GLOBALIZATION, LAW ENFORCEMENT AND CYBER CRIME IN NATIONAL LAW SYSTEM

By Prof. Dr. Jeane Neltje Saly.[1]

[1]Senior Researcher in National Law Development Agency (BPHN), Department of Law and Human Rights of RI. Post Graduate Program in 1995 from Tarumanegara University, Doctorate in Law Majoring International Trade Law from Pajajaran University (2004)

A. Introduction

Globalization is the impact of technology development which makes the inter-personal communication and even among countries communication easier, and in turn, it results in the increase of daily activities. It impacts on the contradiction of various needs which were static in past and is changing nowadays and which moves forward fast towards a universal arrangement to fulfil human beings' needs globally.

The increase of technology utility will bring more surprise which should be responded in the field of law. In another word, it will result in law problems.

In conjunction with this, law should function itself as the facility of order as stated by Mochtar Kusumaatmadja,[2] regarding with the development implementation. In the daily activities, law will perform when there is a collision between value, rights and moral worth. John Rawls,[3] who has opinion about 'A

[2]Mochtar Kusumaatmadja, *Fungsi Hukum Dalam Pembangunan Nasional (Law Function in National Development)*, Binacipta, Bandung, 1979, p. 11

[3]John Rawls, *A Theory of Justice*, Harvard University Press, Cambrige, Massachusetts, 1995, p. 129-130.

Theory of Justice' stated that rights have tight relation with individual. Even it is stated that a person needs principles for national law and prioritized regulations to explain the emphasis when various principles to fulfil certain needs collide each other. To implement justice needs requirements which are arranged in law to be considered.

Traditionally, existing regulations are not adequate to accommodate activities in IT. The regulations in criminal codes are not enough to hold the electronic crime evidence. How the justice implementation in law enforcement on IT so that people will be safe to do their daily activities, and policy implantation to fulfil the law space in national law will be discussed further in the next part.

B. Globalization and Information Technology

Legal problems are always related with other fields outside law. Moreover in very progressive fields, such as information and technology which are one of aspects which accelerate globalization marked by the less significant borders among countries. Therefore, to keep the country in its order to increase people life, law should function itself as the guidance in considering national and international interest to keep them in balance.

Other expert Kenichi Ohmae,[4] stated that fields which accelerate globalization is investment, industry, information technology, and individual consumers.

It shows that the fast technology development gives benefit impact and also loss if law can not respond to the problems rising and bringing harm for people.

It brings benefit to people because it facilitates communication by using electronic information as the result of investment and information technology development. Kenichi Ohmae,[5] stated his opinion about the benefit of technology and information development which makes communication easier even when it crosses the country borders. He stated that the capital markets in most developed countries are flush with excess cash for investment (investment), industry is also far more global in orientation today than it was a decade ago. It is the effect of the growth of multinational corporations which cross the border cooperating with local companies (local markets). Also the movement of both investment and industry has been greatly facilitated by information technology, which now makes it possible for a company to operate in various parts of the world with having to built up an entire business system in each of countries where it has a presence. Individual consumers have also become more global in orientation. It is different with some decades ago. In the past, with the interests of their home government clearly mind, companies would strike deals with host governments to bring in resources and skills in exchange for privileged access to local markets.

[4]Kenichi Ohmae, *The End of The Nation State, How Capital, Corporations, Consumers, and Communication are Reshaping Global Markets*, FP New York London Toronto Tokyo Singapore, A Divitsion of Simon & Schuster Inc. 1230 Evenue of the Americas New York, 10020, 1995, p. 2-4.

[5]Kenichi Ohmae, *The Next Global Stage, Challenges And Opportunities In Borderless World*, Pearson Education Inc. Publishing as Whaton School Publishing. Upper Saddle River, New Jersey o7458, 2005, p. 21-23.

