IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# LEGAL POLICY IN HANDLING CYBER CRIME FOR CREATING PERSONAL DATA SECURITY

[1] Dona Raisa Monica, [2] Rodhi Agung Saputra,

[1-2] Lecturers & Students of the Faculty of Law, University of Lampung Indonesia

[1-2] Faculty of Law, University of Lampung, Bandar Lampung, Indonesia

***Abstract:*** The purpose of this study is to find out and understand the Cyber Crime Countermeasures Policy to Realize Personal Data Security. The existence of Internet media that is so large and easy if not used wisely will give birth to crime in cyberspace or known as cyber crime. The problem that will be discussed in this research is how the Cyber Crime Countermeasures Policy Realizes Personal Data Security. The research method used is a normative research method with a statute approach and analyzed using content analysis. The findings of this study are that the number of cyber attacks that haunt the public and the government is very high and requires immediate anticipation. This is because the development of technology that is increasing demands the role of the government to carry out reforms to deal with cyber crime problems. Therefore, this problem can be done with the politics of criminal law in the scope of penal policy and non-penal policy.

***Index Terms*** **- Legal Policy, Cyber Crime, Personal Data**

## I. INTRODUCTION

Cyber crime is a criminal act that utilizes computer technology and internet networks as its target. Cyber crime itself appears along with the incessant digital technology, information and communication that is growing. Coupled with the Covid-19 pandemic, cyber criminals or take advantage of the situation and launch their actions and reap the coffers of profits that can be considered illegal. These criminals are targeting companies whose workers are required to work from home due to the pandemic by exploiting network security vulnerabilities. Types of cybercrime carried out by cyber criminals, including:

a) Data theft is a form of illegal action by stealing data from someone through a computer system or internet network for personal gain or being marketed by selling stolen data.
b) Hacking and Cracking can be interpreted as the act of forcibly breaking through programs contained in computers belonging to other parties. A Hacker should not have a bad effect, because in some cases there are hacking actions that have a positive effect. However, hacking abilities are often misused by hackers for personal gain that harms others.
c) Dissemination of Illegal Content is an act of spreading content that contains information or data that is not necessarily true, unethical and violates the law.
d) Carding or better known as credit card abuse is a shopping activity but uses the number and identity of a credit card owned by someone else.

The increasing number of cyber crimes, we as a society must be more careful in accessing the internet, especially in terms of shopping and also sharing our personal information in any place. For example, one of the latest and most shocking acts of hackers is the case of data theft of 15 million Tokopedia account information which was reported to have been hacked. Some observers even say that a total of 91 million accounts of the online store giant have been sold on the dark web for US$ 5,000. The extent to which this information is correct is still being investigated by the authorities. Not a few people are victims of fraud, and the actions of cyber criminals who take advantage of public ignorance about how to protect the personal identity of information technology users. Personal identities that should only be known by banking institutions, are

unknowingly given to unknown foreign parties. Thus, they are vulnerable to being exploited by irresponsible parties to access their financial condition.

In this case, there are three approaches to maintaining security in cyberspace, the first is a technological approach, the second is a socio-cultural-ethical approach, and the third is a legal approach. To overcome the security of interference, the technological approach is absolutely necessary, because without a network security it will be very easy to be infiltrated, or accessed illegally and without rights. Seeing the legal facts as they exist at this time, the impact of the development of science and technology that has been misused as a means of crime is very important to anticipate how the legal policy will be, so that cyber crime that occurs can be overcome with criminal law, including in this case is about the proof system. It is said to be very important because in criminal law enforcement the basic justification for a person can be said to be guilty or not committing a crime, in addition to his actions can be blamed on the strength of the existing law (legality principle), also which actions are supported by the strength of valid evidence and to him. can be accounted for (element of error). Apart from that, a very important issue to discuss is what if the perpetrators of this cyber crime are minors, then preventive measures need to be put forward in carrying out law enforcement.

