Indonesia Prime, p-ISSN: 2548-317X, e-ISSN: 2548-4664
Vol. 2, No 1, November 2017, pp. 56-67

The application of criminal sanctions against violations of cybercrime

Sulaeman

West Sulawesi University Social and Politic Science Faculty Department Law
Email : sulaeman_rahman74@yahoo.co.id

ARTICLE INFO

Article history:
Received, July 15, 2017
Revised, September 30, 2017
Accepted, November 21 2017

Keywords:
Cybercrime
Criminal sanction
Violation of the law

ABSTRACT

The era of globalization led to the more sophisticated information technology so that it has brought an impact on the emergence of various forms of crime which affect modern nature greater than the conventional crime. The crime using a computer since long ago is the type of crime that is difficult to classify as a criminal offence at one side of the technology can see as a means to achieve the goal. On the other hand, however, the technology can also be seen as a human activity.

I. Introduction

As the development of an increasingly popular technology discussed in various media both print and electronic, by observers in newspapers, academics in a variety of scientific journals, including by the Government in the formation of laws – an invitation.

Each technology was created to meet the specific needs of a human being. Once created, the technology developed to be more effective and efficient to meet the needs in question; the final parts of the technology will abandoned. But after the technology invented and developed, the use of technology can match the purpose of the creation and development and outside the destination first, as is well known as a double-edged sword.

Technological developments increasingly expanded and became one of the computer technology, and the internet gave birth to a new world called the electronic world – a virtual space, or the internet which marks the start of a new era, that of the digital age or information era. Electronic world – a virtual space, or the internet is a new world that created because of unification between man and technology based on Science and marked the beginning of the digital age. Just as in a conventional world, then in the electronic world – a virtual space ' living ' society (cybersociety) consisting of millions of internet users from all over the world who communicate or interact with one another through the network the computer.

Today, the world has connected to the internet network. The Government of Indonesia itself, through a variety of the program, has developed a network of telecommunications and internet connection throughout all the territory of Indonesia, both the backbone of his or her last-mile up to the remote villages and out. The utilization of this technology for many areas also continue to develop, such as the development of e – government, e – commerce, e – ID card, and so on.

Talking about information and communication technologies that make the electronic world – a virtual space where people can be present without the need of physical existence; the existence and activity of human established through 0 and 1. Thoughts, emotions, and intentions of a person can realize through bits. However, just like the real world, in virtual space, too many of the crimes occurred more

often called cybercrimes. Crime in the virtual space can be either conventional or evil actions – actions which were later criminalization as a new form of crime that is only likely to occur in the room. By because that necessary rules and norms of the law applied in the electronic world – a virtual space to keep the order of the community including giving sanctions to perpetrators of crimes.

The term cyber-crime-laden also knows the crime of ordinary cyber with the use of computer and internet as well as a cross country need not always handling can be done by the conventional method or manner. In many cases, the completion of the crime requires cooperation cyber from various parties, including rule enforcement officers from other countries. Such cooperation can be implemented well if backed by an instrument well inform regional and international are by the national law of each party.

Information and communication technologies in addition to the enormous benefits, potential crimes in this field are also very large. Starting from the libel case, Government and private sites that hacked, fraud on the internet, and so forth, is an occurrence that can read almost every day in the news. Various attempts have been made, ranging from the creation of regulatory enforcement, socialization, and others.

Like the physical world, we have now, in the world of electronic virtual spaces of society requires setting both inter-Community as well as between the community, ranging from the norm up to the law. Technology and law are the two elements that influence each other and either also affect the community.

The settings on the principle approach are towards the attitude of follow up (behavior) of a person and a society against the offense is penalized by the State. Although world cyber is a virtual world, the law remains necessary to set community perpetrated the attitude at least for two reasons. The first community that exists in the world of virtual community that derived from the world real; the community has the value and interest of both singly or together that should protect. Second, although it happens in the world of virtual transactions carried out by the community influenced the real world, both economic and non-economic.

To address the various legal issues that arise in the world of electronics, the Government had established various regulations, including passes law number 11 the Year 2008 of the information and electronic transactions (UU ITE). In General, the settings in the UU ITE divided into two major parts, namely arrangements regarding electronic transactions and arrangements about the prohibited deeds (cybercrime).

As in the law on information and Electronic transaction is the one that makes the author's reference that is arrangements on acts that are prohibited (cybercrime), thus making the author wants to Browse more in the process and application of law criminal about cybercrime, the authors also choose and limit the area that will research in Parepare Town.

