Jurnal Dinamika Hukum

Vol. 21 Issue 3, September 2021
E-ISSN 2407-6562 **P-ISSN** 1410-0797
National Accredited Journal, Decree No. 21/E/KPT/2018
DOI: 10.20884/1.jdh.2021.21.3.3256.

Prevention of Cybercrime through the Development of Criminal Responsibility Principles for Internet Users

Agus Raharjo✉
Faculty of Law, Universitas Jenderal Soedirman, Purwokerto - Indonesia

Abstract
There is no guarantee of security in cyberspace. Cybercrime is the use of computer technology for illegal activities. Cybercrime ignores territory, and can even become an automatic crime according to the nature of the machine. The crime prevention model, which has been more reactive and only suitable for the real world, is not an effective way to deal with cybercrime. This research is normative legal research, with the main data source in the form of secondary data. Hacking is an illegal activity that takes many victims and its handling is not complete. The difficulty that arises is the issue of jurisdiction because perpetrators and victims are often in different jurisdictions. Although legal instruments have adopted provisions on the principle of ubiquity, in practice it is not as easy as imagined. The Bangkok International Summit (2007) invites countries to promote cyber security by increasing and developing international global partnerships to prevent, detect, and cybercrime, but this has not been implemented properly. For this reason, it is necessary to develop the principle of criminal responsibility which can be an incentive in overcoming cybercrime.

Kata kunci: cybercrime; hacking; ubiquity; criminal responsibility.

Abstrak
Tidak ada jaminan keamanan dalam cyberspace. Cybercrime merupakan penggunaan teknologi komputer untuk aktivitas illegal. Cybercrime mengabaikan territorial, dan bahkan dapat menjadi kejahatan yang bersifat otomatis sesuai dengan sifat kerja mesin. Model penanggulangan kejahatan yang selama ini lebih bersifat reaktif dan hanya cocok untuk dunia nyata, tetapi bukan cara yang efektif untuk menangani cybercrime. Penelitian ini merupakan penelitian hukum normative, dengan sumber data utama berupa data sekunder. Hacking merupakan aktivitas illegal yang banyak memakan korban dan penanganannya tidaklah tuntas. Kesulitan yang muncul adalah masalah yurisdiksi, karena pelaku dan korban seringkali berada pada yurisdiksi yang berlainan. Meski instrumen hukum telah mengadopsi ketentuan tentang prinsip ubiquitas, akan tetapi dalam praktiknya tidaklah semudah yang dibayangkan. The Bangkok International Summit (2007) yang mengajak negara-negara di dunia untuk mempromosikan keamanan cyber melalui peningkatan dan pengembangan kemitraan global internasional untuk mencegah, mendeteksi, dan kejahatan dunia maya, akan tetapi hal ini pun belum dapat dilaksanakan dengan baik. Untuk itu diperlu dikembangkan prinsip pertanggungjawaban pidana yang dapat menjadi insentif dalam penanggulangan cybercrime.

Kata kunci: cybercrime; hacking; ubiquitas; pertanggungjawaban pidana.

Introduction

Mandiant's report – a cyber security company based in Virginia, USA – which has 60 pages long, is quite shocking. The report, which is the result of a three-year investigation, exposed the cyber-espionage practices of Unit 61398, which is directly under China's People's Liberation Alliance (PLA). The report states that hacking and espionage practices

✉Corresponding Author: agus.raharjo007@gmail.com

have been going on for at least the last seven years. Recorded 141 companies from all over the world, 115 of them from the United States have become victims. The longest hacking and espionage practice lasted 4 years and 10 months, with the largest amount of data hacked being 6.5 terabytes experienced by one company over 10 months. Of course, the Chinese government denied any involvement in hacking and espionage, but Kevin Mandia – the founder of Mandiant – managed to trace the involvement of the Chinese government through its armed forces (Kompas, 2013a).

The United States government - through its Attorney General, Eric Holder - immediately responded to the results of the investigation by seeking to increase diplomatic pressure to formulate new rules that reduce threats to security and the country's business world. In addition, Holder also revealed plans to collaborate with other countries governments to jointly suppress China and other cybercriminal countries. Some of the world's largest companies have fallen victim to cyber hacking and espionage, including General Motors, Ford, DuPont, Dow Chemical, Motorola, Boeing, and Cargill. As a result of these illegal activities, they suffer heavy losses due to loss of market position, competitive advantage, and efficiency (Kompas, 2013b).

What happened to the United States Government and big companies was only one activity of many hacking activities from hackers. Not only political issues, such as the endless cyber war between Palestine and Israel, North and South Korea, or Indonesia and Malaysia when there is a problem with Indonesian migrant workers, even trivial issues can spread to the cyber world quickly. It has become an adage in the cyber world, that there is no guarantee of security so any security system can be penetrated by hackers. As the saying goes, water that continuously drips onto a rock will cause the stone to have a hole, so it is the same with security in cyberspace. Valuable information – in this case, a trade secret – when stored on servers connected to the internet becomes a target for hackers.

There are many incidents in cyberspace, and what appears on the surface does not appear murky in its depths. Criminal statistics on cybercrime recorded by the police do not reflect the true face of incidents in cyberspace, so there are no accurate cybercrime statistics. Wearden noted that there were two reasons why this could happen, namely that many cybercrimes were not detected and many cybercrimes were detected but not reported. Cybercrime goes undetected because security systems can't detect outside penetrations or because the attack was carried out by a trusted insider, who knows how to remove the traces. Entrepreneurs or economic actors who own websites sometimes do not admit that their websites are attacked by cyber criminals, so there is no anxiety for customers and shareholders (Brenner, 2008).

There are many reasons why victims are reluctant to report incidents that happened on their websites to the authorities. The characteristics of cybercrime that make it easy for perpetrators to erase their tracks, distance that is not a problem, and the inability of law enforcement agencies, are some of the dominant reasons for not disclosing cybercrime. Of course, if you rely on law enforcement officers, cybercrime will not be resolved, because this problem does not only involve legal aspects, more than that it is a technology problem

that from time to time continues to grow faster. The ability of hackers or cybercrime actors from time to time continues to grow.

The penal system in criminal law does not provide specific deterrent properties to criminals with a technological dimension. Several types of punishment that exist in criminal legislation are more oriented towards traditional criminals. This is coupled with the criminal implementation system in prisons that still tolerates prisoners either openly or secretly bringing information technology products into the correctional institution. Of course, you still remember how Imam Samudera – a prisoner in the Bali Bombing case – was able to get a laptop and communicate with his colleagues outside the prison.

The prevention and control of cybercrime are not finished with the criminalization of the act through the promulgation of Law no. 11 of 2008 concerning Information and Electronic Transactions in conjunction with Law no. 19 of 2016 concerning Amendments to Law no. 11 of 2008. Moreover, the type of punishment threatened is still oriented to the type of crime contained in the Criminal Code, so it does not provide a deterrent effect of technology on criminals. This article tries to provide an alternative form of punishment while still basing it on the principle of criminal individualization which is in line with the spirit of reforming the national criminal law.

Research Problems

The rise of cybercrime with various forms of crime, both broad sense and narrow sense, deserves proper attention from stakeholders, including academics. There are two main problems discussed in this article, namely: first, what is being done by the state/government in the prevention and control of cybercrime; and second, how to develop the principle of criminal responsibility for internet users as an effort to create a deterrent effect and provide education for them.

Research Method

The research method used to answer the problems above is doctrinal normative legal research, through a statutory approach, conceptual approach, and case studies. The statutory approach is carried out by examining the laws and regulations related to the problems studied, while the conceptual approach is carried out to understand the concepts related to crime prevention, cybercrime, and criminal liability. The case approach is carried out to examine cases that occur and solve problems in these cases. The research specification is descriptive. The main data source is secondary data generated from the literature study. The data that has been obtained, is then analyzed using qualitative descriptive analysis.

Discussion

Internet and Cybercrime in The Perspective of Technological Theory

Since telecommunications technology and computer technology – supported by micro-electronics, materials, and software, and based on chemistry, physics, biology, and mathematics – can be mated and give birth to a "smart" object called the internet, since then humans have started to think and act to transcend the traditional boundaries of his mind and territory. The borderless way of thinking as introduced by Steven Harnad and the reluctance to deal with convoluted bureaucracies (smash the boundaries, tear down the hierarchy and dismantle the bureaucracy) as stated by Lipnack and Stamps (1994; Branscomb, 1983) have become characteristics of the way of thinking and doing of humans (old and young) internet enthusiasts. Such people have entered a new zone in life, namely the technology intoxication zone (Naisbitt, Naisbitt and Philips, 2001).

The Internet eventually became a symbol, a symbol of progress as well as civilization. The Internet offers many advantages, conveniences, hopes, pleasures, and opportunities. In this millennium era, the internet is like a god who is being praised and able to replace the myth of the gods in the Ancient Greek era. However, like a coin that has two sides, like binary logic, the Internet also offers easy ways to commit crimes without being hindered by the traditional boundaries of the criminal world.

As a result of technology, the Internet is of course a source of rampant crime in the cyber world or better known as cybercrime. Brenner said that cybercrime is the use of computer technology for illegal activities (Cybercrime consists of using computer technology to engage in illegal activity or the use of computer technology to achieve illegal ends, i.e., to commit crimes) (Brenner, 2004, 2008). Is it right that the internet should be blamed? This certainly deserves to be discussed, especially when viewed from the perspective of the theory surrounding technology and the results of the technology itself. Of course, the explanation for this cannot be obtained from law or criminology, but from the science that is developing in Europe and the United States, and few Indonesians are concerned about the development of this science, namely social science of technology or the social construction of technology (Raharjo, 2007a).

If we look closely, the internet is actually "just" a tool from a technological product, but from what was original "only" a tool it has now developed into an entity that cannot be simply ruled out in our lives. If we look at the internet in terms of instrumental theory and other technological outcomes, then the internet is a tool or tool that is ready to serve the purposes of its users. Technology is considered “neutral”, without an assessment of the content of the technology itself. Technology has nothing to do with good or bad and can be used in whatever way, political or social, according to the wishes of people or institutions. Technology is a “rational entity” and is generally accepted, followed by standards of the same or similar size so that it can be applied to different situations (Feenberg, 1991).

If it is followed by thoughts from substantive theory, there will be different judgments about technology (c.q. internet). The substantive theory known through the thinking of Ellul and Heidegger argues that technology underlies a new type of cultural system that reorganizes the entire social world as an object of control. Feenberg (1991) suggests that

when we choose to use technology, we are making a variety of cultural choices without realizing it. Technology is not only meaningful but has become an environment and a way of life, this is a substantive impact. When the thought arises of the neutrality of a machine, Pacey says that we must look further at the human network that surrounds the machine which includes its practical use, its role as a status symbol, and in the second step as part of life, not something that can survive from a separate space.

Based on these two theories, an explanation of the internet's position in cybercrime can be obtained. For adherents of instrumental theory, the internet is only a tool or means to commit crimes, the use of the internet to commit crimes is traditionally described as cybercrime. The use of this theory to explain cybercrime is in line with the term stated by Grabosky (2001) who describes cybercrime as "old wine in new bottles". In the view of instrumental theory, the internet is only a place of migration from crimes in the real world or traditional crimes that have existed since antiquity to cyberspace, such as fraud, theft, counterfeiting, and so on. The motive used to commit this crime is the same as the motive for traditional crimes in general, the only difference is the means.

For adherents of substantive theory, the internet is not just a tool. It is a technological product that has certain characteristics, created through a socio-cultural process – not just technical – which causes it to have the form and content it is today. It is not neutral, and because it is not neutral, it also influences the mindset of people. The internet is a material symbol of the embryo of a global society, which offers a new space, namely cyberspace, a new reality, namely virtual reality, and a new community, namely virtual community. The internet as a cultural product – especially in American culture – is new ground for the development of wild-wild west, postmodern, cyberpunk, and so on.

Based on this, and based on Lacasagne's opinion that society has its criminals, then cyberspace besides having its criminals also has unique evil deeds or crimes that cannot be found in the real world. It is said to be typical, because this form of crime is only possible through the internet, nothing else. Of the many typical crimes, there are several that are often examples, namely hacking, virus dissemination, and DDos (a distributed denial of service) attack.

Hacking is a way to enter other people's sites by getting unauthorized access even though there is no intention to commit a crime, but this is still a violation category. This is different from cracking, where unauthorized access is followed by an intent to commit a crime, which Brenner uses as an analogy with burglary (robbery). Similarly, the dissemination of viruses, worms, or malicious code is equated with vandalism. Denial of Service Attack is an attack through certain packets, numbering very much, by reducing website performance continuously to repeat requests to servers from several sources simultaneously. This attack aims to make the victim's server become overwhelmed in serving requests that end in activity termination or stop by itself. DDoS attacks are "new", crimes that are the product of new technologies.

Some countries, such as Indonesia, use the existing law to prosecute perpetrators of this type of cybercrime. both the method and the effects. Hacking, cracking, and spreading

viruses even though they look the same as traditional forms of crime, however, the environment in which the behavior occurs is different, one in the real world and the other in cyberspace, in addition to many other differences. Vandalism in the real world tends to pose little harm, but the spread of a virus or malware can result in loss or damage worth millions or even billions of dollars. This is because the nature of the internet is open, Mondial, and the perpetrators have high skills so that when they commit a crime their hands are invisible (invisible handshake).

Based on the perspective of substantive theory in technology, it can be explained that technology/internet is not neutral. The internet has given birth to a new type of cultural system with various cultural choices that have unconsciously influenced the way people think and act, but also become a new environment and way of life, this is a substantive impact. The internet is finally not only a status symbol of progress but has also become a part of our lives. If you look at this rationale, and it is associated with new forms of crime that exist in cyberspace, then based on the perspective of substantive theory, the term is no longer old wine in new bottles but new wine without bottles. This happens because many cybercrimes cannot be analogous to traditional crimes and there is no regulation in criminal law. Therefore, a new arrangement is needed to accommodate this cybercrime, so the term is changed to new wine in new bottles.

One thing to remember is that actors in cyberspace in the philosophy of technology can be classified as adherents of technological determinism with several variants, either in full or in part (Raharjo, 2007a). For them, technology/the internet is the only talisman or passport to support their activities. Without this technology or without the energy source that is the life force or supports the operation of the technology, their activities will stop. We can simply give an example of our dependence on technology so that when the power goes out or the battery runs out, our work is delayed or finished prematurely.

Reaction to *Cybercrime* and The Prevention

Quite a variety of reactions arise as a result of cybercrime. For government-owned public agencies – such as the websites of General Election Commissions (Komisi Pemilihan Umum/KPU), Indonesian Police (Kepolisian Republik Indonesia/POLRI), Defense and Security, and other ministries – or business entities whose websites are attacked or damaged by hackers have different reactions. The government whose website is attacked will officially announce to the public about the attack, but some do not publish it, while business entities, prefer to remain silent or hide what happens to their website after being visited by cyber criminals.

It's natural to have mixed reactions because this is related to the investment that has been invested in building a website. If the government uses State Budget (Anggaran Pendapatan dan Belanja Negara/APBN) or Regional Revenue and Expenditure Budget (Anggaran dan Pendapatan Belanja Daerah/APBD) funds, notification to the public is a form of accountability (accountability), so they need not be ashamed to disclose it, although this will have an impact on the website manager. Business entities are often not

reactive in responding to this cybercrime because usually the damage caused can be resolved alone or the damage does not cause systemic impacts that can change or disrupt their business activities.

The government in a wider context reacted by making laws and criminalizing cybercrime, so Law no. 11 of 2008 concerning Information and Electronic Transactions. However, prevention of cybercrime is not enough with the birth of law, or in other words, prevention is only entering the early stages. In reality, this law still has many weaknesses, especially with its nature as an umbrella act so that it cannot reach cybercrime that is new and detailed. More detailed and specific arrangements are still needed to make it easier for law enforcement officers to use or apply when dealing with cybercrime in practice.

Law enforcement in the cybercrime prevention framework reacts in much the same way as dealing with traditional crimes. Traditional crimes have a limited scope, scale, time, and place, so law enforcement can react quickly to them. Whereas cybercrime – as introduced by Brenner (2008) – has different characteristics from traditional crimes in several pages.

