CRIMINAL LAW POLICIES IN OVERCOMING CYBER CRIME IN INDONESIA

Syahranuddin, SH.,M.H,[1)] , Suci Ramadani, SH.,M.H. [2)]
[1)] Sosial Sains Faculty, University of Pembangunan Panca Budi
Email shsyahranuddin@gmail.com
[2)] Sosial Sains Faculty, University of Pembangunan Panca Budi
Email: suciramadanish@gmail.com

ABSTRACT

The globalization of information technology that has changed the world into the cyber era by means of the internet which presents cyberspace with its virtual reality offers humans various hopes and conveniences. However, behind that, a problem arises in the form of a crime called cyber crime, this crime knows no boundaries (borderless) and the time of occurrence because victims and perpetrators are often in different countries. Cyber crime can be carried out through the computer network system itself which is the target and the computer itself which is the means for committing crimes. The rapid development of information technology must be anticipated by the law that regulates it. These negative impacts must be anticipated and mitigated by laws related to the use of information and communication technology. Based on the background of these problems to conduct research on the Criminal Law Policy in Combating cyber crime in Indonesia. The purpose of this research is to find out the criminal law policy through the Criminal Code approach to tackling cyber crime in Indonesia and to know the criminal law policy through the ITE Law to tackle cyber crime in Indonesia and to know the enforcement of cyber crime law in Indonesia penal and non penal. This research is normative juridical in nature as the main approach, bearing in mind that the discussion is based on laws and legal principles that apply to the problem of cyber crime.

Keywords: Criminal Law Policy, Countermeasures, Cyber Crime.

1. INTRODUCTION

Criminal law policy is a policy from the state through authorized agencies to implement the desired regulations which are expected to be used to express what is contained in society and to achieve what is aspired to. Efforts and policies to make good criminal law regulations cannot be separated from the goal of crime prevention. So criminal law policy or politics is also part of criminal politics. Viewed from the perspective of criminal politics, the politics of criminal law is synonymous with the notion of "crime prevention policies with criminal law.

nformation technology is believed to bring great benefits to countries in the world. A new legal regime was born, known as cyber law, taken from the word Cyber Law, which is a legal term related to the use of information technology. Other terms used are Information Technology Law (Law Of Information Technology), Virtual World Law (Virtual World Law). These terms were born considering the activities of the internet and the benefits of virtual line information technology. The term cyber law is used in this paper based on the premise that if cyber is identified with "the World of Maya" it will be enough to face problems if it has to prove a problem that is assumed to be "virtual", something invisible and apparent.

Indonesia is trying to carry out harmonization policies with other countries, especially in the Asian and Asean environment regarding the issue of cyber crime. Anticipating the problem of cyber crime is not only through the Electronic Information and Transaction Law (UU ITE), but also trying to anticipate it in the drafting of the Criminal

Code Bill. In Book I of the Indonesian Criminal Code Bill in Article 174 in the General Provisions, it is stated about the meaning of "goods", which includes intangible objects in the form of data and computer programs, telephone services, telecommunications, or computer services. The text of Article 174 is as follows: "Goods are tangible objects including water and demand deposits, and intangible objects including electricity, gas, data and computer programs, telephone services, telecommunications services, or computer services." In Book I of the Indonesian Criminal Code Draft Article 188 also stated the meaning of "letter", including data written or stored on diskettes, magnetic tapes, computer storage media or other electronic data storage. In that article it is stated: "Letters are in addition to letters written on paper, also letters or data written on or stored on diskettes, magnetic tapes, or computer storage media or other electronic data storage media". The definition of "letter" describes the meaning of a letter in tangible (written) and intangible (virtual) terms. The meaning of an intangible letter can be in the form of email, massage in chat/guest book sites, written comments on a site in any form of application, short massage service (SMS) or Whatsaap (WA), including software. Based on these 2 (two) articles, it can be an illustration to see cyber crime from the point of view of the RUU KUHP. This is intended to prevent and reduce crimes that occur in cyberspace. In addition, so that the perpetrators of crimes related to technological advances can be snared by the law.

