THE INTERNATIONAL JOURNAL OF
HUMANITIES & SOCIAL STUDIES

Effectiveness of Criminal Application or Fine for Applicants of Violation Information and Electronic Transaction

Dr. Gomgom TP Siregar
Lecturer, Darma Agung University, Indonesia

Abstract:
Efforts to prevent information technology crimes in the future will be carried out by law enforcement officials, such as the following: First, educating law enforcement officials, because dealing with crimes through social media requires specialization of investigators and public prosecutors can be considered as one way to enforce law against cybercrime. Currently Indonesia is in dire need of "Cyber Law Enforcement", such as: Cyber Police, Cyber Prosecutors, Cyber Judges and Cyber Advocates, in the context of cybercrime law enforcement in Indonesia. Without the presence of law enforcers who are in the field of information technology, it will be difficult to enforce "Cyber Law" in an equitable Indonesia. Second, Building forensic computing facilities to be established by the National Police. The improvement of facilities or facilities in dealing with information technology crimes is not only limited by trying as much as possible to up-date and up-grade the facilities and infrastructure that are already owned by law enforcement officials but also by completing these facilities or facilities in accordance with today's technological developments. Third, increasing investigative efforts, because criminal acts regulated by the ITE Law are special crimes, so special investigators are needed. Article 43 of the ITE Law states, in addition to the police, the authority of investigation is on the shoulders of Civil Servants (PPNS). Cyber task force involves not only the National Police but also PPNS, Prosecutors and judges whose scope ranges from the central level to the provinces and also the regencies. The collaboration effort is not only done with fellow cyber law enforcement officers, but also asks for help from experts who required in the investigation. The "expert" referred to here is of course someone who has special expertise in the field of IT and must be accountable academically and practically.

Keywords: *Prison criminal, fines, actors, information and electronic transactions*

1. Introduction

The development of technology makes it easy for humans to carry out their daily activities. Technology in addition to bringing benefits such as making it easy for people to carry out their activities, also causes losses such as the rise of crimes committed through information technology. Technology not only gives a positive value to improving human well-being, but also can be used as a means to do various acts that violate the law (onrechtmatig) or even through law (wenderechttelijk). The advancement of science and technology has had a very positive impact on the civilization of the ummah human. One of the phenomena of the modern age which until now is still growing rapidly is the internet. At first the internet network can only be used by the educational environment (universities) and research institutions. Then in 1995, the internet could only be used for the public a few years later Berners-Lee's team developed a Word Wide Web application (WWW) that made it easy for people to access information on the internet. After the opening of the internet for public purposes more and more business applications appeared on the internet. The development of the internet network has a negative impact, as stated by Roy Suryo, an information technology expert, in his research quoted by the Kompas daily as saying:

- "Cyber-crime is now rampant in five major cities in Indonesia and is at a level that is sufficiently concerned with and carried out by hackers who on average are young people who seem creative, but actually they steal credit card numbers through the internet"

`The crime of cybercrime is divided into 2 categories, namely cyber-crime in a narrow sense and in broad terms. Cybercrime in a narrow sense is a crime against computer systems, while cybercrime in the broad sense includes crimes against computer systems or networks and crimes using computer equipment. The terms that are still used are still directed at the notion of crimes against computers (Crimes utilizing computers), or computer-related crimes (Crimes related to computers), even though these terms have not provided the right images. Nevertheless, any term used, various parties have tried to make definitions individually based on their understanding.