> First, though it is carried out by a small percentage of the population of a society (or of the world since cybercrime tends to ignore boundaries), a relatively small group can commit crimes on a scale far surpassing what they could achieve in the real-world where one-to-one victimization and serial crimes are the norms. Consequently, the number of cybercrimes will exponentially exceed real-world crimes. Second, cybercrime is additional to the real-world crime with which law enforcement must continue to deal; people will still rape, rob, and murder. These two factors combine to create an overload; law enforcement's ability to react to cybercrime erodes because the resources that were minimally adequate to deal with real-world crime alone are inadequate to deal with cybercrime and real-world crime in combination.

The crime control model or reactive model as it is known in criminal justice and carried out by the police is not effective enough to prevent cybercrime. Reactive strategies for cybercrime cannot be implemented properly because once the crime is committed, the perpetrator can easily remove the trail. After all, this crime takes place in an electronic environment, so physical evidence is easily lost from memory, or evidence can be easily destroyed. The police may be able to determine the location where the perpetrator accessed the internet after tracing the activity through log files, but when examined, the perpetrator may have left or even used anonymity where which is possible in cyberspace. In other words, the use of formal activities (affirmative model) is not suitable for dealing with cybercrime.

Likewise, with the due process model, it is not suitable to solve cybercrime completely. The typology of the due process model with the negative model always emphasizes restrictions on formal power and modification of the use of that power, where the dominant power in this model is judicial and always refers to the constitution. In Indonesian criminal justice, judicial power rests with the courts and is said to be the last wall of justice, even though cybercrime cannot be quickly prevented through a complicated court process. This model is suitable for legal certainty but is not suitable for

preventing crime, especially the types of crimes that have a high level of speed and mobility such as cybercrime.

A good prevention model that is worth trying is a combination of the various prevention models mentioned above based on internet users themselves (prevention based on user). This means that the focus to prevent cybercrime is no longer on the government, police, or judiciary, but on internet users. In a narrow sense, internet users must be equipped with knowledge about good ways of using the internet (guidance principle using the internet) or understanding cyber ethics or antiques. This step is referred to as prevention by defense by the user himself which tends to arise within him. In addition, users must also equip their internet infrastructure with a security system that should continue to be updated keeping in mind the speed of technological development. This model relies more on the user's sense of responsibility for himself and more broadly for the community to feel safe using the internet.

Another model is the model introduced by Brenner (2008), namely prevention law enforcement. This model gives the police or law enforcement officers the power to identify and incapacitate those who might commit crimes before they commit them. In other words, law enforcement has acted before the evidence is complete by intervening before the crime materializes. This allows law enforcement to intervene and incapacitate individuals based on predictions of their potential for crime. However, this model tends to rely on someone's indicators that appear on the surface, are too broad, and tend to ignore the guarantees of the legal process. If this is implemented, it will be dangerous because law enforcers can be suspected of having abused their power, and there will certainly be more pretrial law enforcement actions.

The problem of preventing cybercrime is not enough just by criminalization alone, or any other prevention model, especially with the nature of cybercrime that crosses national borders. Law enforcement will find it difficult to deal with it if it is related to the issue of different jurisdictions. Therefore, other efforts are needed so that prevention can be carried out effectively. The experience of several countries shows that cooperation between the government, law enforcement officers, NGOs/NGOs, and the community can reduce the number of cybercrimes (The Cybercrime Convention Committee (T-CY), 2006). This is what Sweden did, where NetClean Technology collaborated with the Swedish National Criminal Police Department and the NGO ECPAT in preventing pornography. Similarly, the Swedish and Norwegian National Police cooperate in updating the data on banned sites with the help of Swedish ISPs. In Denmark, ISPs, in collaboration with the National Police Department and the Danish NGO Save the Children, provide banned sites to block. In the UK, British Telecom is working with the Internet Watch Foundation (IWF) and the British Police to block forbidden websites (Raharjo, 2007b).

This thinking is in line with what was decided in the European Convention on Cybercrime. The European Convention advises countries (especially European countries, or other countries that see the importance of this convention) to do several things in preventing and combating cybercrime, that is: (1) harmonizing the domestic criminal

substantive law elements of offenses... in the area of cybercrime; (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offenses. . . [and] (3) setting up a fast and effective regime of international co-operation."

