ISSN 1533-9211

DOI 10.5281/zenodo.7330689

LEGISLATIVE POLICY REFORMULATION IN COMBATING CYBERCRIMES

HUMUNTAL PANE[1], IRWANSYAH[2], ARFIN HAMID[3] and SYAMSUDDIN MUCHTAR[4]

[1, 2, 3, 4] Faculty of Law, Hasanuddin University, South Sulawesi, Indonesia. [1]E-mail: humuntal.pane@gmail.com

Abstract:

Internet technology-based activities are now no longer a new thing in the information society. The netters can quickly find out the development of technological research in various parts of the world. The phenomenon of criminal acts using information technology is a relatively new form of crime when compared to other forms of conventional crime. Internet penetration is so large if not used wisely it will causes criminal acts in cyberspace. Type of the study is a normative-legal research by using statute, case, and comparative approaches. It was conducted in the High Court of Manado, Regional Police of Metro Jaya, West Java, East Java and Manado District Court. This paper provides information on the latest trend in research. The results show that cybercrimes have reached a red warning that penetrated various aspects of people lives and also have an impact in many countries. The form of legislative policy reformulation as an effort to take criminal responsibility for cybercrimes in Indonesia and in the future requires restructuring in cybercrime prevention which is carried out in an integrated and not partial way with other regulations and also requires an integralistic approach. As a form of high tech crime, it is mandatory if cybercrime prevention efforts must be taken with a technological approach or techno prevention especially in defining phrases or terms that appear in cyber technology.

Keywords: Cybercrime; Cyberspace; Criminal Law; Legal Policy

1. INTRODUCTION

Nowadays, the world economy is experiencing many changes caused by the development of financial, production, investment and trade activities that have pushed the level of dependence between countries and causes competition and towards globalization (Halwani, 2006). One of the driving factors of globalization is information technology that allows humans to interact with each other without being limited by national boundaries, so that the world seems to be flat. Advances in information technology and electronic media are considered a pioneer symbol, which integrates the entire world system, both in socio-cultural, economic and financial. From small systems locally and nationally, the process of globalization is moving fast, even very quickly towards a global system.

Internet technology-based activities are now no longer a new thing in the information society (Broadhurst & Chang, 2013). Internet has even been used by preschoolers, parents, business people, agencies, employees and housewives. This interactive digital communication media is able to connect the information society quickly, easily and without being limited by regional boundaries (Hartono, 2006). Countries that control internet in the millennium era are certain to be developed countries if it is used wisely, especially in the fields of research, education, administration, socialization, networking and business.

The netters can quickly find out the development of technological research in various parts of the world. By simply managing a search engine like google, users around the world have easy internet access to various kinds of information. Compared to books and libraries, the internet symbolizes the spread (decentralization), knowledge of information and data extremely. The mechanism of library access (e-library) can be done using a special program with Z39.50 standard such as WAIS (Wide Area Information System), telnet application or through a web browser.

The phenomenon of criminal acts using information technology is a relatively new form of crime when compared to other forms of conventional crime (Rachbini, 2001). Internet penetration is so large if not used wisely it will causes criminal acts in cyberspace or what is termed cyber-crime as a further development of computer crime (Ajayi, 2016). This is understandable because the presence of computers that have gone global has led to the universalization of actions and the perceived consequences of these computer crimes.

In general, cyber crime consists of 2 (two) groups: First, ordinary crime that use technology information as a tool, and the second is a crime that emerged after the Internet, where the computer system as a victim. The types of crimes in this group are increasing along with the advancement of information technology itself. One example that is included in the second group of criminal acts is the destruction of internet sites, sending viruses or computer programs whose purpose is to damage the destination computer' work system. As a consequence, weaknesses in legislative policies will certainly affect the application and execution stages in implementing the cybercrime accountability system in Indonesia and for criminal acts that have an impact in Indonesia.

2. METHODOLOGY

This research is normative legal research that supported by empirical data (Irwansyah, 2021). The research uses a statutory, case, and comparative approaches. It was conducted in the High Court of Manado, Regional Police of Metro Jaya, West Java, East Java and Manado District Court. Determination of sample is done by using purposive sampling method.

3. RESULTS AND DISCUSSION

Legislation Policy Reformulation as an Effort for Criminal Accountability against Cybercrimes

The criminalization policy is a policy in determining an act that was originally not a crime (not punished) to become a criminal act (can be punished). In essence, the criminalization policy of information technology crimes is part of a criminal policy using the means of criminal law (penal), and therefore is part of the penal policy, especially its formulation policy (Arief, 2003).