In this case there are three approaches to maintaining security in cyberspace, first is the technology approach, the second is the socio-cultural approach to ethics, and the third is the legal approach. To overcome the security of technological approach disruption is absolutely necessary, because without a network security it will be easily infiltrated, or accessed illegally and without rights. Seeing the legal facts as at present, the impact of the development of science and technology that has been misused as a suggestion of crime is very important to anticipate how the legal policy can be, so that cyber-crime can be carried out efforts to deal with criminal law, including in this case regarding the proof system. It is very important because in the enforcement of criminal law the basis of justification can be said to be guilty or not committing a crime, besides its actions can be blamed for the power of the existing law (legality principle), also actions supported by the validity of evidence and can be accounted for (element of error). Such thinking is in accordance with the application of the principle of legality in our criminal law (KUHP), namely as explicitly formulated in Article 1a (1) of the Criminal Code "Nullum delictum nulla poenasine praevia lege poenali" or in other terms can be known, "no crime, no there is a crime, without the prior regulation of criminal law ".

2. Arrangements in Indonesia

The rapid development of technology requires legal arrangements relating to the utilization of the technology. Unfortunately, until now many countries do not have specific legislation in the field of information technology, both in criminal and civil aspects. If seen from the criminal, Soedjono Dirdjosisworo stated that:

"Changes and social adjustments as well as technological developments for half a century since 1985 (Law No. 73/58) are so rapid, and the agility of social and technological developments and the increasingly influential globalization that continues to be driven by information and communication technology is strongly felt that the Penal Code for a long time it has not been able to perfectly accommodate and anticipate crimes that have increased, increased qualitatively, or quantitatively with the types, patterns and modus operandi that are not contained in the Criminal Code (a prominent example is the Crime Crime) ".

Many cases prove that legal instruments in the IT sector are still weak, this can be seen from juridical constraints and non-juridical constraints. The juridical constraint is that the electronic documents are still not explicitly recognized as evidence by the Criminal Procedure Code. This can be seen in Law No. 8/1981 Article 184 paragraph (1) that this law definitively limits evidence only as witness statements, expert statements, letters, instructions, and statements of defendants only, and there is no authority for investigators to search computer systems that are suspected of being tools or targets of crime. Meanwhile, non-juridical constraints, namely the limited ability and number of members of the national police who control the field of computer technology, evidence of cybercrime is easily eliminated or removed, the difficulty of detecting banking crimes using computer means. The difficulty of detecting crime is caused by lack of adequate equipment, reluctance of some victims to report to the police, a relatively weak security system of asset / system owners, difficulty tracking the whereabouts / domicile of the perpetrators of crime.

Until now, there is no article in our country that can be used to ensnare cyber-crime criminals. For carding cases, for example, the new police can ensnare the perpetrators of computer crimes with Article 363 of the Criminal Code concerning theft because what the suspect did steal other people's credit card data. Since its introduction in 1988, the development and growth of the internet has become very fast. With a population of more than 250 million and with the use of an active number of internets as much as 88.1 million, Indonesia has grown to become the largest internet user in ASEAN. Although in terms of percentage distribution and internet penetration, Indonesia is actually still very low.

This great growth turned out to also make policy makers in Indonesia begin to look at ways to regulate the internet, especially by conducting recriminalization of actions that have been regulated in the Criminal Code. This regulation and recriminalization was realized in Law No. 11 of 2008 concerning Information and Electronic Transactions (UU ITE). Utilization of Information Technology, media and communication has changed both people's behavior and human civilization globally. The development of information and communication technology has also caused borderless relations and caused significant social, economic, and cultural changes to take place so quickly. Information technology is now a double-edged sword because in addition to contributing to improving welfare, progress, and human civilization, as well as being an effective means of lawlessness.

Now a new legal regime has been born known as cyber law or telematics law. Cyber law or cyber law, internationally used for legal terms related to the use of information and communication technology. Likewise, telematics law is a solution of the convergence of telecommunications law, media law, and informatics law. Other terms that are also used are information technology law (law of information technology), virtual world law, and mayantara law. These terms are born considering the activities carried out through a network of computer systems and communication systems both locally and globally (the internet) by utilizing computer-based information technology which is an electronic system that can be seen virtually. Legal problems that are often faced are when related to the delivery of information, communication, and / or transactions electronically, especially in terms of evidence and matters relating to actions / laws carried out through an electronic system. Electronic systems are also used to explain the existence of information systems which are the application of information technology based on telecommunications networks and electronic media, which functions to design, process, analyze, display, and transmit or disseminate electronic information. Information and technical systems are actually embodiments of product implementation. information technology into a form of organization and management in accordance with the characteristics of the needs of the organization and in accordance with the intended purpose. On the other hand, information systems are technically and functionally integrated systems between humans and machines that include hardware components, software, procedures, human resources, and the substance of information that includes input functions, output processes, storage, and communication.