The main aspect of its activities, cyber crime is carried out with more focus on attacking other people's content, computer systems and communication systems, both personally and publicly in cyber space. For this reason, it is necessary to secure a system to prevent tampering. Countermeasures against cyber crime are carried out by preventing and enforcing the law, in order to achieve the supremacy of law. If allowed to continue, it can disrupt security both nationally and internationally. In fact, cyber crime has disrupted domestic and foreign security, so that strategic steps are needed by law enforcement officials to deal with it. Cyber crime occurs because personal control and social control are weak. This is because this crime is virtual, when the perpetrator is not physically visible. In the normative approach, there are cyber crimes which are conventional crimes but with new modes such as pornography, fraud, defamation and so on, which use internet media as a means to commit crimes, so they can be punished by looking at the Criminal Code (KUHP). Criminal Code), meanwhile for new types of cyber crime such as hacking, this crime has no provisions in the Criminal Code. Thus there is a legal vacuum (rechts vacuum).

2. PROBLEM FORMULATION

Based on the background of the problems described above, the authors identify the problems that will be the subject of discussion, namely:

a. How is the criminal law policy in dealing with cyber crime in Indonesia?

b. How is cyber crime law enforced in Indonesia through penal and non-penal means?

3. RESEARCH METHODS

The type of research used is normative juridical law research which analyzes problems based on applicable laws and also literature that discusses the problems reviewed. Approach through the Act, namely the approach taken by examining all laws and regulations that are related to the legal issue being studied.

4. LITERATURE REVIEW

a. Definition of Criminal Law Policy

The term policy comes from the English policy or the Dutch politie. In general, policies can be interpreted as general principles that function to direct the government in managing, regulating or resolving public affairs, community problems or the fields of drafting laws and regulations and applying laws/regulations, with a

goal that leads to . Efforts to protect society (social defense) and efforts to achieve social welfare (social welfare) are essentially an integral part of crime prevention policies or efforts. The definition of criminal law policy or politics can be seen from legal politics and criminal politics. According to Sudarto, "Legal Politics" is:

1. Efforts to realize good regulations in accordance with the circumstances and situation at a time
2. Policies from the state through authorized bodies to establish the desired regulations which are expected to be used to express what is contained in society and to achieve what is aspired to

Starting from this understanding, Sudarto further stated that carrying out "criminal law politics" means holding elections to achieve the best results of criminal legislation in the sense of fulfilling the requirements of justice and efficiency. On another occasion he stated that carrying out "criminal law politics" means, "efforts to realize criminal laws and regulations that are in accordance with the circumstances and situation at one time and for the future. Thus, seen as part of legal politics, the politics of criminal law implies, how to seek or make and formulate a good criminal legislation.

The background for the penal law reform can be viewed from sociopolitical, socio-philosophical, sociocultural aspects, or from various policy aspects, especially social policy, criminal policy, and law enforcement policy. That is, the renewal of criminal law in essence must be a manifestation of changes and updates to various aspects and policies that are the background to these reforms. Apart from that, a cultural/cultural approach, a moral/educational approach, and even a global approach through international cooperation are also needed. Penal policy operationalization includes criminalization, decriminalization, penalization and depenalization. Enforcement of criminal law is highly dependent on developments in legal politics, criminal politics, and social politics.