The rapid development of technology requires legal arrangements relating to the use of this technology. There are many cases that prove that legal instruments in the IT sector are still weak, this can be seen from the juridical and non-juridical constraints. The juridical obstacle is that electronic documents have not been explicitly acknowledged as evidence by the Criminal Procedure Code and in court regulations. The difficulty in detecting these crimes is caused by the lack of adequate equipment, the reluctance of some victims to report to the police, the security system of the asset owner/system which is relatively weak, and it is difficult to trace the whereabouts/domicile of the perpetrators of the crime. Until now, in our country, it turns out that there is no article that can be used to ensnare cyber criminals. For the carding case, for example, the police can only ensnare the perpetrators of computer crimes under Article 363 of the Criminal Code regarding theft because what the suspect did was steal other people's credit card data.

Apart from that, regulations related to personal data protection are also strengthened by the issuance of the Law on Personal Data Protection which aims to overcome the problems that have recently occurred, namely many cases of the central government system and state officials being hacked. The protection of personal data will be very closely related to the concept of privacy. Every individual has a right to privacy, so they have the right to determine who can hold information about them and how that information will be used. Once this law is passed, it will take a lot of Data Protection Officers to assist consumers in protecting their personal data. This is the background why it is necessary to pursue a role or action from the government, both preventively and repressively in dealing with the problems of cyber crime, which are increasing in number, otherwise people will feel less safe and comfortable. Based on the description of the background above, the problem in this research is how the Cyber Crime Countermeasures Policy Realizes Personal Data Security.

## II. RESEARCH METHODOLOGY

The research method used is a normative research method. By using a statute approach related to the Cyber Crime Countermeasures Policy to Achieve Personal Data Security. The statute approach is to examine matters relating to legal principles, legal views and doctrines, and laws and regulations related to the environment, and data that is accurate and can be accounted for for truth related to the Policy for Overcoming the Increase of Cyber Crime Realizing Personal Data Security. In addition, an in-depth examination of the legal facts is also held to then seek solutions to the problems that arise in the symptoms in question.

## III. RESULTS AND DISCUSSION

Technological developments in Indonesia. In line with the development process and the era of globalization, as well as the increasing quality of technology, Indonesian society has undergone many changes as a result of the progress of science and technology today. People's thinking has also been influenced by various things. These impacts can be in the form of positive impacts or negative impacts. The positive impact makes it easy for the community to complete their activities, while the negative impact can be in the form of a decline in public morals, with the unlimited entry of foreign cultures through online media, the rise of pornography which causes sexual harassment, online gambling, cyber crime, and recently. This is rife is the practice of online prostitution business through social networks or other sites. In addition, there are also negative impacts that arise with the internet. The internet can also be used for negative things and harm others, such as credit card theft, piracy or website destruction. The enactment of Law Number 11 of 2008 concerning Electronic Information and Transactions is intended to provide many benefits, including to ensure legal certainty for people who conduct electronic transactions, encourage economic growth, prevent information technology-based crimes and protect service users by utilize information technology.

In Indonesia, cyber crime is actually not a new crime. Cyber crime is a term that refers to criminal activity using a computer or computer network as a tool, or as a target, as well as the location of the crime. Ideally speaking, of course it should not be and it is not easy for people to become victims of cybercriminals. But in Indonesia, guarantees and efforts to protect the public from becoming victims of the abuse of cybercriminals are often not easy. A number of factors that make it easy for hackers and cybercriminals to carry out their actions, namely, first, when people are facing anxiety and are hit by excessive fear due to news about the dangers of Covid-19 that continues to bombard cyberspace and social media. Many cases prove that people are victims of fraudulent practices by cybercriminals who take advantage of the moment when the demand for medical devices such as masks and hand sanitizers spiked sharply. People who try to buy masks or hand sanitizers through sales sites in cyberspace, often become victims of irresponsible people.

Some people who have already bought goods via online and have transferred a certain amount of money, it turns out that they get unwanted goods. In fact, the goods they ordered were never delivered. Second, due to public ignorance about the importance of maintaining the confidentiality of their accounts and personal identities, some people have become victims of fraud by cyber criminals. Fraudulent e-mails, SMS, messages on social media asking for item ordering codes, credit card numbers, PIN numbers, etc., are often answered innocently without further verification. Yet it is very risky. People who live in the era of a cashless society, some are not aware of the risks and dangers of conducting online transactions, but are often trapped in the lure of prizes. Self-awareness and various other fraudulent practices are developed by cybercriminals. Whatever the situation, the public should be aware and aware of the social engineering and phishing that cybercriminals usually develop to deceive their prey. People who live or work at home, and rely more on information from online sources, such as e-mail and chat, are usually more likely to be exploited by hackers to steal important data and information by phishing methods. Fraudsters are toying with the psychological rift of society with something that seems urgent.