In connection with that, the world of law has in fact been extending the principle interpretation and norms for a long time when facing material problems that did not materialize, for example in the case of theft of electricity as a criminal act. In reality cyber activities are no longer simple because their activities are no longer limited by the territory of a country, which is easily accessible anytime and from anywhere. Losses can occur either on the transaction agent or on other people who have never made a transaction, for example, theft of credit card funds through spending on the internet. In addition, proof is a very important factor, considering that electronic information has not only been comprehensively accommodated in the Indonesian procedural law system, but also turned out to be very vulnerable to be changed, tapped, falsified, and sent to various parts of the world in a matter of seconds. Thus, the impact it causes can be complex and complicated.

Broader problems occur in the field of civilization because electronic transactions for trading activities through electronic systems (electronic commerce) have become part of national and international trade. This fact shows that the relevance in the field of information technology, media, and informatics (telematics) is developing steadily unstoppable, along with the discovery of new developments in the fields of information technology, media and communication. Activities through electronic systems, also called cyber space, although virtual in nature can be categorized as real legal actions or actions. Juridically, activities in cyberspace cannot be approached with conventional legal measures and qualifications because if this method is pursued there will be too many difficulties and things that escape legal enforcement. Activities in cyber space are virtual activities that have a very real impact even though the evidence tools are electronic. Thus, the subject of the perpetrators must also qualify as people who have taken legal actions in real terms. In e-commerce activities, among others, it is known that there are electronic documents whose position is synchronized with documents made on paper. In this regard, it is necessary to pay attention to the security and legal aspects of the use of information technology, media and communication in order to develop optimally. Therefore, there are three approaches to safeguarding security in cyber space, namely the approach of legal aspects, technological aspects, social, cultural and ethical aspects. To overcome security disturbances in the implementation of electronic systems, the legal approach is absolute because it appears legal certainty, problem the use of information technology is not optimal. Cybercrime or often called cyber-crime, according to crimes and criminal acts Cyber Crime is focused on the use of computer technology in committing crimes both new crimes and traditional crimes. According to Barda Nawawi, Cyber Crime crime is divided into two categories, namely Cyber Crime in a narrow sense and in a broad sense. Cyber-crime in a narrow sense is a crime against a computer system, while cyber-crime in a broad sense includes those covering systems or computer networks and crime using computer facilities.

The terms that are still used are still directed at the understanding of computer crime (crimes utilizing computers), or computer-related crimes (crimes related to computers) even though these terms have not yet provided the right images, however, whatever terms are used, various parties have tried to make their own definitions based on their understanding.

Since the ITE Law was passed, criminal cases involving internet use in Indonesia began to rise significantly. For example, in the provisions of Article 27 paragraph (3) of the ITE Law which is considered to be a provision of duplication with its rubber formulation. Not only that, a very high criminal threat, the conditions of lawyers and courts are exacerbated which do not have sufficient experience in the basic cases of internet freedom, as well as specifically the basic cases of internet freedom, specifically the cases related to ITE. The act of violating the provisions violates the law in Law number 11 of 2008 concerning Information and Electronic Transactions, crime in information technology is called cyber-crime. Cyber-crime is a type of crime that is related to the utilization of an information and communication technology without limits, and has strong characteristics with an engineering technology that relies on a high level of security, from an information delivered and accessed by internet users. Based on the provisions of the ITE Law, the determination of the criminal for the perpetrators of crimes subject to the ITE Law is regulated in Article 45 to Article 50. In those articles the criminal provisions applied are still in the granting of basic crimes and additions in the form of imprisonment and criminal penalties. Being a problem is that the application of criminal law stipulated in the law is in fact not appropriate. This can be seen from the many demands of the public prosecutor who is still not maximal in prosecuting the perpetrators of criminal acts of the ITE Law, and many judges who decide on imprisonment that is light and without giving criminal penalties for crimes committed by the perpetrators.