Kenichi Ohmae's opinion which was stated in 1986 was re-emphasized in his comment about the cyber-connected related with challenges and opportunities in our borderless world in 2005 that IT is really needed in all aspects of human life, stating "you have to married with IT". Global economy can not be and is not comprehensive without cyber technology prices. The internet is only the most public part of this. Today, the Internet Protocol (IP) is capable of handling transmission of not only data, but also images, voice, music, and videos. Voice over IP (VoIP) is rapidly making inroads into the world of traditional telecom providers, but music and movies are also downloaded across national borders, as long as there is a line with IP routers. Everything and everyone connects.

Nowadays, it is obvious that with the development of information technology, almost all aspects of human life are connected with technology and information. However, this condition can facilitate someone to do crime not only nationally but also internationally. It inflicts the damage, moreover concerning regulations are not sufficient to function themselves as the facility of order, especially in developing countries. Law (both about substance scopes,[6] rights and duties and burdening proof) is not adequate to support its certainty, which is arranged in dispersed regulations, and results in various different interpretations.[7]

The real condition can be depicted for instance in information technology application which in justice practice is considered by the judge not as the letter unless it is written and/or printed in front of authorized officials. Therefore public are questioning again about the status of electronic information in national law system, relating with criminal justice process, for instance,[8] which is applied in the case of Tempo and KPU-IT. This condition shows the needs of the determination of law enforcement apparatus in interpreting proof device, especially the assumption that the existence of electronic information has less legal value just because that it is susceptible to changes. Eventhough this assumption is not against the law, but it does not fit in its implementation and will inflict damage.

With the reason about the electronic format[9] its performance in justice process is often put aside, not further studied by the judge to make it as the lead. Judge in its function is

[6]One of the examples can be seen in Criminal Codes about goods interpretation (Pasal 174) includes non physical goods, those are data and computer program, telephone/telecommunication/computer service. Interpretation on key (Chapter 178) which includes inside the secret code, computer password, magnetic card, signal to open something.

[7]Relating with the fake testimony, in its development, the existence of information technology is recognized as "other evidence" beside chapter 184 Criminal Procedural Law based on Chapter 38 Act No. 15/2002 on Money Laundering, Chapter 27 Act No. 16/2003 jo Act No. 15/2003 on Combating Terrorism Crime, and Chapter 26 (a) Act No. 20/2001 on the Substitution on Act No. 31/1999 about Corruption Eradication. In short, it can be concluded that as the new evidence, it is the completion to evidence tool in Chapter 184 Criminal Procedural Law (letter, lead, witness explanation, expert opinion, and accused explanation) and not as the part of evidence tool recognized. Seems that this perspective tends to be wrong. As the consequence, there are two opinions. One states that electronic information can only be appropriately accepted in the scope of certain crimes, as clearly stated in Terrorism Act, Money Laundering Act, and Corruption Act. The other opinion states that it should also be accepted in court for other crimes. At least it should be categorized as leading proof tool or even letter as long as its validity is accountable in the judge's opinion.

[8]Warta Ekonomi No. 9, 5 Maret 2007, *Perangkat hukum di Indonesia dalam mengatasi kejahatan computer (Law Equipments in Indonesia to Combat Cybercrime)* , h. 12-14

[9]Electronic Information can be interpreted by referring to Chapter 41 Criminal Procedural Law, which in its explanation it is stated that those included in "letter" are telegram, telex, and its types, which contain news. Telegram or telex is originally in form of electronic message which is delivered electronically, which later converted in paper.

obliged to interpret information from the letters, experts' opinion, and the explanation from the accused. Therefore judge is assumed to know enough and up to date, especially about the existing technology development or at least can figure out from experts' opinion.

Information technology application as one of the modernity products has experienced a giant leap. In the end of this 20th century, some works were founded in the field of information technology; one of them is internet, an information technology media of virtual basis known as "virtual world". At the beginning, internet is neutral (free of values). But in its progress, this technology tempts some parties to misuse.

The emergence of the new crime dimension as the result of internet misuse is the real implication. The internet existence has brought the huge impact. Therefore is is recognized that the development of science and technology is able to increase the human life quality, but also it is undeniable that inside its progress, there are potentials of bigger problems.

As in the real world, in the virtual world there are various forms of crimes. Internet has invited the criminals to find material benefit or just for fun. It rises the specific phenomenon called *cyber crime*.[10]

Basically, the crime related with information technology (IT) can be divided into two main parts. First, crime to damage or attack system or computer network. Second, crime using computer or internet as the tool to facilitate its crime. However, considering that information technology is a telecommunication, computer and media convergence, the types of crimes improves fast. The category of general crimes which are facilitated by information technology are among them credit card fraud, stock exchange fraud, banking fraud, child pornography, drug trading, and terrorism. Meanwhile, crimes which make information technology facility as their target are denial of service attack (Ddos), defacking, cracking or phreaking.[11]

Cahyana Ahmadjayadi, states that the impact of crimes in information technology is potential to inflict damage in politic, economy, socio culture, which are bigger than other high intensity crimes.[12].

It is also stated by Supancana in the same seminar that the fact and data about cyber crime progress shows the significant increase in the aspects of

[10]In the study of BPHN on the Convergence between Information Telecommunication and Computer 1998, some problems were found out: legal burden proof in term of electronic transaction, piracy towards intellectual property rights relating with telecommunication and information, contain, unlawful inadmissible content; information security, law documents legality in electronic transaction, mobility freedom towards the telecommunication and information equipments in personal use interest relating with the problems of tax, customs, etc, law enforcement,), state sovereignty relating with producer responsibility, consumer protection relating with producer responsibility, telecommunication and information equipment standard, hardware and software certification, personnel certification, information access freedom, monopoly prevention, limited natural resources management, institutions, professionalism if law enforcers, license and monitoring, government role, government income, harmonization of national regulation and international regulations, etc

[11]See: Heru Sutadi, *Cyber Crime, apa yang bisa diperbuat?(Cybercrime, What can we do?)* in Htttp://www.sinar harapan.co.id., see also: Budi Rahardjo, *Cybercrime*, in http://budi.insan.co.id/articles/ cybercrime.doc. According to Budi Rahardjo, cyber crime can be done by 1) stealing and using other's account, 2) web hacking(deface), 3) spreading virus, 4) Denial of Service (DoS) and Distributed DoS (DDos) attack), and cyber squatting.

[12]Cahyana Ahmadjayadi, *Cybercrime dan Cyberporn dikaitkan dengan UU Informasi dan Transaksi Elektronik (ITE) (Cyber Crime and Cyberporn Relating with Electronic Information and Transaction Law)*, a paper for the Seminar on Cyber Crime and Cyber Porn in the Perspective of Criminal Law and Technology Law, held by BPHN in cooperation with Post Graduate Programme of Diponegoro University and Regional Office of Department of Law and Human Rights Central Java, Semarang, 5-7 Juni 2007.

quantity, quality, frequency and modus operandi[13].

There is also the tendency of cyber crime in Indonesian national law which impacts in various problems. Those problems should be anticipated both to reduce or to prevent the crime.

C. The Problems of Cyber Crime

In fact, *cyber crime* has made restlessness and discourages from all parties. *Cyber crime* can happen to everyone and every party, whether individual, consumer, corporation, government and other law institutions with unpredictable methods but with fatal impact. Meanwhile the scope of cyber criminals does not recognize the border and jurisdiction as the result of globalization. It adds the complexity which is faced in its uncover, prosecute, justice and law enforcement.

With its specific character, the existing law can not cover the cyber crime yet. Especially on the conventional principles in criminal law and existing doctrine such as legality base, culpability base, jurisdiction base, evidence tool, and many more.

In legal approach, cyber crime and its eradication face various problems such as legality base, jurisdiction base, and evidence tool.