### A. Legal Policy In Handling Cyber Crime For Creating Personal Data Security

The threat of cyber crime in Indonesia is a crime in the era of digital society which is increasingly worrying. In the 2013 State of The Internet report, for example, Indonesia was mentioned as the second country in cyber crime cases in the world. The number of cyber crime in Indonesia that year was reported to have reached 36.6 million attacks. During the Covid-19 outbreak, it is certain that the number of cyber attacks that haunt the community will spike sharply and require immediate anticipation. More than just protection and preventive measures that rely on the work of the National Cyber Agency, efforts to protect the public from becoming victims of cyber crime of course also depend on the ability and information literacy of the community itself. Train the public's sensitivity and critical attitude so as not to open e-mails and links that are suspicious or come from untrusted sources. Always be aware of any attached electronic files. Because, it could contain harmful content, namely things that should automatically be done by people who are aware and have adequate information literacy. In the midst of the information boom and increasing public anxiety about the dangers of Covid-19, we should not be trapped and become victims for the second time due to the actions of cyber criminals. Get used to only opening official sites to get updates on the latest conditions of Covid-19, in order to avoid malware infections, and not become a victim of cyber crime.

In the midst of the outbreak of the Covid-19 pandemic, various countries are faced with increasing cyber crimes and targeting groups related to Covid-19. In this all-digital society, one of the ways to get acquainted is through the internet. However, this thirst for information about the Corona virus is also used by cyber criminals or cybercriminals to launch their attacks and reap profits which are certainly illegal. Without heeding ethics, cybercriminals are targeting billions of people who are wary and play an important role in responding to the pandemic such as governments, and other relevant institutions such as hospitals. They also attacked companies whose workers were required to work from home due to the pandemic by exploiting network security vulnerabilities. Phenomena like this are no longer new in the cyber world. The mention of hot events has repeatedly been used as bait in the social engineering of cyber criminals. In response to this, the problems that arise in relation to cyber crime are how to eradicate or enforce the law. The rapid development of technology requires legal arrangements relating to the use of such technology. Unfortunately, until now many countries (including Indonesia) do not have specific legislation in the field of information technology, both in criminal and civil aspects. The lagging legislation in adapting to advances in information technology requires a temporary solution to overcome cybercrime, namely through a breakthrough in court decisions. This of course requires a judge who is creative, technologically savvy, and dares to make a breakthrough through his decision. Many cases prove that legal instruments in the IT sector are still weak. For example, the Criminal Procedure Code has not explicitly acknowledged electronic documents as evidence. This can be seen in Law No. 8/1991 Article 184 paragraph 1 that this Law

definitively limits the evidence to only witness testimony, expert testimony, letters, instructions, and statements of the defendant.

Furthermore, in addition to legal instruments, special institutions, both government-owned and non-governmental organizations (NGOs), are needed as an effort to overcome crime on the internet. For example, the United States has the Computer Crime and Intellectual Property Section (CCIPS) as a special division of the U.S. Department of Justice. This institution provides information about cybercrime, conducts intensive socialization to the public, and conducts special researches in the prevention of cyber crime. There is also the National Infrastructure Protection Center (NIPC) as an institution in the United States that handles issues related to infrastructure. This institution identifies parts of infrastructure that are critical for the country (especially for the United States of America). Internet or computer network has been considered as an infrastructure that needs special attention. This institution also provides advisory for everyone who needs a solution for crimes in the computer field. Problems related to cyber crime if there is no proper supervision or law enforcement, in any case, this crime will continue to increase.