In 2017 the Aceh Regional Police handled three cyber-crime cases, one case with pornographic content and two cases of humiliation and defamation. North Sumatra Regional Police (North Sumatra) handles 95 cyber-crime crimes with details of one pornographic content, one online gambling, 53 cases of insult and defamation, as many as 30 cases of fraud, two spreads of hostility, six cases of threatening three cases of illegal access. Of the total, 45 cases have been resolved. West Sumatra Regional Police (Sumbar) handles six pornographic content, one online gambling, 30 cases of humiliation and defamation, 65 fraud cases, two cases of hostility dissemination, three cases of threats, illegal access to four cases, so in 2017 the total cases handled 125 with the completion of 15 cases. South Sumatra Police (Sumsel) handles two pornographic case content, seven cases of defamation and defamation, 11 cases of fraud, one case of Defacing or Hacking the website of an agency or individual. In total, the South Sumatra Regional Police handles 21 cyber-crime cases and has completed 2 cases. Riau Islands Regional Police (Kepri) in 2017 handled 40 cases, details of four pornographic content, 16 cases of insult and defamation, 17 cases of fraud, and three cases of identity theft.

3. Cyber Crime

The Prevention of Crime and Treatment of Offenders in Havana, Cuba in 1999 and in Vienna, Austria in 2000, mentions two known terms:

- Cybercrime in the narrow sense is called computer crime, which is illegal or violating behavior that directly attacks the security system of a computer or data processed by a computer.
- Cybercrime in the broad sense is called computer related crime, which is illegal or violating behavior related to a computer or network system.

Various definitions of cyber-crime according to experts, the conclusion of the definition of cyber-crime is a crime that can violate the law by using computer technology as a means of crime. In its development, the conventional crime of cyber-crime is known as:

3.1. Blue Collar Crime

This crime is a type of crime or criminal act carried out in a conventional manner such as robbery, theft, murder and others.

3.2. White Collar Crime

This type of crime is divided into four crime groups, namely corporate crime, bureaucrat crime, malpractice, and individual crime.

Cyber-crime itself as a crime that arises as a result of the existence of cyberspace communities on the internet, has its own characteristics that are different from the two models above. The unique characteristics of crime in cyberspace include the following five things:

- The scope of crime
- The nature of crime
- Crime perpetrators
- Crime mode
- Types of losses incurred

From some of the characteristics above, to facilitate the handling of cyber-crime classified:

- Cyber piracy: Use of computer technology to reprint software or information, then distribute information or software through computer technology.
- Cyber trespass: Use of computer technology to increase access to a computer system of an organization or individual.
- Cyber vandalism: The use of computer technology to create programs that disrupt the electronic transmission process, and destroy data on a computer.

Cyber-crime crime is increasing along with the development of information and communication technology. Some of which are included in cyber-crime, as follows:

- Denial of Service Attack: this purpose attack is to jam the system by interfering with access from legitimate internet service users by sending or flooding websites with unnecessary junk data for the intended person so that the website owner suffers a loss, because of controlling or re-controlling the website can take a little time to drain energy and energy.
- Hate sites: This site is often used by hackers to attack each other and make rude and vulgar comments that are managed by "extremists" to attack parties they don't like. This attack on opponents or opponents often raises racial issues, program wars and promotion of policies or a view (ism) adopted by a person / group, nation and state to be read and understood by another person or party as a "message" conveyed.
- Cyber Stalking: all forms of e-mails that are not desired by the user or junk e-mail that often uses folders and are not often forced. Although this "junk" e-mail is not desired by the users.