D. Policy in Cyber Crime Law Enforcement

In fact, the policy on cyber crime eradication has been brought about. The policy is not only based on juridical approach, but also should be adjusted with technology approach it self and cultural approach[14]. This policy as stated in UN Congress Resolution VIII/1990 about *computer related crimes*[15]. As stated by Minister of Law and Human Rights of the Republic of Indonesia that

[13]I.B.R. Supancana, Cahyana, Peran Kerjasama Internasional Dalam Pencegahan Dan Penanggulangan Cybercrime, Khususnya Cyberpornography (International Cooperation Role in Preventing and Eradicating Cybercrime, especially Cyber Pornography) , a paper for the Seminar on Cyber Crime and Cyber Porn in the Perspective of Criminal Law and Technology Law, held by BPHN in cooperation with Post Graduate Programme of Diponegoro University and Regional Office of Department of Law and Human Rights Central Java, Semarang, 5-7 Juni 2007. 1. Information Technology Company Computer Associate (CA) is mapping 7 (seven) attack pattern which are potential to threat internet in 2007 with increasing intensity. At least there are some attack patterns threatening internet. It is more sophisticated in stealing intellectual property rights, personal identification, financial report across the country boundaries, in organization and social network. A lot of harm ware damaging network with Trojan, worm, virus and spyware. Phising is smarter with social manipulation tactics. Spamming is increasing due to "spam image based" which can penetrate all anti spam filters. Due to its cheap cost to spread spam via botnet, internet criminals use Trojan spread medium. Meanwhile local computer virus called "Pacaran" now attacks by using format to hack local network computer data (Roni Yunianto, *CA: Serangan ke Internet makin canggih (CS: Attack to Internet is more Sophisticated)*, Bisnis Indonesia, 13 Februari 2007). 2. US Federal Trade Commission (FTC) noted consumers complains over 670.000 fraud and identity theft in 2006 which inflicted financial loss US $ 1.2 billion. For 7 years in row, identity theft had the highest number 36% or 2466.035. Identity theft was generally a credit card fraud (carding) 25%, and followed by phone or utilities fraud and bank fraud. After identity theft, other thefts were Shop at-home, catalog fraud , fraud in prices, sweepstakes and lottery, fraud at internet auction web sites (Christopher S Rugaber, "Identity Theft tops consumer complaints in 2006:FTC Report", The Jakarta Post, 9 Pebruari 2007). 3. Mid Year Report of Internet Security Threat Report from Symantec software vendor stated that 157.000 unique messages "phising" were spread throughout the world in the first periode of 2006, with the growth of 81% compared with the same period before in 2005(Reuters, "Criminal flock to the internet, survey finds", 23 September 2006). 4.AT & T Inc. reported that due to hackers accessing the computer and stealing personal data and credit card information from thousands consumers who bought DSL equipments from AT & T online store. Almost 19.000 consumers were attacked by those hackers. At the same moment, an NGO called Privacy Rights Clearing House counted more than dari 170 internet security violation which openly expressed relating to the personal sensitive information (Reuters, "Criminal flock to the internet, survey finds", 23 September 2006).

[14]Lihat : Ahmad M. Ramli, Cyber Law dan HAKI Dalam Sistem Hukum Indonesia (*Cyber Law and Intellectual Property Rights in Indonesian Law System)*, Refika Aditama, Bandung, 2004, p. 3-4.

[15]See : Eight UN Congress on the Prevention of Crime and the Treatment of Offenders, Report, in Barda Nawawi Arief, Tindak Pidana Mayantara (*Mayantara Crimes)*, Raja Grafindo Persada, Jakarta, 2005, p. 2-5.

to cope with information technology progress, especially to prevent the forms of *Cybercrime* needs to: first, close the access from technology equipment; second, with law signs; and third, developing the people mental attitude on the information entry.[16].

Crime in information technology is closely related with criminalization policy concerning with *cyber crime.* This criminalization policy is a policy in determining an activity which is previously not a crime (not get the punishment) becomes a crime (punishable). So, basically, the criminalization policy is a part of criminal policy by using penal tools to be included in criminal policy. Actually, criminalization policy in *cyber crime* is not merely national (Indonesia) policy problem, but also related with regional and international policy[17].

While the criminalization policy can be viewed in the perspective of penal policy, not merely policy to formulate activities which are punishable (including the punishment), but also includes the problem of how the formulation/ legislation policy can be arranged in one united system in harmonious criminal law system (legislative policy).[18]

UN Congress Resolution VIII/1990 about *computer related crimes* suggests some policies relating with cyber crime eradication, those are[19] :

1. Requesting the member countries to intensify the more effective efforts to eradicate computer misuse.
2. Requesting member countries to increase international activities in eradicating cyber crime.
3. Recommending to United Nations Committee on Crime Prevention and Control to :
   a. Spread the guidance and standard to help member countries to face cyber crime in national, regional, or international level;
   b. Develop further research and analysis to find new methods to face cyber crime problems in the future.
   c. Consider cyber crime in reviewing extradition agreement implementation and cooperation assistance in crime prevention.

Although Indonesia has not yet brought about the harmonisation policy steps with other countries, especially in ASIA/ASEAN, Indonesia has tried to anticipate it in the new Criminal Code arrangement[20], for instance in First Book (General Arrangement), are made the stipulations about:

a. Interpretation on goods (Chapter 174) which includes inside non physical goods, those are data and computer program, telephone/ telecommunication/computer service.
b. Interpretation on key (Chapter 178) which includes inside the secret code, computer

[16]See : Minister of Law and Human Rights of the Republic of Indonesia, *Keynote Speech* in the opening of the Seminar on Cyber Crime and Cyber Porn in the Perspective of Criminal Law and Technology Law, held by BPHN in cooperation with Post Graduate Programme of Diponegoro University and Regional Office of Department of Law and Human Rights Central Java, Semarang, 5-7 Juni 2007.

[17]*Ibid.,* p 21. in UN Congress X/April 2000 about computer related crime stated that States should seek harmonization of the relevant provisions on criminalization, evidence and procedure.

[18]*Ibid.,*

[19]*Ibid..*

[20] *Ibid.,* p. 15.

password, magnetic card, signal to open something.

c. Interpretation about letter (Chapter 188) includes written/ saved data in disk, magnetic tape, computer storage media or other electronic storage media.

d. Interpretation on space (Chapter 189) includes range or computer terminal which is accessible with certain methods.

e. Interpretation on entry (Chapter 190), includes computer access or entry into computer system.

f. Interpretation on network (Chapter 191) includes computer network or computer communication system.

Besides, in Book II (Crime), the formulation of cases or addition of new cases concerning technology progress is carried out, among them are[21] :

a. Tapping conversation in a room with technical help tool (Chapter 264);

b. Installing technical help tool to hear/record the conversation (Chapter 264);

c. Recording (possessing/ broadcasting) images with technical help tool in room not for public (Chapter 266);

d. Damaging building for public service infrastructure (among them are long distance telecommunication/ communication via satellite)-Chapter 546;

e. Money Laundering)-Chapter 641-642.

Concerning with *cybercrime* handling, Indonesia which follows positivism faces some problems. Therefore, it needs changing in cyber crime handling, as well as the bravery and innovation from law enforcement apparatus to make the existing rules effective by doing interpretation or law construction which is based on the basis idea which is accountable conceptually.

E. Cybercrime in National Law

National Law is basically a system.[22] System is an order, an entity which consists of parts relating one to another, arranged in a plan or pattern, a result of a thought to achieve the goal.[23] This system consists of various elements or components or variable/function which influence each other, related one to another by one or some principles and interaction. All elements/components/ functions/variables are closely joined and organized in accordance with a certain pattern or structure, so always influence each other. The main principle connecting all elements or national law components is Pancasila (Five Principles) and 1945 Convention, beside some law principles such as archipelago, nationality, diversity. National Law System does not merely consist of norms and rules, but also includes all apparatus institution

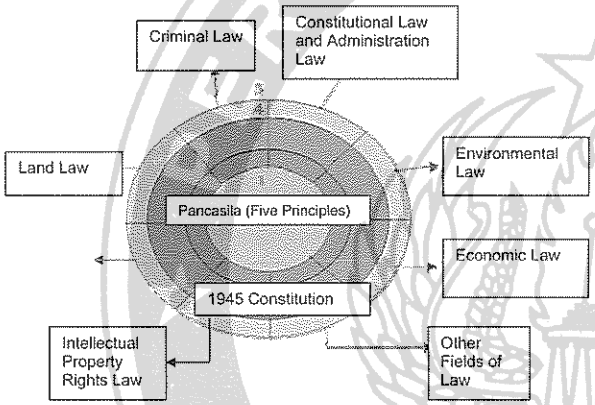
[21] *Ibid.*, p. 16.

[22] BPHN, *Pola Pikir dan Kerangka Sistem Hukum Nasional Serta Rencana Pembangunan Hukum Jangka Panjang (Paradigm, National Law System Frame, and Long Term Law Development)* (Jakarta: BPHN, 1995/1996) p. 19.

[23] Subekti, *Beberapa Pemikiran Mengenai Sistem Hukum Nasional Yang Akan Datang (Some Views on the Future National Law System)*, Paper for National Law Seminar IV, 1979 p. 79

and organisation, law mechanism and procedure, legal philosophy and culture, including legal behaviour of government and people.

Based on the systemic perspective, National Law System includes various sub fields of law and various forms of law which are in effect which all of them have the source in Pancasila. The diversity of law which previously happened in Indonesia (law pluralism) transforms into law fields which will be developed *(ius constituendum)*.



These fields of law become the focus in National Law progress and development toward the order of Indonesian Modern Law which has source in the behaviours (last circle), jurisprudence (forth circle), regulation (third circle), 1945 Convention (second circle), and Pancasila as the source of all legal sources.

From the picture above, especially at the fifth circle, some laws will emerge. It is caused by law. Therefore, Prof. Sunaryati anticipated it by writing other fields of laws. And, today, it happens amidst the existence of information technology as the convergence of telecommunication, information and computer which results in a new media called internet and produces a new law regime called cyber law.

Cyber law development from substance perspective should anticipate various forms of crimes in cyber (cyber crime)[24]. The problems in establishing rules in cyber, at the beginning, faces many obstacles. Therefore, in the study carried out by BPHN, there are some views, opinions related with the formulation of policy and arrangement in this cyber field, those are[25]:

1. Formulating the really new legislations as the specific form of regime to arrange all aspects related with information technology activities.
2. Applying existing regulations on the cases emerged in information technolgy.
3. Adopting regulations as being valid in more advanced countries or ones which are internationally valid.

Concerning with *cybercrime*, there may be regulations which arrange problems in IT generally, however cybercrime is arranged by its own regulations.

The conventional penal code, as it is seen, can not fully cope with crimes using information technology media. This condition underlines the statement that law is always behind the progress. Therefore, Cyber Law (Bill on Information and Electronic Transaction) should be able to accommodate public interest on the Information Technology misuse. In that conjunction, criminal codes should

[24]In Prof Sunaryati's opinion, law development includes law substance development, apparatus developments, infrastructure and legal culture

[25]BPHN, Pengkajian Hukum tentang Konvergensi Telekomunikasi, Informasi dan Komputer (Study on Telecommunication, Information and Computer Convergence), 1998. p.36-37

anticipate technology progress. And, however in Criminal Codes Bill there are some changing, the specific regulations as the *lex specialist* can not be ignored.

F. Conclusion and Suggestion

From the explanation above, some points can be elaborated as follow:

1 Cyber Law, can be classified as particular law regime because it has multi-aspects, such as aspect of criminal, private, international, administration and Intellectual Property Rights.

2 The negative impacts of information technology (internet) can not be ignored. Crimes which are previously conventional can be carried out by using online media nowadays whose damage impacts are bigger, both on the people and country.

3 Cyber crime also results in new crimes. Due to its different character from general crime, either in the aspects of doer, victim, modus operandi and location, it needs specific handling and arrangement outside from Criminal Codes.

4 Responding the demand and challenge of global communication via internet, the expected Law (*ius konstituendum*) is law equipment which is accommodative towards the development and anticipative towards the problems, including negative impacts of internet misuse with various motivations which result in victims such as material and no material damage.

5 Indonesia has not had yet the specific law/cyber law about cyber crime. It is expected in the near future, the bill on Information and Electronic Transaction which is being discussed today can be established soon.

6 Without specific regulations on cyber, it needs to develop the expert opinions and doctrines which can become the basis in handling the cyber crime

7 To give the same perception about IT problems, and to strengthen cyber crime eradication, it also needs to improve human resources development in IT for law enforcement apparatus.

BIBLIOGRAPHY

Ahmad M. Ramli, *Cyber Law dan HAKI Dalam Sistem Hukum Indonesia (Cyber Law and Intellectual Property Rights in Indonesian Law System)*, Refika Aditama, Bandung, 2004.

Barda Nawawi Arief, *Tindak Pidana Mayantara (Mayantara Crimes)*, Raja Grafindo Persada, Jakarta, 2005.

BPHN, *Pengkajian Hukum tentang Konvergensi Telekomunikasi, Informasi dan Komputer* (*Study on Telecommunication, Information and Computer Convergence*), 1998.

BPHN, *Pola Pikir dan Kerangka Sistem Hukum Nasional Serta Rencana Pembangunan Hukum Jangka Panjang (Paradigm, National Law System Frame, and Long Term Law Development)* (Jakarta: BPHN, 1995/1996).

Budi Rahardjo, *Cybercrime*, in http://budi.insan.co.id/articles/cybercrime.doc.

C.F.G Sunaryati Hartono, *Pembinaan Hukum Nasional dalam Suasana Globalisasi Masyarakat Dunia (National Law Development in World Globalization).* Speech in the Professor Inauguration in Law Faculty, Padjadjaran University Bandung, 1991.

Cahyana Ahmadjayadi, *Cybercrime Dan Cyberporn Dikaitkan Dengan UU Informasi dan Transaksi Elektronik (ITE) (Cybercrime and Cyberporn Relating with Electronic Information and Transaction Law)*, a paper for the Seminar on Cybercrime and Cyberporn in the Perspective of Criminal Law and Technology Law, held by BPHN in cooperation with Post Graduate Programme of Diponegoro University and Regional Office of Department of Law and Human Rights Central Java, Semarang, 5-7 Juni 2007.

Heru Sutadi, *Cybercrime, apa yang bisa diperbuat? (Cybercrime, What Can We Do?)* in Htttp://www.sinar harapan. co.id.

I.B.R. Supancana, Cahyana, *Peran Kerjasama Internasional Dalam Pencegahan Dan Penanggulangan Cybercrime, Khususnya Cyberpornography (International Cooperation Role in Preventing and Eradicating Cybercrime, especially Cyber Pornography)*, a paper for the Seminar on Cybercrime and Cyber porn in the Perspective of Criminal Law and Technology Law, held by BPHN in cooperation with Post Graduate Programme of Diponegoro University and Regional Office of Department of Law and Human Rights Central Java, Semarang, 5-7 Juni 2007.

John Rawls, *A Theory of Justice*, Harvard University Press, Cambrige, Massachusetts, 1995, p. 129-130.

Kenichi Ohmae, *The End Of The Nation State, How Capital, Corporations,Consumers, And Communication are Reshaping Global Markets*, FP New York London Toronto Tokyo Singapore, A Divitsion of Simon & Schuster Inc. 1230 Evenue of the Americas New York, 10020, 1995, p. 2-4.

....., *The Next Global Stage, Challenges And Opportunities In Borderless World*, Pearson Education Inc. Publishing as Whaton School Publishing. Upper Saddle River, New Jersey o7458, 2005, p. 21-23.

Kusnu Goesniadhie S, *Harmonisasi Hukum Dalam Perspektif Perundang-undangan (Lex Spesialis Suatu Masalah) (Law Harmonization in the Legislation Perspective (lex specialist of Certain Problem)*, (Surabaya: JP BOOKS, 2006).

Minister of Law and Human Rights of the Republic of Indonesia, *Keynote Speech* in the opening of the Seminar on Cyber crime and Cyberporn in the Perspective of Criminal Law and Technology Law, held by BPHN in cooperation with Post Graduate Programme of Diponegoro University and Regional Office of Department of Law and Human Rights Central Java, Semarang, 5-7 Juni 2007.

Subekti, *Beberapa Pemikiran Mengenai Sistem Hukum Nasional Yang Akan Datang (Some Views on the Future National Law System)*, Paper for National Law Seminar IV, 1979.