**B. The Urgency of Legal Policy and Legal Reform in Overcoming Cyber Crime Problems**

Traditional crimes are now transformed into crimes in cyberspace (cyber crime) using the internet and other electronic tools. The internet provides opportunities for criminals in cyberspace to commit crimes more neatly, hidden, organized and able to penetrate space and time with a very wide reach. As a form of globalization of crime, cyber crime can be carried out by involving several perpetrators who are in several jurisdictions of different countries with target victims who are in other countries as well. Crimes committed in cyberspace generally aim to generate financial gain for the perpetrators. Various actions are taken to attack security systems in cyberspace to get money. There are also perpetrators who use the internet as a medium to make money, for example using the internet for the illicit trade in weapons and organs, prostitution and pornography. In its development, criminals use the internet as a means to attack someone personally without directly or not aiming for financial gain, for example, defamation through the internet, political hacking, cyber terrorism, cyber bullying and so on.

Indonesia has come under greater scrutiny from cybercrime authorities in recent years, especially since a 2013 survey by Akamai Technologies, an IT security company, reported that Indonesia had overtaken China as the world's largest source of hacking traffic (translation by researcher). The data does not merely mean that the perpetrators are from Indonesia, but until now problems related to cyber crime continue to increase, plus with the Covid-19, all activities must be carried out at home using electronic media, this requires the government to strengthening regulations to deal with cyber crime problems. Furthermore, the problems related to cyber crime are related to:

1) The characteristics of cybercrime shows that these crimes can cross state jurisdictions, while the existence of international agreements regarding law enforcement against cybercrime is still very limited.
2) Penal policies in overcoming cyber crime have not been balanced with non-penal policies such as policies in the work environment, policies in applications, policies in schools and so on.
3) Law enforcers have to deal with billions of netizens (internet users) with various kinds of internet behavior. Inadequate law enforcement resources are a challenge in tackling cyber crime

Therefore, there is a need for synergy between the government and the private sector as well as other countries in dealing with cyber crime so that the number does not continue to increase, especially during the Covid-19 pandemic. This is related to the prevention of cyber crime, which must be prioritized on legal reform because it is an urgent matter or can be called the urgency of legal reform related to cyber crime which can be done with criminal law politics to deal with this problem. Criminal policy is used as an alternative in solving social policies. Overcoming social problems is carried out by law enforcement which is a response to crimes committed by the community. As a response to crime, the criminal policy has limitations in tackling such a broad and complex crime, therefore crime prevention is carried out by means of a penal (the use of criminal law) and balanced with non-penal means. Cyber crime is one of the products of the globalization of crime, where crimes are committed without being limited to space and time. Muladi and Diah Sulistyani R.S. explained that the acceleration of modern transportation, communication and information gave birth to the globalization of technology that had an effect on the globalization of crime. Furthermore, it is said that criminal law policies (criminal policy) that can be carried out in overcoming this are warmaking criminology or harm creating on crime that is hostile (adversarialism) as a repressive approach and combined with a preventive approach of mutualism or togetherness on the basis of peacemaking criminology. In tackling cyber crime, comprehensive efforts are needed both through criminal law and through criminal law channels. Crime prevention and control is carried out with an integral approach between penal policies and non-penal policies. The penal policy has several limitations and weaknesses, namely it is pragmatic, individualistic (offender oriented), more repressive and must be supported by

infrastructure that requires high costs. Thus, crime prevention is better done by using non-penal policies that are preventive in nature. Policies in overcoming cyber crime can be carried out in two ways, namely:

1. **Penalty Policy**

The penal policy is a policy related to the use of criminal sanctions in the settlement of criminal cases in cyberspace. This is related to cyber crime law enforcement. Law enforcement is carried out to fulfill the value of justice, especially for victims. The value of justice occupies a vital and essential element in the formation, application and enforcement of the law. The value of justice is an absolute requirement in the life of society, nation and state in accordance with the ideals of Pancasila law. The government hereby issues laws for the protection of personal data.

2. **Non Penalty Policy**

Non-penal policies that can be implemented are as follows:

a) Develop policies outside of criminal law that support efforts to prevent cybercrime, such as through anti-hate policies, anti-bullying policies and healthy internet policies through the education system;
b) Conducting socialization of potential crimes in cyberspace by educating the internet user community not to include personal identities, transact in places with safe internet facilities and so on;
c) Build cooperation with the private sector to build a security system in cyberspace;
d) Establish an institutional network in preventing cyber crime both at the national and international levels. International cooperation in overcoming cyber crime is very necessary considering that cyber crime is an organized transnational crime.