In various forms of actions that are carried out, we divide cyber-crime into 2 (two), namely:

a) Types of cyber-crime based on the type of activity, as follows:

- Unauthorized Access to Computer System and Service
- Illegal Contents
- Forgery data
- Cyber Espionage
- Cyber Sabotage and Extortion
- Offense against Intellectual Property
- Infringements of Privacy
- Cracking
- Carding

Types of cyber-crime based on motives, as follows:

- Cyber-crime as an act of pure crime.
- Cyber-crime as a gray crime.

In addition to the two types of cyber-crime based on motives it is divided into:

- Cyber-crime that attacks individuals.
- Cyber-crime that attacks copyright (property rights).
- Cyber-crime that attacks the government.

In the ITE Law regarding the provisions of article 45 paragraph 2, each person fulfills the elements as intended in Article 28 paragraph 1 2 and is punished with a maximum imprisonment of 6 (six years) and a maximum fine of Rp. 1,000,000,000.00 (one billion rupiah). Actually, in the issue of cyber-crime there is no legal vacuum, this occurs if an interpretation method is known in law and this should be held by law enforcement officials in the face of new dimensioned actions that have not been specifically regulated in law.

In general, there are two opinions regarding the need for laws governing cyber-crime among them

The group said that until today there are no legislation that regulates the problem of cybercrime, because if criminal acts occur in the cyber world, it is very difficult for law enforcement officials to ensnare the perpetrators. This opinion is reinforced by the case of Cybercrime which cannot be resolved by our justice system. The problem is based on the difficulty of finding articles that can be used as a basis for prosecution in court.

Those who think that there is no legal vacuum. They believe, even though there are no laws specifically regulating cybercrime, law enforcers can use existing legal provisions. To implement it, it takes courage for judges to explore existing laws by stealing legal provisions (jurisprudence) as a basis for court decisions.

Law No. 11 of 2008 concerning Information and Electronic Transactions is reviewed in the perspective of criminal policy, in general in terms of formulation of criminal acts, formulation of criminal witnesses in procedures or mechanisms of the criminal justice system. There are several problems provisions in deserving attention, including the following.

In the case of the formulation of a criminal act. In general, this law is in the formulation of criminal acts from the Criminal Code which are extended to cyberspace, besides that there is also a new criminal act, namely interception or tapping. In addition to dealing with various types of criminal acts in this law also regulates jurisdiction different from conventional criminal law (KUHP)

In terms of formulating criminal sanctions. In general, this law uses criminal sanctions in the form of imprisonment and heavier penalties combined with the Criminal Code. Criminal sanctions are of a special nature. Criminal charges are imposed on corporations who are perpetrators, if also the target of the crime is a government institution / institution, as well as if it is carried out in relation to the weighting of criminal sanctions.

In terms of criminal justice system procedures. This law regulates the problem of investigation procedures only. In this case there are several differences with conventional procedural law (KUHAP). Among them, he admitted that electronic evidence as a legitimate evidence was presented and regulated also concerning investigators of civil servants who could carry out investigations into cybercrime.

The review of the policy problem definition in law number 11 of 2008 concerning Information and Electronic Transactions is the most strategic stage of the whole which functions as a criminal law or criminal law enforcement process in the context of combating cybercrime crime. Crime prevention policies or plans as outlined in the laws and regulations, generally include:

- Planning or policy regarding prohibited acts which will be overcome because they will be considered dangerous or harmful;
- Planning or policy about what sanctions can be imposed on the perpetrators of prohibited acts (either in the form of criminal acts or actions) and the implementation system.
- Planning or policy regarding procedures or mechanisms of the criminal justice system in the context of criminal law enforcement processes.

