OPEN ACCESS
Scholars International Journal of Law, Crime and Justice
Abbreviated Key Title: Sch Int J Law Crime Justice
ISSN 2616-7956 (Print) |ISSN 2617-3484 (Online)
Scholars Middle East Publishers, Dubai, United Arab Emirates
Journal homepage: https://saudijournals.com

Original Research Article

Management of Improvement of Cyber Crime at the Time of the COVID-19 Pandemic Happening Restorative Justice

Rodhi Agung Saputra[1*], Rinaldy Amrullah[1], Agus Triono[1], Bonifa Refsi[1]

[1]Faculty of Law, University Lampung, Indonesia

DOI: 10.36348/sijlcj.2022.v05i07.006 | **Received:** 18.06.2022 | **Accepted:** 23.07.2022 | **Published:** 26.07.2022

***Corresponding author:** Rodhi Agung Saputra
Faculty of Law, University Lampung, Indonesia

Abstract

The purpose of this study is to find out and understand the problems of overcoming the increase in Cyber Crime during the Covid-19 pandemic. 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 problems that will be discussed in this study are how are the problems of overcoming the increase in Cyber Crime during the Covid-19 pandemic and what is the role of the Prosecutor in providing legal policies against Cyber Crime perpetrators, especially children. The findings of this study are that 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. This is because technological developments that are increasing demand 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.

Keyword: Law Enforcement, Cyber Crime, Covid-19.

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 are growing [1]. However, recently, the impact of the Covid-19 pandemic is that many people have isolated and kept their distance from each other (social distancing) which was implemented by the government in March 2020 [2]. This regulation itself is called Large-Scale Social Restrictions (PSBB), this regulation makes all business activities and normal activities such as schools hampered [3]. This incident has made many illegal activities appear with many online activities that can harm others. With the emergence of the consumptive nature of society during this pandemic, it opens up many opportunities for Cyber Crime actors to carry out their actions [4].

The increasing Covid-19 outbreak requires all of us to limit activities outside the home, so many people choose to work from home to reduce the risk of contracting Covid-19 [5]. Many people use online sites for shopping, studying, working, and other things. This is of course used by irresponsible people to commit crimes. Lack of public knowledge of this can make it

[1]Kashif, M., Muhammad, K. J., & Digvijay, P. (2020). A surge in cyber-crime during COVID-19. *Indonesian Journal of Social and Environmental Issues (IJSEI)*, 1(2), 48-52.

[2]Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies*, *23*(sup1), S47-S59.

[3] Hawdon, J., Parti, K., & Dearden, T. E. (2020). Cybercrime in America amid COVID-19: The initial results from a natural experiment. *American Journal of Criminal Justice*, *45*(4), 546-562.

[4] Sari, N. W. (2019). Kejahatan Cyber Dalam Perkembangan Teknologi Informasi Berbasis Komputer. *Jurnal Surya Kencana Dua: Dinamika Masalah Hukum Dan Keadilan*, *5*(2), 57-68.

[5] Fontanilla, M. V. (2020). Cybercrime pandemic. *Eubios Journal of Asian and International Bioethics*, *30*(4), 161-165.

easier for these elements to commit crimes. The crime committed is called Cyber Crime [6].

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:

1. Data theft is a form of illegal act by stealing data from someone through a computer system or internet network for personal gain or being marketed by selling stolen data.
2. 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.
3. Dissemination of Illegal Content is an act that spreads content that contains information or data that is not necessarily true, unethical and violates the law.
4. 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 cybercrimes or cybercrimes, 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 [7]. 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 [8]. 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 [9].

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 [10]. 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 [11]. 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) [12]. Apart from that, a very important issue to discuss is what if the perpetrators of this cybercrime are minors, and 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. Many cases 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 recognized as evidence by the Criminal Procedure Code and in court regulations. The difficulty of detecting these crimes is caused by the lack of

[6] Collier, B., Horgan, S., Jones, R., & Shepherd, L. (2020). 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*.

[7] Wicaksana, R. H., Munandar, A. I., & Samputra, P. L. (2020). Studi Kebijakan Perlindungan Data Pribadi dengan Narrative Policy Framework: Kasus Serangan Siber Selama Pandemi Covid-19 (A Narrative Policy Framework Analysis of Data Privacy Policy: A Case of Cyber Attacks During the Covid-19 Pandemic). *JURNAL IPTEKKOM (Jurnal Ilmu Pengetahuan & Teknologi Informasi)*, *22*(2), 143-158.