As a developing country, Indonesia must be swift in adapting to legal developments and strategies for dealing with cybercrimes. Legal politics in tackling cyber crime is carried out by formulating a global strategy in preventing and enforcing laws against crimes in cyberspace, compiling responsive legal formulations and preparing institutions that can take quick action when problems occur in cyberspace. Legal reform is an effort to further improve and improve legal guidance related to cyber crime. This effort is carried out by conducting renewal of the codification and unification of law, in its implementation it must pay attention to the legal awareness that develops in the community. It is more emphasized on the conditions that continue to develop, the law will continue to follow the times. In this case the development of the times in the field of technology that can lead to criminal acts, therefore it is necessary to organize and form laws that are more responsive in dealing with cyber crime problems.

## IV. CONCLUSION

Based on the results of research related to Cyber Crime Countermeasures Policies for Realizing Personal Data Security, it can be concluded that cyber crimes or cyber crimes occur a lot, especially those who are in an uproar at this time are government officials who are attacked by spreading their personal data. In tackling cyber crime, comprehensive efforts are needed both through criminal law and through criminal law channels. Crime prevention and control is carried out with an integral approach between penal policies and non-penal policies. The penal policy has several limitations and weaknesses, namely it is pragmatic, individualistic (offender oriented), more repressive and must be supported by infrastructure that requires high costs. Thus, crime prevention is better done by using non-penal policies that are preventive in nature.

## REFERENCES

[1] Abdulkadir Muhammad, Law and Legal research, Bandung: Citra Aditya Bakti, 2004, 32
[2] Akub, M. Shukri. "Regulation of the Mayantara Crime (Cyber Crime) in the Indonesian Legal System." Al-Ishlah: Scientific Journal of Law 21.2 (2018): 85-93.
[3] Barda Nawawi Arief, 2005, Criminal Law Reform; In the Perspective of Comparative Studies, Citra Aditya Bakti, Bandung, 102.
[4] Barda Nawawi Arief, 2006, Mayantara Crime and the Development of Cybercrime Studies in Indonesia, Jakarta: Rajawali Pers, page 25.
[5] Buil-Gil, David, et al. "Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK." European Societies 23.sup1 (2021): 47-59.
[6] Flowers, Goddess. "Politics of criminal law against cybercrime countermeasures." Indonesian Legislation Journal 16.1 (2019): 1-15.
[7] Collier, Ben, et al. "The implications of the covid-19 pandemic for cybercrime policing in scotland: a rapid review of the evidence and future considerations." Scottish Institute for Policing Research (2020).
[8] Fontanilla, Marites V. "Cybercrime pandemic." Eubios Journal of Asian and International Bioethics 30.4 (2020): 161-165.
[9] Hafidz, Jawade. "Juridical Studies in Anticipating Cyber Crime." Journal of Legal Reform 1.1 (2014): 32-40.