A review of the criminalization of information technology (cybercrime) criminalization of information technology (cybercrime) crimes in the ITE law must also be focused on the three policy areas above. By reviewing these three things in this law, it is expected to be able to analyze the functionalization of criminal law in the formulation stage so that it can find out the basis for considering legislation in drafting a criminalization policy. In addition, it can also find out the location of the weaknesses of criminalization (cybercrime) in the ITE Law that need to be considered by law enforcement officials who implement this law. So, based on the description above the author is interested in taking the title of the effectiveness of imprisonment or fines for violators of ITE.

4. General Review of Mayantara Crime / ITE Crime

Cybercrime is a type of crime related to the use of an infinite information technology and has strong characteristics with an engineering technology that relies on a high level of security and credibility from information that is delivered and accessed by internet customers. In its development the internet turned out to bring a negative side, by opening up opportunities for the emergence of anti-social actions which had been considered impossible or unthinkable would occur. A theory states that crime is a product of society itself, which simply means that society itself is the one who produces evil.

In general, we can conclude that cyber-crime is a whole form of crime aimed at computers, computer networks, and its users as well as forms of traditional crimes in the form of computer-assisted crimes. This computer crime was issued by an organization of European community development (OECD) namely as follows: "any illegal, unethical or unauthorized behavior relating to automatic processing and / or transmission of data". From this definition, this computer crime includes all illegal access or unauthorized access to a data transmission. So that everything Unauthorized activity in a computer system is a crime. According to Andi Hamzah, computer crimes in general can be interpreted as illegal use of computers. From the understanding given by Andi Hamzah it can be concluded that he expanded the notion of computer crime, which is all illegal activities that use computers for criminal acts. No matter how small the impact or consequences arising from the use of computers illegally or illegally is a crime.

According to Barda Nawawi Arif, the forms of cyber-crime generally known in the community are divided into 3 (three) general qualifications, namely;

- Cybercrime related to confidentiality, integrity and existence of data and computer systems.
- Cybercrime that uses computers as a crime tool.
- Cybercrime related to data content or charge or computer systems.

In the opinion of Abdul Wahid and M. Labib, cyber-crime has several characteristics, namely:

- Actions carried out illegally without rights and / or unethical in cyberspace / territory, so that jurisdiction of the State which applies to them cannot be ascertained.
- The act is carried out using whatever equipment related to the internet
- The action resulted in material and in-material losses which tended to be greater than those of conventional law.
- The culprit is the person who controls the use of the internet and its applications.

Therefore, cyber-crime is a crime that is not only aimed at violating individual interests but can also result in damage to the system or order of life of the community.

5. Cybercrime Countermeasures

Although Indonesia was ranked first in cybercrime in 2004, there were not many cases decided by the court. In this case the number of the dark number is quite large and the data collected by the National Police is also not data originating from the Police investigation, most of the data is in the form of reports from victims. There are several reasons why the handling of cybercrime cases in Indonesia is unsatisfactory:

- Availability of funds or budgets for training HR is very minimal so that law enforcement institutions find it difficult to send them to training both at home and abroad.
- Absence of Computer Forensic Laboratories in Indonesia causes huge time and costs. In the case of Dani Firmansyah who hacked the KPU website, the Indonesian National Police had to bring a hard disk to Australia to examine the type of damage caused by the hacking.
- The image of the judiciary has not improved, even though various efforts have been made. This poor image causes people or victims to be reluctant to report their cases to the police.
- Legal awareness to report cases to low police. This is triggered by the image of the judiciary itself which is not good, another factor is the victim does not want the weaknesses in the computer system to be known to the public, which means it will affect the performance of the company and its web master.
- Efforts to deal with cybercrime require the seriousness of all parties since information technology, especially the internet, has been used as a means to build a culture of information. The existence of laws that regulate cybercrime is indeed necessary, but what is the meaning of the law if the implementers of the law do not have the ability or expertise in that field and the people who are targeted by the law do not support the achievement of the objectives of the law.