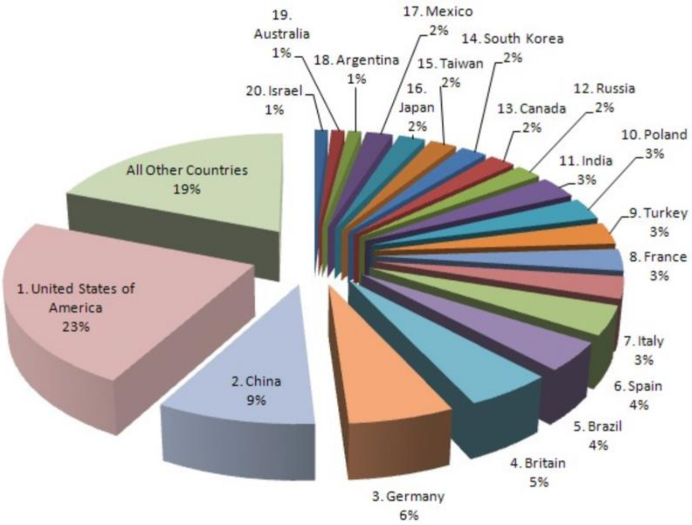
According to the Southeast Asian Freedom of Expression Network (SAFEnet), since the Law on Information and Electronic Transactions was enacted, from 2008 to 2019, there have been 271 case reports to the police. The existence of multiple interpretation articles in the Laen on Electronic Information and Transaction has caused a number of negative impacts. The first is

ISSN 1533-9211

DOI 10.5281/zenodo.7330689

limiting freedom of expression, especially in expressing opinions and giving criticism. This condition became a shock therapy for the community, some responded with caution while others chose not to express opinion (Clough, 2014). It certain hinders the development of democracy. Whereas the cyberspace culture that is developing today requires a more democratic society. The second, it creates arbitrariness because law enforcers in determining people who trapped on the Law on Information and Electronic Transactions are guilty and suitable to be punished, without choosing which article elements are violated. The third is an instrument for some groups in order to take revenge and even become a weapon to trap political opponents. The fourth is less guarantee of legal certainty. Decisions related to multiple interpretations articles are varied and even contradictory. In chart form, the cybercrime can be described as follows:

Chart 1: Top 20 Cybercrime several countries in the world



Source: Secondary data, 2022 (edited)

Based on the graph above, it can be seen that cybercrime is not only in Indonesia but also in various countries in the world. Construction of law enforcement on the responsibility of cybercrime in Indonesia in our national legal system there are still legal gaps in determining the criminal responsibility of the perpetrators and fulfilling the elements of punishment for the perpetrators, resulting in legal bias which leads to a legal vacuum or loopholes becomes a real obstacle in the context of norms (substance) and mechanisms (law enforcement procedures).

The unclear formulation of the concept in the Law on Electronic Information and Transaction raises the question, on what basis was the cyber law built? So as to give the impression that the legislators in formulating the Law on Information and Electronic Transaction seem to stand alone, without any conceptual connection with existing laws. Whereas in scope, cyber law is formed from several laws that are directly related, such as the Law on Public Information Disclosure, the Law on Archives, the Law on Company Document and other laws as part of the cyber law. Based on the concepts defined by the legislators, it is clear that several definitions of prohibited acts are not included in the Lawn on Electronic Information and Transactions. Regarding terminology in the field of information and electronic transactions law, it is also one of the key factors for understanding the normative provisions of the Law on Information and Electronic Transaction. Some terminology that will be explained in this section includes digital evidence terminology, social media terminology, hardware terminology, software terminology, and terminology in the Law on Information and Electronic Transactions which is interpreted as stated in the decision on the case of defamation and fake news.

The formulation stage is most strategic stage in efforts to prevent and overcome or eradicate criminal acts. Explained further by Arief, that in this formulation stage there is a stage where criminal legislation is made or formulated. By making or formulating the legislation, it has been determined what actions are prohibited acts or what actions are permitted by criminal law. This means, at the stage of formulation of laws and regulations, there has been a criminalization process that regulates both the scope of actions that are against the law, criminal liability that can be requested, even criminal sanctions that can be imposed, which in this case can be in the form of crime or action. In relation to the regulation regarding criminal liability for cybercrimes, at this formulation stage it will be determined what form of criminal liability arrangements for cybercrimes are appropriate to be carried out.

This new reality is in fact formed through a computer network that connects between countries or between continents based on the transmission control protocol/internet protocol. This means, in its working system, it can be said that cyber space (internet) has changed distance and time to be unlimited. The internet is described as a collection of computer networks consisting of a number of smaller networks that have different network systems (Hunton, 2011).

Cybercrime is also called a telematics crime (convergence). This is based on the argument that cybercrime is an activity that uses a computer as a medium supported by a telecommunications system, be it a dial-up system, using a telephone line or wireless system that uses a special wireless antenna (Judhariksawan, 2005). The convergence between computers and telecommunications systems as above is called telematics. So when mentioning a telematics crime, then what is meant is also a cybercrime. However, on the other hand, some experts argues that both computer crimes, cybercrimes and telematics crimes is same crime with a different name. The argument behind it is that although initially the computer was only a means of collecting and storing data that could be used to commit conventional crimes, but in its development computer crimes have also been carried out on an internet basis such as Trojan horse, hacking and data leakage.

Controversy of term as described above does not have to be “stuck” in the debate over which terms will be used. Therefore, for reasons of consistency, the author chooses to use cybercrime as a description of telematics crimes. Of the 19 (nineteen) types of cybercrimes, from the author’s interview with the Adjunct Police Commissioner Roberto GM Pasaribu who is the Director of the Special Criminal Investigation Department of the Regional Police of Yogyakarta, who previously as Head of the Cybercrime Sub-Directorate of the Police Special

Criminal Investigation Directorate Metro Jakarta Raya and Deputy Director of Special Criminal Investigation of Metro Jakarta Rata, there are a total of 12 (twelve) types of cybercrimes which is often carried out based on statistical data from the Directorate of Cybercrime in period January 2016 to September 2021 as Table 1.

Table 1: Cybercrimes report by public to the Police

No.	Types of Cybercrime	Number of Cases
1.	Online Scam	7.047
2.	Share Provocative Content	6745
3.	Pornography	1.173
4.	Illegal Access	949
5.	Gambling	152
6.	Extortion	226
7.	Data/Identity Theft	337
8.	Electronic System Hack	244
9.	Illegal Interception	57
10.	Site Appearance Change	65
11.	System Crash	98
12.	Data Manipulation	331
	Total Report	**17,424**

Source: Secondary data, 2022 (edited)

The results show that cybercrimes in the period 2016 to 2021 were recorded as fraud crime through online networks which ranked the highest from reports submitted to the Patrolisiber. It means that public awareness of the dangers of fraud through online networks is still quite low. In relation with the tendency of increasing cybercrime through online networks, it is necessary to make efforts from the Government and related institutions to socialize other forms of cybercrime to the public through various efforts through existing media, either through television, radio or organizing seminars, training and so on (Maskun et al, 2020).

Furthermore, cybercrime in the form of provocative content in second rank, there was a significant increase during the presidential and regional head election process. Sharing content at that time was dominated by groups of supporters of each candidate in order to create a negative image of political opponents from their supporters with the aim of increasing vote acquisition. The third highest ranking is pornography. Pornography by Indonesians and Westerners are quite disturbing to Indonesians (especially parents) due to the ease with which everyone can access channels that provide pornography consumption. Of the 19 (nineteen) types of cybercrimes as described above, Kepala Badan Siber Sandi Negara or BSSN said that the financial sector was sector that needed attention which experienced cyber-attacks after the government sector. This is certainly a serious threat to the security of transactions and customer data.

An independent and sovereign country obtains full recognition and sovereignty to make regulations or legislation that regulates efforts to overcome cybercrime crimes, one of which is by regulating the criminal liability system for cybercrimes. The preparation of a law or the formulation stage or the legislative stage, especially those relating to the criminal responsibility system for cybercrimes as discussed in the writing of this dissertation is part of an effort to enforce concepts that contain the values of legal certainty, justice and expediency. In other words, it can be said that the reformulation of legislative policies regarding the criminal responsibility system for cybercrimes in positive law in Indonesia must be directed to guarantee the values of legal certainty (because in the context of the rule of law there is the value of the rule of law) but still guarantee the values of justice. society and the benefits of the law concerned. Related to this, Satjipto Rahardjo stated that in essence law contains ideas or concepts that can be classified as abstract, including ideas about justice, certainty and social benefits, when we talk about law enforcement we are essentially talking about the enforcement of ideas and concepts which are abstract.

Through the establishment of criminal legislation, it will continue at the application stage, namely the application of criminal legislation that has been made by the judge. In other words, the criminal legislation that has been made by the legislature will be applied by the judge in a case and will be followed up with the execution stage. Thus, the formulation stage is the beginning or the core of law enforcement efforts, specifically the prevention of crime. Furthermore, if the legislation policy or the stage of drafting the law can form a law that guarantees legal certainty, justice and benefit, it is hoped that the application or application of the law that has been formed can also be carried out with certainty, justice and benefit the community.

4. IMPLICATIONS AND RECOMMENDATIONS

In Indonesia, cybercrimes have reached a red warning that penetrated various aspects of people lives and also have an impact in many countries. The role of legislative policy in criminal liability for cybercrimes in Indonesia, although laws and regulations have been issued that regulate and seek to minimize cybercrimes, but cybercrimes by using sophistication of information technology have not been able to be anticipated, this is due to because there are still blur articles that can lead to multiple interpretations. The form of legislative policy reformulation as an effort to take criminal responsibility for cybercrimes in Indonesia and in the future requires restructuring in cybercrime prevention which is carried out in an integrated and not partial way with other regulations and also requires an integralistic approach. As a form of high tech crime, it is mandatory if cybercrime prevention efforts must be taken with a technological approach or techno prevention especially in defining phrases or terms that appear in cyber technology.

ACKNOWLEDGMENTS

The authors acknowledge all contributors involved in this study. The authors declare no conflict of interest and no research funds or grants received.

DECLARATION OF INTEREST

Authors declare there are no competing interests in this research and publication.

ISSN 1533-9211

DOI 10.5281/zenodo.7330689

References

1. Ajayi, Emmanuel Femi Gbenga. "Challenges to enforcement of cyber-crimes laws and policy." Journal of Internet and Information Systems 6, no. 1 (2016): 1-12.
2. Amarullah, Abdul Hanief, Arthur Josias Simon Runturambi, and Bondan Widiawan. "Analyzing cybercrimes during Covid-19 time in Indonesia." In 2021 3rd International Conference on Computer Communication and the Internet (ICCCI), 78-83. IEEE, 2021.
3. Amin, M. Erham, and Mokhamad Khoirul Huda. "Harmonization of Cyber Crime laws with the Constitutional Law in Indonesia." International Journal of Cyber Criminology15, no. 1 (2021): 79-94.
4. Arief, Barda Nawawi. Kapita Selekta Hukum Pidana. Bandung: PT. Citra Aditya Bakti, 2003.
5. Broadhurst, Roderic, and Lennon YC Chang. "Cybercrime in Asia: trends and challenges." Handbook of Asian criminology(2013): 49-63.
6. Clough, Jonathan. "A world of difference: the Budapest convention on cybercrime and the challenges of harmonisation." Monash University Law Review 40, no. 3 (2014): 698-736.
7. Halwani, Hendra. Ekonomi Internasional & Globalisasi Ekonomi, Jakarta: Ghalia, 2002.
8. Hartono, Sunaryati. Bhineka Tunggal Ika Sebagai Asas Hukum Bagi Pembangunan Hukum Nasional. Bandung: PT. Citra Aditya, 2006.
9. Hirst, Paul and Grahame Thompson. Globalisasi adalah Mitos, Jakarta: Yayasan Obor, 2001.
10. Hunton, Paul. "The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation." Computer Law & Security Review27, no. 1 (2011): 61-67.
11. Irwansyah. Penelitian Hukum; Pilihan Metode dan Praktik Penulisan Artikel. Yogyakarta: Mirra Buana Media, 2021.
12. Ismail, Nurwita, Aminuddin Ilmar, M. Djafar Saidi, and Muh Hasrul. "Simplification of the Bureaucracy through the Merit System." Review of International Geographical Education Online 11, no. 9 (2021).
13. Judhariksawan. Pengantar Hukum Telekomunikasi. Jakarta: Rajawali Press, 2005.
14. Koto, Ismail. "Cyber Crime According to the ITE Law." International Journal Reglement & Society (IJRS) 2, no. 2 (2021): 103-110.
15. Maskun, Achmad, Naswar, Assidiq, Hasbi., Syafira, Armelia., Napang, Marthen., and Hendrapati, Marcel. "Qualifying Cyber Crime as a Crime of Aggression in International Law." Journal of East Asia & Int'l L. 13 (2020): 397.
16. Saragih, Yasmirah Mandasari, and Andysah Putera Utama Siahaan. "Cyber Crime Prevention Strategy in Indonesia." SSRG Int. J. Humanit. Soc. Sci 3, no. 6 (2016): 22-26.