[10] Hawdon, James, Katalin Parti, and Thomas E. Dearden. "Cybercrime in America amid covid-19: The initial results from a natural experiment." American Journal of Criminal Justice 45.4 (2020): 546-562.
[11] Herdiana, Yudi, Zen Munawar, and Novianti Indah Putri. "Cyber Security Risk Threat Mitigation During the Covid-19 Pandemic." Journal of ICT: Information Communication & Technology 20.1 (2021): 42-52.
[12] Hilmy, Muhammad Irfan, and Rama Halim Nur Azmi. "Construction of State Defense and Security Against Data Protection in Cyberspace To Face New Habit Patterns." Journal of Studies of Lemhannas RI 9.1 (2021): 579-591.
[13] Jeronimo, Advento. "The Globalization Effect Of Law And Economic On Cybercrime." Journal of Legal Reform 6.3 (2019). 12-27
[14] Kashif, Muhammad, Muhammad Kashan Javed, and Digvijay Pandey. "A surge in cyber-crime during COVID-19." Indonesian Journal of Social and Environmental Issues (IJSEI) 1.2 (2020): 48-52.
[15] Kemp, Steven, et al. "Empty streets, busy internet: A time-series analysis of cybercrime and fraud trends during COVID-19." Journal of Contemporary Criminal Justice (2021): 34-45
[16] Laksana, Andri Winjaya. "Cybercrime Comparison Under Criminal Law In Some Countries." Journal of Legal Reform 5.2 (2018): 217-226.
[17] McGuire, Mike, and Samantha Dowling. "Cyber crime: A review of the evidence." Summary of key findings and implications. Home Office Research report 75 (2013).
[18] Mufid, Firda Laily, and Tioma Roniuli Hariandja. "Effectiveness of Article 28 Paragraph (1) of the ITE Law concerning the Spread of Fake News (Hoax)." Journal of Rechtens 8.2 (2019): 179-198.
[19] Mukti Fajar and Yulianto Achmad, Normative & Empirical Legal Research Dualism, Yogyakarta, Student Library, 2010, 34
[20] Muladi and Diah Sulistyani R.S., 2016, Complexity of the Development of Crime and Criminal Policy, Alumni, Bandung, 24.
[21] Nugraha, Riko. "Indonesian Legal Perspective (Cyberlaw) Handling Cyber Cases in Indonesia." Scientific Journal of Aerospace Law 11.2 (2021). 12-25
[22] Panggabean, Mompang L. "Understanding the Criminal Policy Regarding Humiliation and/or Defamation in Electronic Transactions." (2020): 49-63.
[23] Peter Mahmud Marzuki, Legal Research, Kencana Prenada Media Group, Jakarta, 2011, 35
[24] Rahardaya, Astrid Kusuma. "Literature study of the use of Tiktok social media as a means of digital literacy during the Covid-19 pandemic." Journal of Technology and Business Information Systems-JTEKSIS 3.2 (2021): 308-319.
[25] Ratulangi, Pitra, Henny Saptatia Drajati Nugrahani, and Audrey G. Tangkudung. "Types of Crime During the Covid-19 Pandemic in the Perspective of National Cyber Security in Indonesia." Syntax Literate; Indonesian Scientific Journal 6.2 (2021): 987-1001.
[26] Sa'diyah, Nur Khalimatus. "Inhibiting Factors in the Prevention and Countermeasures of Cyberporn in the Cyber World in Efforts to Renew the Criminal Law." Perspective 23.2 (2018): 94-106.
[27] Sari, Nani Widya. "Cyber Crime in the Development of Computer-Based Information Technology." Surya Kencana Dua Journal: The Dynamics of Legal and Justice Issues 5.2 (2019). 56-78
[28] Sidik, Suyanto. "Impact of the Law on Information and Electronic Transactions (UU ITE) on Legal and Social Changes in Society." Widya Scientific Journal 1.1 (2013): 1-7.
[29] Situmeang, Sahat Maruli. "The Phenomenon of Crime During the Covid-19 Pandemic: Criminological Perspectives." UNIKOM Scientific Magazine 19.1 (2021): 35-43.
[30] Soetrisno, Research Methodology, UGM, Yogyakarta, 1978, 49.
[31] Sumarwani, Sri. "A Juridical Review of Cybercrime Criminal Law in a Positive Criminal Law Perspective." Journal of Legal Reform 1.3 (2014): 287-296.
[32] SW, Muhamad Mahrus, Eko Soponyono, and Laila Mulasari. "The Contribution of Islamic Criminal Law in Efforts to Combat Cybersex Crimes in the Context of Renewing Indonesian Criminal Law." Diponegoro Law Journal 5.2 (2016): 1-19.
[33] Tanthawi, Dahlan. "Protection of Victims of Cyber Crime in the Indonesian Criminal Law System." Journal of Legal Studies 2.1 (2014).
[34] Wicaksana, Ratnadi Hendra, Adis Imam Munandar, and Palupi Lindiasari Samputra. "A Narrative Policy Framework Analysis of Data Privacy Policy: A Case of Cyber Attacks During the Covid-19 Pandemic." JOURNAL OF IPTEKKOM (Journal of Science & Information Technology) 22.2 (2020): 143-158.
[35] Winarno, Wahyu Agus. "A Study on the Information and Electronic Transactions Law (UU ITE)." Journal of Economics, Accounting and Management 10.1 (2011). 23-35

[36] Zulkifli, Nur Fika Ramadhani. "Legal Protection for Victims of Online Buying and Selling Fraud during the Covid-19 Pandemic at the Surabaya Police Station." Journal of Syntax Transformation 2.5 (2021): 638-649.