Therefore, law enforcement does not only pay attention to autonomous laws, but also pays attention to social problems and the science of social behavior. The criminalization policy is a policy in determining an act that was originally not a crime to become a crime. So in essence, the criminalization policy is part of the criminal policy (criminal policy) by using criminal law means so that it is part of the criminal law policy (penal policy), especially policy formulation.

b. Definition of Cyber Crime Control Policy

The cyber crime prevention policy with criminal law is included in the field of penal policy which is part of the criminal policy (crime prevention policy). From a criminal policy point of view, efforts to combat crime (including cybercrime) cannot be carried out solely in part with criminal law (means of penal), but must also be pursued with an integral/systemic approach as a form of high-tech crime that can go beyond national borders (transnational/transborder in nature), it is natural that efforts to tackle cyber crime must also be pursued with a technological approach (techno prevention). Apart from that, a cultural/cultural approach, a moral/educational approach, and even a global approach through international cooperation are also needed. Penal policy operationalization includes criminalization, decriminalization, penalization and depenalization. Enforcement of criminal law is highly dependent on developments in legal politics, criminal politics, and social politics. Therefore, law enforcement does not only pay attention to autonomous laws, but also pays attention to social problems and the science of social behavior. The criminalization policy is a policy in determining an act that was originally not a crime to become a crime. So in essence, the criminalization policy is part of the criminal policy by using criminal law means so that it is included as part of the penal policy, especially formulation policies.

c. Definition of Cyber Crime

The term cybercrime currently refers to an act of crime related to cyberspace (cyber space) and crime using a computer. There are experts who equate cyber crimes with

computer crimes, and there are experts who differentiate between the two. Some of the uses of the word to refer to cyber crime that are commonly used in various literature are cyber crimes, computer crimes, cyber crimes, crimes in the field of information technology, and many more. The legal concept of cyber space, cyber law, and cyber line which can create a community of 60 million internet network users, involving 160 countries has aroused the anger of legal practitioners to create security through regulations, especially protection of private property. Didik M. Arief Mansur and Elisatris Gultom in their book "cyber law legal aspects of information technology" state that in general what is meant by computer crime or crime in cyberspace is: "change and or damage to the computer facility that is entered or used".

5. DISCUSSION

a. Criminal Law Policy in Combating Cyber Crime in Indonesia.

Cases of cyber crime in Indonesia defacing, phishing, pornography, cases of defamation, hacking of state websites. Criminal law, namely part of the overall law that applies in a country, which establishes the principles and regulations to determine actions that may not be carried out, determine when and in what cases those who have violated these prohibitions can be subject to or be subject to punishment as stipulated threatened, determines how the imposition of the penalty can be carried out if there is a person who is suspected of having violated it. Criminal law policy through the Criminal Code approach to dealing with cyber crime in Indonesia still has legal overlap and is still not fully contained in the Criminal Code product, there are many analogies related to legal ensnarement of cyber crime suspects such as the carding case which is linked to the theft article, namely, article 368 Criminal Code. Crime is an entity that is always attached to the dynamics of the development of human civilization. The crime that Saparinah Sadli calls deviant behavior always exists and is inherent in every form of society; there is no society free from crime. Therefore, crime prevention efforts are actually continuous and continuous efforts.

The more advanced human civilization, as an implication of the development of science. knowledge and technology, various types of crimes with new dimensions emerged, which included cyber crime. In line with that, countermeasures are needed to ensure order in society. From a legal perspective, this effort is realized through criminal law. Criminal law is expected to be able to fulfill public order. It also occurs in the approach of the ITE Law which has not fully regulated various cybercrime crimes themselves so that they do not yet have a definite legal umbrella.

b. Cyber Crime Law Enforcement in Indonesia Through Penal and Non Penal Facilities

1. Cyber Crime Law Enforcement Through Penal Facilities.

The criminalization policy is a policy in determining an act that was originally not a crime (not criminalized) to become a criminal offense (an act that can be punished). So in essence, the criminalization policy is part of the criminal policy (criminal policy) by using the means of criminal law (penal), and therefore it is included as part of the "criminal law policy" (penal policy), especially the policy formulation. We can see the positive criminal law provisions related to cybercrime in Law Number 19 of 2016 amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions, as contained in Articles 27 to 36. There is also Law Number 20 of 2001 concerning Amendments to Law Number 31 of 1999 concerning the Eradication of Corruption Crimes, where the mayantara side of this criminal act of corruption is that the crime has used the internet media as a tool for committing corruption or facilitating criminal acts. the commission of the crime even though it is not explicitly regulated in this law. Penal law enforcement of cyber crime in Indonesia still refers to the system of the Criminal Procedure Code (KUHAP) absolutely.