Based on this description, preventing cybercrime cannot be completely resolved with only one prevention model. As stated by Arief (1998), the use of criminal law in crime prevention is only a "*kurieren am symptom*", therefore criminal law is only a "symptomatic treatment", and not a "causative treatment". Therefore, the use of the models or a combination of the various models above can overcome the limitations of criminal law in tackling cybercrime.

Modification of Criminal Sanctions as an Incentive in Combating Cyber Crime

The last part of this article will discuss the need to modify criminal sanctions for cybercrime perpetrators. In philosophical studies, the philosophy of punishment has two functions, namely:

1. Fundamental functions, namely as the basis and normative principles or rules that provide guidelines, criteria, or paradigms for criminal and sentencing issues. This function is formally and intrinsically primary and is contained in every teaching of a philosophical system, because the arguments formulated in various schools of philosophy can undoubtedly be used by jurists and penologists as empirical research hypotheses on sentencing, and are useful in determining a sanction (criminal law).
2. The function of theory, in this case as a meta-theory. That is, the philosophy of punishment serves as a theory that underlies and underlies every theory of punishment.

In the implementation process, the determination of criminal sanctions and actions is an activity of legislation and/or judicial programs to norm the types and forms of sanctions (criminalization) as the basis for the validity of law enforcement through the application of sanctions (Sholehuddin, 2003; Priyatna, 2009).

By this philosophy of punishment, efforts to formulate the types of sanctions must also be adjusted to the thoughts about the actions that form the basis of the determination as criminal acts. Cybercrime, for example, is a criminal act based on the use of information technology or the internet. The philosophy of technology teaches that dependence on technology causes technology to be considered a god, an automatic machine that can bring people prosperity, happiness, peace, and so on. Therefore, the determination of the type of sanction that relies on this – technological determinism – will help in the accuracy of the type of sanction to be given to the perpetrators of the crime.

Giving punishment to criminals is not just suffering or sorrow for the perpetrators as introduced by the retributive theory with all its variations, or is an effort to protect the interests of the community as expressed by the relative theory, but more than that, punishment must be able to make a major contribution to the perpetrators. crime to realize his mistakes, change his behavior, and if necessary, become agents of change, or

can also develop awareness to realize as God's creatures who have dignity, a sense of solidarity, and the ability to control themselves.

Given this, it is necessary to state punishment in the perspective of Pancasila, where punishment must be oriented to the following principles (Sahetapy, 1982; Sholehuddin, 2003; Priyatna, 2009):

1. Recognition of humans (Indonesia) as creatures of God Almighty. The form of punishment must not conflict with any religious beliefs held by the Indonesian people. Punishment must be directed at the awareness of faith, becoming a man of faith and obedience. Punishment must function to develop the mentality of the convicted person and transform that person into a religious human being;
2. Recognition of the nobility of human dignity as God's creation. Sentencing must not injure his most basic human rights and must not degrade his dignity for any reason.
3. Growing national solidarity with others as fellow citizens of the nation. Perpetrators must be directed at efforts to increase tolerance with others, cultivate sensitivity to the interests of the nation, and direct them not to commit crimes again.
4. Growing maturity as a solemn citizen, able to control oneself, be disciplined, and respect and obey the law as a form of people's decisions.
5. Growing awareness of the obligations of each individual as a social being, who upholds justice together with others as fellow citizens.

Sentencing is not just matching the principles or objectives of sentencing, because the people and the community are the addressees of the punishment. Therefore, the purpose of punishment, according to Arief (2009), basically contains two main aspects, that is:

1. Aspects of community protection against criminal acts. This aspect includes the objectives:
   a. Crime prevention;
   b. Protection (preservation) of the community;
   c. Restoring the balance of society, in the form of conflict resolution (conflict oplossing) and bringing a sense of peace (*vredemaking*).
2. Aspects of protection/development of individual perpetrators of criminal acts (an aspect of criminal individualization). This aspect includes objectives:
   a. Rehabilitation, reeducation, resocialization (revive) the convicts such as:
      1) not to commit acts that damage/harm themselves and others/society;
      2) having the character (morals) of Pancasila
   b. Release the guilty;
   c. Protect the perpetrator from the imposition of arbitrary sanctions or inhumane retaliation (criminals are not intended to suffer and demean human dignity).

The punishment that must be oriented to Pancasila and other goals will only be seen in the implementation of the crime (the coaching process) and the output of the process. Although the criminal sanctions given are by the legislation – both type and severity – but if the process is not correct then the results obtained will certainly be far from expectations. Therefore, this final section does not discuss the process, but the need to

determine the type of criminal sanctions that have a technological dimension so that cybercrime actors who incidentally use technology can feel the effects or impacts of the reduced right to use technology.

If we look closely at the types of sanctions contained in Law no. 11/2008, it was found that there were 2 (two) types of criminal sanctions, namely imprisonment and fines with a cumulative alternative formulation. Various studies have shown that imprisonment has a bad effect on perpetrators, and many fines are unpaid. However, the legislators still formulate the type of criminal sanction as the prima donna. This type of sanction does not provide a deterrent at all to cybercriminals, especially with the guidance system in correctional institutions that still allows convicts – either openly or secretly – to bring information technology results, even though it is formally prohibited.

As introduced by the principle of criminal individualization, punishment must also look at the circumstances or conditions of the person being convicted, both inside and outside of him. Therefore, it is not true that all cybercrime perpetrators are subject to imprisonment and/or imprisonment only. The condition of cybercrime actors must also be seen. In this case, the cybercrime perpetrator will not be able to commit a crime if he does not use or access information technology, so it is necessary to formulate a form of sanction that can provide a deterrent effect or avoid recidivism in similar crimes by revoking the right to access information technology products or the internet for a certain period.

If it is synchronized with the types of sanctions in the sources of the Criminal Code (KUHP), then this type of sanctions cannot be included in the main types of criminal sanctions, but rather in additional criminal sanctions. The criminal sanction that prohibits accessing information technology or internet products applies both when he is still in prison or when he is free. For a certain period after being free, he may not access the internet with several expectations, namely:

1. For perpetrators who have an addiction to the internet, the prohibition on accessing the internet is already a pain in itself, which means that this prohibition is expected to cause deterrence for the perpetrator;
2. With the prohibition of being accessed, it is intended to mature the perpetrator himself, as well as learn to control himself so as not to disturb other people or tolerate what other people do, and further than that is not to use information technology or the internet as a weapon that makes people others suffer;
3. This type of sanction is by the principle of punishment, namely criminal individualization, where the punishment must be adjusted to the condition of the perpetrator. In general, cybercriminals are adherents of technological determinism, therefore the prohibition on accessing the internet is on the situation and condition of the perpetrators of the crime.

Indeed, the idea of this type of sanction is not yet popular in Indonesia, but in the future, lawmakers can see this sanction as the main choice in providing additional criminal sanctions to deter criminals. In the United States, these criminal sanctions are known as

electronic sanctions. The term was introduced by Reidenberg, where this sanction covers those who spread viruses, worms, and other types of malware, including hacking and Denial of Service Attacks. Furthermore, Reidenberg (2004) explained:

> "states could electronically sanction rule offenders by using technologies to penalize or destroy the offenders' online presence... [A] state might launch a 'denial of service or a 'distributed denial of service attack. This online death penalty prevents an offender from interacting on the Internet. A state may also use hacking techniques to `seize' or paralyze rule-violating web pages. ... [T]he state may use techniques similar to the MS Blaster worm for law enforcement purposes".

This thinking is not only based on the principle of criminal individualization, but also based on the principle of punishment in criminal law reform, especially as stated in the Criminal Code Bill which introduces the principle of the double track system, elasticity/flexibility of punishment, and modification/change/adjustment of criminal. As an idea and based on the practice of criminal law by judges who tend to just apply the law, it seems that this will only provide incentives for criminal law knowledge and ideas for lawmakers. Unless the judge dares to take advantage of the leniency or flexibility in choosing the type of sanction that is by the situation and condition of the perpetrator based on his constitutional duty to seek and find a law or even judge-made law. Included in this is the possibility for judges to modify the sentence according to changes in prisoners during the sentencing process.

Conclusion

Based on the description above, it can be concluded that cybercrime is a form of using the internet for illegal activities. The threat posed by this act is very disturbing, not only at the individual, group, or business entity level but even on a larger scale, namely national defense and security. The criminalization of cybercrime followed by the use of several models of prevention and control of cybercrime is expected to overcome this problem. However, in the formulation and application of criminal sanctions, it is necessary to consider based on philosophy or theory in technology, the idea of criminal individualization, flexibility in choosing criminal sanctions, criminal modifications, and of course the use of broad powers on judges to judge-made law can help the realization of an Indonesia that is free from cybercrime.

References

Arief, Barda Nawawi. (1998a). *Beberapa Aspek Kebijakan Penegakan dan Pengembangan Hukum Pidana.* Bandung: Citra Aditya Bakti;

-------. (2009b). *Tujuan dan Pedoman Pemidanaan, Perspektif Pembaharuan Hukum Pidana dan Perbandingan Beberapa Negara*. Semarang: BP UNDIP;

AS Tanggapi Serius Spionase Siber. *Kompas*, 22 February 2013.

Branscomb, Anne. (1983). Global Governance of Global Networks: A Survey of Transborder Data Flow in Transition. *Vand. L. Rev*. 36. 987-88.

Brenner, Susan W. (2008a). Distributed Security: Moving Away from Reactive Law Enforcement. *International Journal of Communication Law and Policy*, Special Issues Cybercrime Spring.

-------. (2001b). Is There Such a Thing as Virtual Crime?. 4 *CAL. CRIM. L. REV.* 4. 1-12, e-paper version at http://boalt.org/CCLR/v4/v4brenner.htm, accessed date 3 Maret 2007.

Feenberg, Andrew. (1991). *Critical Theory of Technology,* Oxford: Oxford University Press.

Grabosky, Peter N. (2001). Virtual Criminality: Old Wine in New Bottles. *Social & Leg. Studies* 10. 243.

Harnad, Steven. Post-Gutenberg Galaxy: The Fourth Revolution in the Means of Production of Knowledge. Public-Access Computer System Review 2(1): 39-53, e-paper version can be read in http://cogprints.org/1580/00/harnad91.postgutenberg.html, accessed date 23 August 2003.

Lipnack, Jessica & Jeffrey Stamps. (1994). *The Age of the Network, Organizing Principles for the 21st Century.* New York: John Wiley & Sons, Inc;

Nasibitt, John. Naisbitt, Nana. and Philips, Douglas. (2001). *High Tech, High Touch, Pencarian Makna di Tengah Perkembangan Pesat Teknologi.* Bandung: Mizan.

Priyatna, Dwidja. (2009). *Sistem Pelaksanaan Pidana Penjara di Indonesia*. Bandung: Refika Aditama.

Raharjo, Agus. (2007a). *Hukum dan Teknologi: Suatu Tinjauan Filosofis dan Kritik terhadap Positivisme Hukum*. Semarang: BP UNDIP.

-------. (2007b). Kajian Yuridis terhadap Cyberporn dan Upaya Pencegahan serta Penanggulangan Penyebarannya di Internet", *Jurnal Hukum Respublica*. 7(1).

Reidenberg, Joel R. (2004). States and Internet Enforcement. *U. Ottawa L. & Tech. J.* 1, 19.

Sahetapy, J.E. (1982). *Suatu Studi Khusus Mengenai Ancaman PIdana Mati Terhadap Pembunuhan Berencana*. Jakarta: Rajawali Press.

Sholehuddin, M. (2003). *Sistem Sanksi dalam Hukum Pidana, Ide Dasar Double Track System dan Implementasinya*. Jakarta: Rajawali Press.

Spion Siber Unit 61398. *Kompas*, 25 February 2001;

The Cybercrime Convention Committee (T-CY), *Strengthening Co-Operation, Between Law Enforcement and the Private Sector, Examples of How the Private Sector has Blocked Child Pornographic Sites*, Strasbourg, 20 February 2006, http://www.coe.int/t/e/legal_affairs/legal_co-operation/combatingeconomic_crime/6_cybercrime/t-cy/T-CY_2006_04-e-child.pdf., accessed date 28 Maret 2007;