II. Literature Review

I. Crime

a. Understanding Crime

The notion of crimes according to the great Indonesian Language Dictionary (2008:557) is "evil deeds" that common people know or heard of the evil deeds such as murder, theft, sacrilege, fraud, abuse, insult and others is done by humans.

Crime is a complex phenomenon that can understand from many different sides, that's why in everyday life can be captured numerous comments about an event different crime with one another.

The effort to understand this crime was many centuries ago by the famous scientists thought.

According to Plato (Topo Santoso and Eva Hq, 2001:11) that: "gold, man is the source of much of the crime."

Furthermore, according to Aristotle (Topo Santoso and Eva Hq, 2001:11) States that: "the poverty cause crime of rebellion, a crime that not made to obtain what is necessary for life, but for luxury."

While Thomas Aquino (Topo Santoso and Eva Hq, 2001:11) States that:

Indonesia Prime, p-ISSN: 2548-317X, e-ISSN: 2548-4664
Vol. 2, No 1, November 2017, pp. 56-67

"the influence of poverty over evil IE rich people who live for pleasure and extravagant waste her wealth, if at any time the poor, then it is easy to be a thief."

The opinion of the scholars mentioned above then accommodated in science called Criminology. Criminology is a branch of science that emerged in the 19th century, which at its core is a science that investigates the causes of the causes for the crime. Up to now the limitation of the scope of Criminology there is still a wide difference of opinion among scholars.

According to Edwin h. Sutherland (Topo Santoso and Eva Hq, 2001:11) enters the process of making laws, violations of the laws and the reaction of the offences Act *(reacting toward the breaking of the law).*

II. Cybercrime

a. Understanding *Cybercrime*

Research Center of law and Justice of the Supreme Court of Indonesia (2004:4): Cybercrime defined as computer crime. Regarding the definition of computer crime himself, to now scholars have not agreed on the understanding or definition of computer crime. English computer still has not been uniform. However, more scholars generally accept the use of the term "computer crime" is therefore considered more extensive and regular to used in international relations.

The British Law Commission defines (Research Center of law and Justice of the Supreme Court of Indonesia, 2004:4) "computer fraud" as a manipulation of the computer in any way money is done in bad faith to obtain money, goods or other benefits or intended to cause harm to the other party. Madeel shared a "computer crime" top two activities, i.e.:

(a) The use of a computer to carry out the deed fraud, theft or concealment is meant for financial gain, profit, wealth or business services.
(b) That to the computer itself as hardware or software theft, sabotage, and blackmail.

Information technology system in the form of the internet has been able to shift the paradigm of the law against computer crime definitions as defined previously, that legal experts had initially focused on the tools/hardware IE computer. However, with the development of information technology in the form of a network the internet, then the focus of identification of cybercrime more expanded definition again, i.e. covering activities that can do in the world of internet through information systems used. So, it's not just the hardware components in the course of such crimes meant cybercrime, but it can expand within the framework of the world information technology systems by crawling is concerned, so it would be more appropriate if the definition of Cybercrime is crime information technology, as well as allegedly n. a. Barda (Yoshua Sitompul, 2012:15) as the evil crack.

Therefore, Budi Suharianto (2012:11), said that: basically, cybercrime includes all criminal acts relating to information systems, information system itself, as well as the communication system is a means for the delivery/ the exchange of information to the other party (transmitter/originator to reciptient).

According to Widodo (Nasrullah Rulli, 2014:128), the world's crime more sib or cybercrime is a form of new technology-based crime information by leveraging the hardware and software of a computer. According to Pardew Maskun (Nasrullah Rulli, 2014:128), cybercrime is a tort that done using the computer as a means/tools or computer as objects, whether for profit or not, with the detriment of the other party. But according to Chin (Nasrullah Rulli, 2014:128), the crime of criminal action or more sib is against the law to use computers and the internet.

b. Characteristics *Cybercrime*

Abdul Manan (2006:63-64), said that: globalization that hit the adult world is causing changes in all aspects of human life,

especially in developing countries, including Indonesia. Changes that occur to it by itself on legal changes occurred due to the needs of the community will change quantitatively and qualitatively. Problems that arise in a legal change that is the extent to which the law could achieve after the change and how the order of the law so as not to be left behind with the changing society. Also, the extent to which the public can bind themselves in the development of the law so that there is harmony between people and the law to give birth order and harmony expected.

The era of globalization has also led to the more sophisticated information technology so that it has brought an impact on the emergence of various forms of crime which affect modern nature greater than the conventional crime. In contrast to conventional crime, characterized by at least consists of several things, among them, outlaws bias anyone and the tools used are simple, and his crime did not need to use a skill.

Merry Magdalena and Maswigrantoro Rous Setyandu (2007:28), said that: crime in the field of information technology can be classified as a white colour crime because the perpetrators of cybercrime are the ones who master the use of the internet and its application or experts in their field. Also, the deed is often done in a transnational or cross the border so the two criteria of evil inherent in cybercrime at the same time, the white colour crime and transnational crime. Here interpreted as a modern sophistication of the crime so that any such disclosure through sophisticated advice anyway.

Budi Suharianto (2012:13), said that: the development of information technology including the internet in it also provides its challenges for the development of the law in Indonesia. Laws in Indonesia are required to be able to adjust to the social changes that occur. The change of social change and changes in the law or otherwise do not always take place together. That means that in certain circumstances the legal developments may be left behind by the development of other elements of society and its culture or maybe the opposite.

According to Abdul Wahid and m. Labib (2005:76) based on some of the literature and practice, cybercrime has some characteristics, i.e.:

a. The deed is done illegally, without rights or unethical occurs in space/territory more sib/cyber (cyberspace), so it is uncertain which country's jurisdiction applies to it.
b. Committed to the use of any equipment that connected to the internet.
c. The deed resulted in losses of material or immaterial (time, value, services, goods, money, self-respect, dignity, confidentiality of information) that are likely to be greater than the evil conventional.
d. The culprit was a man who mastered the use of the internet and its application.
e. Do is often done in a transnational/cross the border.

III. The Form of Cybercrime

According to Ari Juliono Echo (Maskun, 2013:51), crimes closely connected with the use of technology based computer and telecommunications networks in some literature and practice in a group in some form among others :

1. *Unauthorized access to computer systems and service, namely crimes committed into a system of computer network illegally, without permission, or without the knowledge of the owner of the computer network system which he enters. Usually, the perpetrator of a crime (hacker) does it with intent to sabotage or theft of important and confidential information. However, there are also doing just because it feels challenged to try his skill to penetrate a*

Indonesia Prime, p-ISSN: 2548-317X, e-ISSN: 2548-4664
Vol. 2, No 1, November 2017, pp. 56-67

system that has a high level of protection. This crime is getting popular recently with the development of internet technology.

2. *Illegal contents, namely the crime by entering data or information to the internet* about a thing that is not true, unethical, and considered breaking the law or disturb public order. As an example, is:
   a) Filling of hoax news or slander which will sproutswill the dignity or self-esteem of others.
   b) Filling things related to pornography.
   c) Loading information which is a State secret, agitation, and propaganda against the legitimate Government, and so on.
3. Forgery of data, namely crimes with falsified data on important documents stored as script less document via the internet. These crimes usually go on documents e-commerce by making as though it happened "typo" that ultimately will benefit the perpetrator.
4. *Cyber espionage, namely crime utilizing internet networks to do spy activities against the other party, by entering into a computer network system (computer network system) target party. These crimes usually directed against rival business documents, or the importance of the data stored in the computerized system was.*
5. *Cyber sabotage and extortion, that crimes committed by creating a disturbance, destruction or the destruction of a computer program, or data network system computer connected with the internet. Usually, these crimes are done with the intrusion of a logic bomb, a computer virus or a particular program, so data, computer programs or computer network system cannot use, does not run as desired by the perpetrator. In some cases, after it occurred, then crime such offender to the victim volunteered to repair the data, computer programs or computer network systems that have sabotage, of course with a certain fee. A logic bomb is a program that is created and used by the perpetrators to come by any time or depending on the wishes of the offender, from there to see that the information in the computer can be interrupted, damaged or even lost.*
6. *An offence against intellectual property, i.e., wealth directed against intellectual property rights belonging to a person on the internet. An example is a web page display the impersonation site belongs to others illegally, broadcasting information on the internet that is the trade secrets of others, and so on*
7. *Infringement of privacy, namely crimes directed against a person's information is private and confidential. These crimes usually directed against a person's personal information stored in the form of personal data stored in computerized, which if known by others, then it can harm people in immaterial, as well as anti-materiel such as credit card number, ATM PIN number, a description of the defect or disease is hidden, and so on.*

IV. The result of the research

A. The process of Law Handling Cybercrime in the town of Parepare

Before discussing the process of legal cybercrime in the town of Parepare then the writer needs to know that cybercrime is a crime that is computerized using the internet network. According to the big Dictionary Indonesian Language grammar (2008:721), Computerized is the "computer usage (count, process data, etc.) in a big way." Surely there must be a crime in the handling of evil. To know the course of the legal proceedings or the handling of cybercrime, the author must know in advance the type of cybercrime in the handle in the town of Parepare.