Some important steps that must be taken by each country in overcoming cyber-crime are:

- Modernize national criminal law and its procedural law, which are harmonized with international conventions related to the crime.
- Improve the national computer network security system according to international standards.
- Increasing the understanding and expertise of law enforcement officials regarding efforts to prevent, investigate and prosecute cases related to cybercrime.
- Increasing citizens' awareness of the problem of cyber-crime and the importance of preventing such crimes from occurring.
- Increasing cooperation between countries, both bilaterally, regionally and multilaterally, in efforts to deal with cyber-crime, including through extradition agreements and mutual assistance treaties.

5. Conclusion

Efforts to prevent information technology crimes in the future will be carried out by law enforcement officials, such as the following: First, educating law enforcement officials, because dealing with crimes through social media requires specialization of investigators and public prosecutors can be considered as one way to enforce law against cybercrime. In this case, especially criminal policies against humiliation and /or defamation through equitable social media by providing protection for the dignity of the President in relation to his position as head of state as a victim of criminal acts of humiliation and / or defamation through social media and with rehabilitation the President's good name. Currently Indonesia is in dire need of "Cyber Law Enforcement", such as: Cyber Police, Cyber Prosecutors, Cyber Judges and Cyber Advocates, in the context of cybercrime law enforcement in Indonesia. Without the presence of law enforcers who are in the field of information technology, it will be difficult to enforce "CyberLaw" in an equitable Indonesia. What is more important in law enforcement efforts is the dissemination in the form of upgrading, courses or joint vocational training between law enforcement officials in the framework of perception in the procedure of proof of criminal cases of information technology.

Second, Building forensic computing facilities to be established by the National Police. The improvement of facilities or facilities in dealing with information technology crimes is not only limited by trying as much as possible to up-date and up-grade the facilities and infrastructure that are already owned by law enforcement officials but also by completing these facilities or facilities in accordance with today's technological developments. Therefore, skilled labor and costs are needed, especially to support the abilities and skills of law enforcement officers in the computer field. The facility should also not only involve the National Police but the Government through the communication and information department builds its own facilities that function as information centers or laboratories as appropriate forensic laboratories as a place of research for the purposes of information technology investigation and development. Third, increasing investigative efforts, because criminal acts regulated by the ITE Law are special crimes, so special investigators are needed. Article 43 of the ITE Law states, in addition to the police, the authority of investigation is on the shoulders of Civil Servants (PPNS). Although it does not openly mention the Depkominfo, this Law describes that the PPNS comes from the government environment which is in charge of IT and Electronic Transactions. By forming a cyber task force by not only involving the National Police but also PPNS, Prosecutors and also judges whose scope starts from the central level to the provinces and also the districts. Collaborative efforts are not only carried out with fellow cyber law enforcement officers, but also ask for expert assistance needed in the investigation. The "expert" referred to here is of course someone who has special expertise in the field of IT and must be accountable academically and practically.

6. References

i. Andi Hamzah, 1989, Aspek-aspek Pidana di Bidang Komputer, Sinar Grafika, Jakarta
ii. Abdul kadir Muhammad, 2006, Etika Profesi Hukum, Citra aditya Bakti, Bandung
iii. Barda Nawawi Arief, 1991, Kebijakan Legislatif dalam Penanggulangan Kejahatan dengan Pidana Penjara, CV. Ananta, Semarang
iv. ---------------------------- 2006, Tindak Pidana Mayantara dan Perkembangan Kajian Cyber Crime di Indonesia, Rajawali Pers, Jakarta
v. --------------------------- 2008, Bunga Rampai Kebijakan Hukum Pidana, Kencana, Jakarta
vi. Bambang Sunggono, 2003, Metode Penelitian Hukum, RajaGrafindo Persada, Jakarta
vii. Eddy O.S. Hiariej, Prinsip-Prinsip Hukum Pidana, Sinar Grafika, Jakarta
viii. Republik Indonesia, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik