national legal provisions with international law in eradicating cybercrime

Sigid Suseno describes that there has been an approach between a global approach and an evolutionary approach which has resulted in a compromise approach that is in accordance with the characteristics and categorization of cybercrime.[31] The evolutionary approach is carried out by amending the non-criminal formula, both the object and the ways in which criminal acts are carried out against computer related offenses from traditional crimes contained in the Criminal Code and regulated in special laws outside the Criminal Code. A global approach is taken to the confidentiality integrity, and availability of computer data or computer systems or electronic systems by establishing new arrangements in special laws.

The National Legal Development Agency (BPHN) in its final report on "EU Convention on Cybercrime Study associated with Information Technology Crime Regulatory Efforts" stated that in drafting regulations in the cybercrime field, Indonesia has several alternative strategies that can be done, namely by:[32]

a) Develop criminal law through the preparation of positive legal norms that can reach crimes in the field of information technology.
b) Adopting global cybercrime regulatory principles from a model of international legal norms into a national regulation.
c) Ratify or access the 2001 EU Convention on Cybercrime in Budapest, and then prepare regulations and implementing regulations at the national legal level.
d) Law enforcement through the imposition of criminal sanctions for cybercrime perpetrators.

In modern law, the use of law as a means of community engineering (law as a tool of social engineering) is carried out by involving lawmakers by formulating sanctions as a means of law enforcement. Law enforcement is carried out to bring about

31 Sigid Suseno, *Yurisdiksi Tindak Pidana Siber,* Refika Aditama, Bandung, 2012, page.198

32 Badan Pembinaan Hukum Nasional (BPHN), *Kajian EU Convention on Cybercrime dikaitkan dengan Upaya Regulasi Tindak Pidana Teknologi Informasi*, Departemen Hukum dan Hak Asasi Manusia Republik Indonesia, Jakarta, 2009, page.7

effective change in society.[33] Law enforcement is carried out to fulfill the value of justice, especially for victims. The value of justice occupies a vital and essential element in the formation, application and enforcement of the law. The value of justice is an absolute requirement in the life of society, nation and state in accordance with the ideals of Pancasila law.[34] The formulation of the law of telematics has not yet reached the level of establishment. This is because this field contains complex elements. Regarding this, Marco Gercke stated as follows:[35]

> Introducing cybercrime legislation is not an easy task as there are various areas that require regulation. In addition to substantive criminal law and procedural law, cybercrime legislation may include issues related to international cooperation, electronic evidence and the liability of an Internet Service Provider (ISP). In most countries elements of such legislation may already exist – often in different legal frameworks. Provisions related to cybercrime do not necessarily need to be implemented in one single piece of legislation. With regard to existing structures, it might be necessary to update different pieces of legislation (such as amending an Evidence Act to ensure that it is applicable with regard to the admissibility of electronic evidence in criminal proceedings) or remove provision from an older law (for example in a Telecommunications Act) within the process of introducing new legislation.

b. Non-penal Policy

The politics of criminal law in overcoming cybercrime through penal means needs to be balanced with non-penal policies. Non-penal policies that can be implemented are as follows:[36]

1) Develop policies outside of criminal law that support cybercrime prevention efforts, such as through anti-hate policies, anti-bullying policies and healthy internet policies through the education system;
2) Conducting socialization of potential crimes in cyberspace by educating the internet user community not to include personal identities, transact in places with safe internet facilities and so on;
3) Build cooperation with the private sector to build a security system in cyberspace;

33 Suteki, *Hukum dan Alih Teknologi; Sebuah Pergulatan Sosiologis,* Thafa Media, Yogyakarta, 2013, page.19

34 Soejadi, *Refleksi Mengenai hukum dan Keadilan;; Aktualisasinya di Indonesia,* Aswaja Pressindo, Yogyakarta, 2017, page.56-57

35 Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal* Response,ITU Telecommunication Development Bureau, 2012, page.100

36 Dewi Bunga, Politik Hukum Pidana Terhadap Penanggulangan Cybercrime, *Jurnal Legislasi Indonesia*, Vol.16 No.1 March 2019, page.13

4) Establishing institutional networks in preventing cybercrime both at the national and international levels. International cooperation in overcoming cybercrime is very much needed considering that cybercrime is an organized transnational crime.

As a developing country, Indonesia must adapt to legal developments and strategies in overcoming telematics crimes. Legal politics in tackling cybercrime is carried out by developing a global strategy in preventing and enforcing laws against crimes in cyberspace, compiling responsive legal formulations and preparing institutions that can take quick action when problems occur in cyberspace.

D. CONCLUSION

Legal Policy Against Crime in Electronic Transaction Activities in Various Sources of Positive Criminal Law in Indonesia (Criminal Law in the Economic Sector and the ITE Law) is carried out in two stages, namely the Applicative Stage: Strategy for Operationalization of Various Sources of Criminal Law in the Economic Sector and the Formulation Stage: Cyber Crime Law Regulatory Strategy in the Future. The Legal Strategy for Combating Telematics Crimes in the Field of Electronic Transactions in Global Trade can be carried out through a penal policy, namely a policy related to the use of criminal sanctions in the settlement of criminal cases in cyberspace by criminalizing acts in the law so that these actions include crimes in cyberspace and committing crimes in cyberspace harmonization of national legal provisions with international law in eradicating cybercrime. Meanwhile, non-penal policies (beyond criminal), namely by formulating policies outside of criminal law that support efforts to prevent cybercrime, Conducting socialization of potential crimes in cyberspace by educating the internet user community, Establishing institutional networks in preventing cybercrime both at the national and international levels.

BIBLIOGRAPHY

Books:

Andi Hamzah, 1987, *Aspek-aspek Pidana di Bidang Komputer*, Sinar Grafika, Jakarta;

Al. Wisnusubroto, 1999, *Kebijakan Hukum Pidana Dalam Penanggulangan Penyalahgunaan Komputer***,** Penerbit Universitas Atma Jaya Yogyakarta, Yogyakarta;

_____2010, *Strategi Penanggulangan Kejahatan Telematika*, Atmajaya Yogyakarta, Yogyakarta;

Anita Rosen, 2000, *The E-Commerce: Question an Answer Book*, American Management Assiciation, New York;

Arrianto Mukti Wibowo et.al., 1999, *Kerangka Hukum Digital Signature Dalam Electronic Commerce, Hasil penelitian yang dilaksanakan oleh Grup Riset Digital Security dan Electronic Commerce*, FIKOM UI, Jakarta;

Barda Nawawi Arief, 1996, *Bunga Rampai Kebijakan Hukum Pidana*, Citra Aditya Bakti, Bandung;

Badan Pembinaan Hukum Nasional (BPHN), 2009, *Kajian EU Convention on Cybercrime dikaitkan dengan Upaya Regulasi Tindak Pidana Teknologi Informasi*, Departemen Hukum dan Hak Asasi Manusia Republik Indonesia, Jakarta;

Hatta, 2010, *Kebijakan Politik Kriminal; Penegakan Hukum dalam Rangka Penanggulan Kejahatan*, Pustaka Pelajar, Yogyakarta;

Johny Ibrahim, 2012, *Teori dan Metodologi Penelitian Hukum Normatif*, Bayumedia Publishing, Malang;

Khor, Martin, 2001, *Globalisasi Perangkap Negara-Negara Selatan (Globalization and the South: Some Critical Issues, Alih Bahasa:* AB. Widyanta & Scholastika Siane), Cinderelas Pustaka Rakyat Cerdas, Yogyakarta;

Laudon, K. C., & Traver, C. G., 2016, *E-Commerce: Business, Technology, Society. 12th Edition*, Pearson Education, Edinburgh, United Kingdom (UK) ;

Marco Gercke, 2012, *Understanding Cybercrime: Phenomena, Challenges and Legal Response,* ITU Telecommunication Development Bureau;

Muladi dan Diah Sulistyani R.S., (2016), *Kompleksitas Perkembangan Tindak Pidana dan Kebijakan Kriminal*, Alumni, Bandung;

Peter Mahmud Marzuki, 2010, *Penelitian Hukum,* Ed. 6, Kencana Prenada Media Group, Jakarta;

Sigid Suseno, 2012, *Yurisdiksi Tindak Pidana Siber,* Refika Aditama, Bandung

Soejadi, (201, *Refleksi Mengenai hukum dan Keadilan: Aktualisasinya di Indonesia,* Aswaja Pressindo, Yogyakarta;

Soerjono Soekanto dan Sri Madmuji, 2015, *Penelitian Hukum Normatif*: Suatu Tinjauan Singkat. PT .RajaGrafindo Persada, Jakarta;

Sri Widoyati Wiratmo Soekito, 1983, *Anak dan Wanita dalam Hukum*, LP3ES, Jakarta;

Sudarto, 1977, *Hukum dan Hukum Pidana*, Alumni, Bandung;

Suheimi, 1995, *Kejahatan Komputer***,** Penerbit Andi Offset, Yogyakarta;

Suteki, 2013, *Hukum dan Alih Teknologi; Sebuah Pergulatan Sosiologis,* Thafa Media, Yogyakarta;

Journals:

Abu Bakar Munir dan Siti Hajar Hj Mohd Yasin, Legal Issues in Cyberspace Contracting, *The Malayan Law Journal*, 1997;

Asep Ahmad Fauzi, Penerapan Prinsip UNCITRAL Model Law Dalam Pembuktian Kasus Transaksi Elektronik di Indonesia, *Jurnal Hukum UBELAJ, FH Universitas Bengkulu,* Vol. 02 No.1 Tahun 2017;

Advento Jeronimo, The Globalization Affect of Law And Economic On Cybercrime, *Jurnal Pembaharuan Hukum FH Universitas Islam Sultan Agung*, Vol.6 No.3 Tahun 2019;

Bendle, M. N., Cyber Crimes: A Challenge to E-Commerce, *Our Heritage*, Vol.68 No.9, 2019;

Boateng, R., Olumide, L., Isabalija, R.S. & Budu, J., Sakawa: Cybercrime and criminality in Ghana, *Journal of Information Technology Impact*, Vol.11 No.2, 2011;

Jonathan Mayer, Cybercrime Litigation, *University of Pennsylvania Law Review*, Vol. 164, 2016;

Patel P., Patel, R., Patel, V. & Pathrabe, T., Survey Of Privacy And Security Issues In Spice World E-Commerce Website, *International Journal for Innovative Research in Science & Technology*, 2017;

Zubair Kasuri, Karachi Flare, Cybercrime Prevention Law Takes Effect, *Karachi* Vol. 12, No. 11, Aug 2016;

Dewi Bunga, Politik Hukum Pidana Terhadap Penanggulangan Cybercrime, *Jurnal Legislasi Indonesia*, Vol.16 No.1 March 2019

Regulation:

Act No. 19 of 2016 concerning Amendments to Act No. 11 of 2008 concerning Information and Electronic Electronic Transactions, Supplement to the State Gazette of the Republic of Indonesia Number 5952), Pub. L. No. 19 of 2016 (2016).

Internet:

Aria, Dion, 2000, *Bill E-Commerce Overview*, Bahan Seminar Sehari "Cyber Law 2000", Bandung

Richard Benda, 1998, *Kriminalitat im Internet*, IPA Austria, page 2 (http://www.ipa.at/inetcrime.htm)

U.S Department of Justice Report, May 9 2010 (*http//www.cybercrime.gov*)