Based on the interview directly to the resource handle cybercrime in Polres Parepare

Town, in the Reskrim (Resort criminal) who handle all criminalization occurring in the town of Parepare, precisely in a handling cybercrime at the Kanit Tipikor (June 22, 2017). As cybercrime is a criminal offence in a particular criminal offence of corruption with equating regarding the process of investigation that the expert Tipkor Kanit that transcends the specific criminal acts.

According To aiptu. Hamka, se. Ps. Kanit Tipikor Polres Parepare Town, type of cybercrime in the handle which is "post through social media (facebook)", which is a crime in the field of computerized network internet, similar with it above, in the rule of law number 11 year 2008 of the information and electronic transactions in Chapter VII concerning the acts prohibited in article 27 paragraph (3) which reads:

"Any person intentionally and distribute and transmits the and make can be accessible electronic information and electronic document which has the charge of insult or defamation."

According to jemmy n. Tirayudi, sh. Mh. The public prosecutor (JPU) State Prosecutor Parepare gives the sense of cybercrime based on (interview, June 29, 2017) that:

Types of cybercrime are currently in by JPU on State Prosecutor Parepare is a kind of crime of insult or defamation against the person committed by perpetrators of cybercrime by way of post writing/make comments use personal facebook account, where perpetrators use social media facebook group the observer Government of Parepare Town containing writings/comments accusing/attacking the honour or dignity of the person.

Viewed from this type of cybercrime are handled in Parepare Town in enforcing the law is certainly no attempt to tackle cybercrime in the town of Parepare. According To aiptu. Hamka, SE. Dealing with cybercrime in the town of Parepare, the Kanit Tipikor (interview, June 22, 2017), in tackling cybercrime with the "efforts of the investigations." The investigation according to legislation as referred to in article 1 point 5 the book of the law of criminal procedure (Code Of Criminal Procedure) is as follows:

"The investigation is a series of actions are hardly being for investigators and find an event on the suspect as a criminal offence to determine which can do or whether the investigation according to the way that set in this Act."

Based on the sound Section 1 number 5 Code Of Criminal Procedure that became the "investigator" in determining events an alleged criminal offence which in the explain on article 1 point 4 Code Of Criminal Procedure is as follows:

"Investigators are police officials of the Republic of Indonesia which were authorized by this Act to conduct investigations."

As the sound of the Code of Criminal Procedure article 1 number 4 above that which became the Authority Police officials, namely investigations. Surely in the handling to tackle cybercrime in the town of Parepare, there is a barrier in handling to tackle cybercrime in the town of Parepare. According To aiptu. Hamka, se. (interview, June 22, 2017) That become obstacles to overcome in the handling of cybercrime in the town of Parepare, namely "lack of experts who deal with the cybercrime." Although cybercrime experts who have obstacles in tackling cybercrime, but investigators in the sphere of Parepare Town Polres still trying to handle and tackling the cybercrime that occurred in the town of Parepare just as other crimes.

In the investigation of the handling of cybercrime that occurred in the town of Parepare, surely takes the process stages in settlement of the matter. That through the stage of a report or complaint and complaint report explanations as found in article 1 paragraph 24 and paragraph 25 and the Code Of Criminal Procedure that became the authority investigators found in article 7 paragraph 1 letter a, namely: "receive reports or complaints from a about the existence of a criminal offence ".

According To aiptu. Hamka, se. (interview, June 22, 2017), that it phases in settlement: the process of cybercrime matters at the start of a report or complaint subsequently made SP. Lidik (Warrant Investigation) to the witness, the rapporteur, and reported. After the investigation has completed, then the investigator does the title matters to determine sufficient evidence or whether a criminal offence. After determining proved to be a criminal offence in the

Indonesia Prime, p-ISSN: 2548-317X, e-ISSN: 2548-4664
Vol. 2, No 1, November 2017, pp. 56-67

title of the case, investigators make SP. Yout (warrant of Investigation) and SP2A (letter Notification the development of investigation) dedicated to the rapporteur. In SP. Prints where witnesses, reporters, reported, and expert witnesses asked for a description of a criminal act which had befallen him, and he felt. Next set the searches and seizures with evidence of the alleged criminal act in conjunction with the arrest and detention of as set forth by law number 11 the year 2008 of the information and electronic transactions in Article 43 paragraph (3) and article 43 paragraph (6) as follows:

Article 43 paragraph (3)

"the search and/or seizure against electronic systems that are related to the alleged criminal act must be done on the permission of the Chairman of the Court of the country."

Article 43 paragraph (6)

"regarding making arrests and detention, the investigator through the public prosecutor is obligated to ask the determination of the Chairman of the local district court within one twenty-four hour time."

In the completion stages things satisfy cybercrime that became a News Event things (BAP), the investigator is obligated to submit dossiers to the State Prosecutor for in researched, and that will be later on in the proceedings in the courts promote the land after a complete file, as described in section 14 letters a to j of the book law of criminal procedure (Code of Criminal Procedure) that:

a. Receiving and checking the docket investigation of the investigator or investigators maid;
b. Hold the prosecution when there is a deficiency in the investigation having regard to the provisions of article 10 paragraph 3 and paragraph 4, by giving instructions in order completion of the investigation of the investigator;
c. Provide the extension of detention; detention conduct advanced and or change the status of prisoners after the subjects assigned by the investigators;
d. Make the indictment;
e. Assign the matter to a court;
f. Convey notification to the defendant about the conditions of the day and time the matter trial which accompanied the summons; either the defendant or witness to, to come at the hearing have determined;
g. Did the prosecution;
h. Close the matter for the sake of the interests of the law;
i. Other actions held in respect of the scope of the duties and responsibilities as a public prosecutor according to the provisions of this Act. '
j. Carry out the determination of the judge.

On the description sounds Article 14 subparagraph (a) up to the letter (j) the State party's Criminal Procedure Code in order to examine the dossiers of the investigators, as a barrier to determine an indictment and prosecution, as in article 13 of the book of law Criminal procedure (Code Of Criminal Procedure) that:

"The public prosecutor was Attorney who was authorized by this Act to do prosecution and carry out the determination of the judge."

According to jemmy n. Tirayudi, sh. Mh. The public prosecutor (JPU) that deal with cybercrime in the town of Parepare (interview, June 29, 2017) that: The Prosecutor poses in researching docket cybercrime in determining the claim is about the means used by the perpetrators of cybercrime itself, as well as he did, given that cybercrime closely connection with the technology where the perpetrators of cybercrime is sometimes difficult to track his existence if he is using a fake account, so that means factors It is one of the elements

that are very determined in the breakdown of the public prosecutor's claim and the description of criminal charges against the defendant.

View of the process the handling of cybercrime in the town of Parepare, the author can take the conclusion that in the process the handling of cybercrime in the town of Parepare already effective although the Polres Parepare have obstructions in the experts tackling cybercrime, but the State Attorney's and Parepare Polres perform duties and functions as law enforcement to tackle cybercrime and crimes that occurred in the town of Parepare.

B. Snares Legal Basis regarding Cybercrime in The Town of Parepare

The legislation of the Republic of Indonesia number 11 the Year 2008 Of the information and Electronic Transaction is one of the basic laws that govern cybercrime, which is the special legislation governing information and electronic transactions. According To aiptu. Hamka, SE. Dealing with cybercrime in the town of Parepare, the Kanit Tipikor (interview, June 22, 2017), which became the legal basis for the cybercrime snares in Parepare Town Polres tackle IE: "law of the Republic of Indonesia number 11 the Year 2008 About information and Electronic Transaction is the Special Act or also called in Dutch leg specialist ". But according to Jemmy n. Tirayudi, SH. MH. The public prosecutor (JPU) that deal with cybercrime in the town of Parepare (interview, June 29, 2017) that: That is the basis of the law the perpetrators of cybercrime snares by the public prosecutor (JPU) in determine the claim i.e. Article directly related to the Act the perpetrators of cybercrime itself, such as the perpetrators of cybercrime who had done the deed post a writing in the form of comments contains writings attacking the honour of a person/accuse someone of doing an act by way of order spread an information via his facebook account a medium social, so by basing on his deeds, then JPU will apply article in the indictment that directly relates to the Act were as follows: article 27 paragraph (3) jo Article 45 paragraph (1) of the Act of the Republic of Indonesia number 11 Year 2008 about information and electronic transactions (ITE) with the reason: "intentionally and without right, distribute and/or transmit and or make can be accessible electronic information and Electronic Documents, or have the charge of insult and or defamation ".Next article claims it will prove in the trial and the facts of the trial relating to the deeds of the perpetrators of cybercrime itself will be in use as the legal basis in JPU criminal charges against perpetrators of cybercrime. Surely that became the legal basis for analysis of Parepare Town in Polres snares cybercrime. According To aiptu. Hamka, SE. Dealing with cybercrime in the town of Parepare, the Kanit Tipikor (interview, June 22, 2017) that: it does matter to determine title enough evidence or whether a criminal act to post through social media (facebook) as in article 27 paragraph (3) of the Act of the Republic of Indonesia number 11 the Year 2008 Of the information and electronic transactions. But according to Jemmy n. Tirayudi, SH. MH. The public prosecutor (JPU) that deal with cybercrime in the town of Parepare (interview, June 29, 2017) that: Analysis legal basis snares cybercrime is based on the existence of tools valid evidence, i.e. where JPU always use analysis in snares perpetrators of cybercrime refers to the existence of evidence of tools as terms in the book Statute of the law of criminal procedure (Code of Criminal Procedure) so that when there have been tools the existence of evidence in the file of things at least 2 valid instruments of evidence in connection with cybercrime, then that would proclaim that JPU docket cybercrime committed investigation by the investigating parties have full or qualified formyl or criminal offence materially to do the prosecution process. Viewed from above snares legal basis in terms of cybercrime in the town of Parepare, the author can take the conclusion that State and Parepare Polres perform duties and functions as the law enforcement agencies to tackle crime occurrence Cybercrime in the town of Parepare, and became the basis of the law of snares i.e. the laws of the Republic of Indonesia number 11 Year 2008 Of

Indonesia Prime, p-ISSN: 2548-317X, e-ISSN: 2548-4664
Vol. 2, No 1, November 2017, pp. 56-67

the information and electronic transactions (ITE), in Chapter VII the Act prohibited in article 27 paragraph (3) the types of cybercrime occurred in the town of Parepare and remain based on the book of the law of criminal law (Penal Code) and the book of the law of criminal procedure (Code of Criminal Procedure) as the legal basis for the citizens of Republic of Indonesia. Viewed from this type of cybercrime according to respondents above, authors can analyze type of cybercrime that occurred in the town of Parepare is a crime in which someone who had personal accounts in social media (facebook) and using that account to begin the crime is one that included in the form of cybercrime, namely illegal contents which according to William Wiebe (Maskun, 2013:50) that the scope of coverage of cybercrime that is:

(a) Piracy;
(b) Fraud;
(c) Theft;
(d) Pornography;
(e) Harassment;
(f) slander; and
(g) Counterfeiting.

As one of the scope of coverage of cybercrime mentioned that occurred in the town of Parepare, namely slander which is included in the illegal contents which according to Ari Juliono Echo (Maskun, 2013:51): that crime by entering data or information to the internet about a thing that is not true, unethical, and considered breaking the law or disturb public order as one example: the loading of a hoax news or slander which will sproutswill the dignity or self-esteem of others.

As an example of one form of illegal contents of the new first-time cybercrime occurred in the town of Parepare.

This author needs to know which becomes snares against cybercrime, of course, the rule of law that govern cybercrime, the legislation of the Republic of Indonesia number 11 Year 2008 Of the information and electronic transactions, which, according to the author analyses the legal snares against cybercrime that occurred in the town of Parepare in elements of article 27 paragraph (3) of the Act of the Republic of Indonesia number 11 Year 2008 Of the information and electronic transactions (UU ITE) namely:

(3) any person intentionally and without the rights to distribute and/or transmit and/or can be accessible electronic information and/or electronic document which has the charge of insult or defamation.

the element of "people" "intentionally and without right", "distribute", "transmits the", "can make it", "electronic information" and "electronic document".

The definition of "person" according to UU ITE article 1 21 grains are those individuals, both citizens of Indonesia, foreign citizens and legal entities. As the author's analysis of the intended person is the perpetrator of the cybercrime which proved to be the culprit. UU ITE confirms the that applies to every person who commits the Act of law outlined in the legislation are both legal relic in Indonesia and outside Indonesia that jurisdictions have legal consequences in the region of Indonesia and/or outside the area of the law of Indonesia and harm the interests of Indonesia.

Intentionally and without right, which according to the author's analysis of these elements is the subjective element of the crime. The words fields ACT ITE to conceive the meaning of that purposely is: knowing (knowingly), and Wills (intentionally) do an act prohibited by the ACT ITE or knowing and willed the occurrence of the prohibited ACT, in consequence, an ITE. Related to article 27 paragraph (3) of the ACT ITE, intentionally is directed against the Act distributes, transmits, or can be accessible information or electronic document which has the charge of insult or defamation. In the sense of deliberately also contained meaning "should know"; the implementation of this understanding will be judged from a case by case. Understanding expressly in the ACT ITE refer to theories expressly applicable in Indonesia, according to e. Utrecht (Yoshua Sitompul, 2012:152):

a. As a deliberate intent (opzet als oogmerk);
b. Deliberate action with conscience assurance

(noodzakelijkheds bij opzet or zekerheidsbewustzjin);

c. Deliberate action with the conscience possibilities (opzet mogelijheids bij-bewustzijin).

Without the right meaning has no right either given by legislation, treaty or another valid legal base (without authorization). Included in this sense is beyond the rights or authority given to the person concerned by the legal base (more than authorization). Therefore, the Treaty and regulations, or another legal base the legal base or benchmark are to assess and determine whether there is a right of a person, or whether the rights granted surpassed him. The pedestal of the law in question must grant it to someone to distribute, transmit, or can charge it insults and/or defamation.

Distribute, transmit, or can be accessible. The definition of "distributing" is the sending of information or electronic documents to multiple parties or through or by electronic systems. This action can do by posting a Word and/or sentence containing the charge of insult or defamation in social media. Such deeds make the information viewable by anyone, such as one of these types of cybercrime that occurred in the town of Parepare, one of the people publishing the on the wall facebook group page of the observer Government of Parepare Town, which contains the charge of insult or defamation of an official in Parepare Town.

While the definition of "transmit" is sending or forwarding of information or electronic documents of a party or one person or place to another place. In distributing meaning transmits, but the difference is the essence of distributing is disseminating information or electronic documents, whereas only limited transmitting from one sender to one recipient. This action can be done by sending short messages via mobile (HP) or electronic mail (Email) to a recipient, or forward (forward) the message to other recipients.

"It can Make" means making information or electronic documents can be accessible by others, either directly or indirectly. That can do by providing links/hyperlinks, i.e. link or reference that can be used by internet users to access the site or document. Letting it can also be done by giving the access code (password) as in according to article 1 grain Act ITE that: "the access codes are numbers, letters, symbols, characters, other or a combination of them, that he is the key to be able to access the computer and/or another electronic system ".

Information or electronic documents as described in the ACT ITE article 1 1 and 4 grains of grains that:

Article 1 electronic information is a one or a set of electronic data, including fixed unlimited on writing, sound, pictures, maps, designs, photos, electronic data interchange (EDI), electronic (email) letter, telegram, telex or telecopy, like, letters, marks, numbers, access codes, symbols, or perforation that has been processed or meaning can understood by people who can understand it.

Definition of the information by the electronic group is time because many electronic data forms include the start of the text, sounds, images, and even perforation. All the electronic data that has processed or the meaning can understand by people who can understand it; the data is electronic information. Whereas electronic documents as that:

Article 1

An electronic document is any electronic information made, forwarded, transmitted, received, or stored in the form of analog, digital, optical, electromagnetic, or similar ones, which can be seen, displayed, and/or heard through computer or electronic systems, including but not limited to text, sound, pictures, maps, designs, photographs, or the like, letters, marks, numbers, access codes, symbols or perforation that have meaning or meaning or can be understood by people who are able to understand it.

According to Yoshua Sitompul (2012:155) gives the essence of the difference between electronic information and electronic documents is that:

Electronic information is essentially content, whereas electronic documents is a media from the content itself that can shape as analog, digital, optical, or electromagnetic. As the image is simple, data file ".doc", ".xls", ".",

Indonesia Prime, p-ISSN: 2548-317X, e-ISSN: 2548-4664
Vol. 2, No 1, November 2017, pp. 56-67

Ods are the electronic information is the words, sentences, pragraf, figures, data, or fonts contained in those files, while the electronic document is the ".doc," ".xls," "ods." Images in .jpg format file are electronic information, whereas the format .jpg is an electronic document. In addition to these differences, it seems there is no difference between the essence of electronic information and electronic documents.

As an element of "the charge of insult or defamation" especially in Chapter VII, article 27 prohibited deeds article (3) and also refers to the book of the law of criminal law (Criminal Code), in particular in chapter XVI of the insult Article 310 and 311 Article a basic understanding of essence or give regarding defamation or insult, i.e. the Act of attacking the honour or good name of another person with the intent to be known by the public. Therefore, the Act of distributing, transmitting it can create in this article must be meant fortunately attacked the honour or good name of another person with the intent to be known by the public. Therefore, distribute, transmit, can be accessible in this article must be intended to attack the honour or good name of another person with the intent to be known by the public.

The essence of humiliation that is attacking the honor or name good others to the public in the know or so in the know by the public. Therefore, the element of "distribute," "transmit," and "make it can" in article 27 paragraph (3) of the ACT ITE is the actions in the virtual world that can achieve the fulfillment of "publicly known" or "General." The action distributes, transmit and make accessible can be done in order or order for information or electronic documents can be known by the public. Thus, the element of "publicly known" or "General" that became the essence of Article 310 of the Criminal Code becomes one spirit in article 27 paragraph (3) of the ACT ITE so must still be proven correct fulfillment of the item.

Then the authors can conclude that satisfy the elements of article 27 paragraph (3) of the ACT ITE then proved as a criminal offence and can are convicted with the provision of article, which is in the elements of the article, that the person is the perpetrator of a crime that strikes the honor of an officials Government through social media in an account facebook group Parepare town Government Observers, one of the new types of cybercrime the first time occurred in the town of Parepare

V. Conclusions and suggestions

1. Conclusion

Based on the explanation above, the authors draw conclusions based on the formulation of the problem of research results and discussion, i.e. as follows:

A. In the process the handling of cybercrime in the town of Parepare already effective although the Polres Parepare have obstacles in experts who deal with cybercrime, and the Prosecution has its own the barriers in determining the elements of article snares and proof of the crime. But the State apparatus of Parepare Polres and perform duties and functions as law enforcement to tackle cybercrime and other crimes that occurred in the town of Parepare.
B. Prosecutor remain a law enforcement to cope with the onset of cybercrime in the town of Parepare, and became the basis of the law of snares i.e. the laws of the Republic of Indonesia number 11 Year 2008 about information and transactions Electronic (ITE), in Chapter VII the Act prohibited in article 27 paragraph (3) types of cybercrime that occurred in the town of Parepare and remain based on the book of the law of criminal law (Penal Code) and the book of the law of criminal procedure (Code Of Criminal Procedure) as the legal basis Citizens Of The Republic Of Indonesia.

2. Suggestions

As for the suggestion that the author may have given in respect of the writing of this study, as follows

A. Polres and Parepare Town State Prosecutor must hold experts in addressing cybercrime and make the security on the internet, not only prevent but tackle cybercrime that occurred in the town of parepare.
B. The relevant parties should provide

socialization about UU ITE so that citizens know regarding the use of the means of information and communication technologies as the development of technology in the country of Indonesia in the field of information and communication technology such. For citizens to know the legal consequences when information and communication technology are abusing.

References

[1] Departemen Pendidikan Nasional. 2008. *Kamus Besar Bahasa Indonesia; Pusat Bahasa; edisi keempat*. Jakarta: Gramedia.
[2] Magdalena Merry dan R . S . Maswigrantoro. 2007. *cyber law tidak perlu takut,* Yogyakarta: Andi.
[3] Marzuki, Peter Mahmud. 2005. *Penelitian Hukum. Edisi revisi*. Jakarta: prenada media group.
[4] Manan, Abdul. 2006. *Apek-aspek Pengubah Hukum.* Jakarta: Kencana.
[5] Maskun. 2013. *Kejahatan Siber. Cybercrime: Suatu pengantar*. Jakarta: Prenada media group
[6] Nasrullah, Rulli, 2014. Teori Dan Riset Media Siber: Cyber Media. Jakarta. Kencana.
[7] Putlitbang Hukum dan Peradilan Mahkamah Agung RI. 2004. *Naskah Akademis Kejahatan Internet* (*cybercrime*).
[8] Sitompul, josua. 2012. *Cyberspace, Cybercrime, Cyberlaw*; *Tinjauan Aspek Hukum Pidana*. Jakarta: Tatanusa.
[9] Santoso, Topo, dan Achjani Zulfa, Eva. 2001. *Kriminologi.* Jakarta : Raja Grafindo Persada.
[10] Suparni Niniek, 2009, *Cybersapce, Problematika & Antisipasi Pengaturannnya*, Jakarta: Sinar Grafika.
[11] Suharianto, Budi. 2012. *Tindak Pidana Teknologi Informasi (Cybercrime),* Jakarta: PT. Raja Grafindo Persada.
[12] Wahid, Abdul dan M. Labib. 2005. *Kejahatan Mayantara* (*cybercrime*), Bandung: Refika Aditama.