2. Cyber Crime Law Enforcement Through Non Penal Means

Crime prevention policies through "non-penal" channels are more preventive in nature before a crime occurs. Therefore, the main objective is to deal with factors conducive to the occurrence of crime centered on social problems or conditions that can directly or indirectly give rise to or foster crime. Thus, seen from the crime prevention policy, these non-penal efforts have a strategic position and play a key role that must be intensified and made effective. Law enforcement with non-penal means, according to the author, this non-penal method is prioritized over penal means with the consequence of immediately preparing law enforcers who master information technology. Or more clearly, we really need cyber police, cyber prosecutors, cyber judges in the context of enforcing cyber crime law in Indonesia without law enforcers who are in the field of information technology, it will be difficult to catch cyber criminals because this cyber crime can cross locus delicti. country. Non penal is carried out through social methods or approaches such as information appeals, educational channels, coaching, and also related to cyber crime prevention.

6. CONCLUSION

1. Criminal law policy through the Criminal Code approach to tackling cyber crime in Indonesia still has legal overlap and is still not fully contained in the Criminal Code product, there are many analogies related to legal prosecution of cybercrime suspects such as carding cases which are linked to the theft article namely, Article 368 of the Criminal Code. It also occurs in the approach of the ITE Law which has not fully regulated various cybercrime crimes themselves so that they do not yet have a definite legal umbrella.
2. Penal law enforcement of cyber crime in Indonesia still refers to the system of the Criminal Procedure Code (KUHAP) absolutely. While on a non-penal basis it is carried out through social methods or approaches such as information appeals, educational channels, coaching, and also related to cyber crime prevention matters.

7. REFERENCE

Abdul Manan. 2013. *Aspek –Aspek Pengubah Hukum*. Jakarta: Kencana.

Abdul wahid dan Mohammad Labib. 2015. *Kejahatan Mayantara (Cyber Crime*). Jakarta: PT Refika Aditama.

Barda Nawawi Arief. 2016. P*embaharuan Hukum Pidana dalam Perspektif Kajian Perbandingan*. Jakarta: Prena Media Group.

Budi Suhariyanto. 2012. *Tindak Pidana Teknologi Informasi (Cybercrime*). Jakarta: Raja Grafindo Persada.

M. Ramli, Ahmad. 2006. *Cyber Law dan HAKI Dalam Sistem Hukum Indonesia*. Bandung: PT Refika Aditama.

Prasetyo, Teguh, dan Barkatullah, Abdul Halim. 2011. *Politik Hukum Pidana Kajian Kebijakan Kriminalisasi dan Dekriminalisasi*. Yogyakarta: Pustaka Pelajar.

Remy Syahdeini, Sutan. 2011. *Kejahatan & Tindak Pidana Komputer*. Jakarta : PT Pustaka Utama Grafiti.

Rukmini. 2014. *Aspek Hukum Pidana dan Kriminologi (Sebuah Bunga Rampai)*. Bandung: P.T. Alumni.

Sehatapy, J.E. 2004. *Pisau Analisis Kriminologi*. Bandung: PT Citra Aditya Bakti.

Hardianto Djanggih, ” Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana Cyber Crime Di Bidang Kesusilaan”. Jurnal Media Hukum. Vol. 1 No. 2, September 2013.

Kitab Undang-Undang Hukum Pidana (KUHP)

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik selanjutnya disebut Undang-Undang ITE

Undang-Undang Republik Indonesia Nomor 36 Tahun 1999 tentang Telekomunikasi