[8] https://mediaindonesia.com/opini/310180/ancaman-cyber-crime-di-tengah-wabah-Covid-19

[9] Barda, N. A. (2006). Tindak Pidana Mayantara dan Perkembangan Kajian. Cybercrime di Indonesia, *Jakarta: Rajawali Pers*, hal 25.

[10] Zulkifli, N. F. R. (2021). Perlindungan Hukum Terhadap Korban Penipuan Jual Beli Online Pada Masa Pandemi Covid-19 Di Polrestabes Surabaya. *Jurnal Syntax Transformation*, *2*(5), 638-649.

[11] Panggabean, M. L. (2020). *Memahami Kebijakan Kriminal Tentang Penghinaan dan/Atau Pencemaran Nama Baik dalam Transaksi Elektronik.* 49-63.

[12] Hilmy, M. I., & Azmi, R. H. N. (2021). Konstruksi Pertahanan Dan Keamanan Negara Terhadap Perlindungan Data Dalam Cyberspace Untuk Menghadapi Pola Kebiasaan Baru. *Jurnal Lemhannas RI*, *9*(1), 579-591.

adequate equipment, the reluctance of some victims to report to the police, the security system of the asset owners/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 Crime 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.

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 during the Covid-19 pandemic, the number of which is increasing, otherwise people will feel less safe and comfortable done. Based on the description of the background above, the problem in this research is how are the problems of overcoming the increase in Cyber Crime during the Covid-19 pandemic and what is the role of the Prosecutor in providing legal policies against children who commit Cyber Crime.

RESEARCH METHODS

The research method used is a normative research method [13]. By using a statute approach related to the problems of overcoming the increase in Cyber Crime during the Covid-19 pandemic [14]. The statute approach is to examine matters relating to legal principles, legal views and doctrines, and legislation related to the environment, and accurate and accountable data related to the problems of overcoming the increase in Cyber Crime during the Covid pandemic -19 [15]. In addition, an in-depth examination of the legal facts is also carried out to then seek solutions to the problems that arise in the symptoms in question [16].

DISCUSSION

Technological developments in Indonesia [17]. 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 [18].

In addition, there are also negative impacts that arise with the internet [19]. 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 (ITE) 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 [20].

In Indonesia, Cyber Crime is actually not a new crime. Cybercrime 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 [21]. 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 cause hackers and cybercriminals to easily carry out their actions are, 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 of cybercrime perpetrators who take advantage of the moment when the demand for medical devices such as masks and hand

[13] Soetrisno. (1978). Metodologi Research, *UGM, Yogyakarta*, 49.

[14] Peter M. M. (2011). Penelitian Hukum, *Kencana Prenada Media Group, Jakarta*, 35.

[15] Mukti, F. D. Y. A. (2010). Dualisme Penelitian Hukum Normatif & Empiris, *Yogyakarta, Pustaka Pelajar*, 34.

[16] Abdulkadir, M. (2004). Hukum dan penelitian Hukum, *Bandung , Citra Aditya Bakti*, 32.

[17]Suryani, K. (2017). *Sanksi Bagi Pelaku Perdagangan Perempuan Melalui Prostitusi Online (Analisis Hukum Positif dan Hukum Islam)* (Doctoral dissertation, IAIN Raden Intan Lampung).

[18]Mufid, F. L., & Hariandja, T. R. (2019). Efektivitas Pasal 28 Ayat (1) UU ITE tentang Penyebaran Berita Bohong (Hoax). *Jurnal Rechtens*, *8*(2), 179-198.

[19]Winarno, W. A. (2011). Sebuah Kajian Pada Undang-Undang Informasi Dan Transaksi Elektronik (UU ITE). *Jurnal Ekonomi Akuntansi dan Manajemen*, *10*(1), 23-35.

[20]Sidik, S. (2013). Dampak undang-undang informasi dan transaksi elektronik (UU ITE) terhadap perubahan hukum dan sosial dalam masyarakat. *Jurnal Ilmiah Widya*, *1*(1), 1-7.

[21]McGuire, M., & Dowling, S. (2013). Cyber-crime: A review of the evidence Summary of key findings and implications Home Office Research Report 75, Home Office, United Kingdom. *October*. *30p*.

sanitizers spikes sharply [22]. 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 an era of 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 playing with society's psychological rift with something that seems urgent.

The Problems of Overcoming the Increase in Cyber Crime during the Covid-19 Pandemic

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 [23]. The number of Cyber Crime in Indonesia that year was reported to have reached 36.6 million attacks [24].

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 [25]. More than just protection and preventive measures that rely on the work of the National Cyber Agency and Kominfo, 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 [26]. 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 dangerous 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 must 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 cybercrime or Cyber Crime which is increasing 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 [27]. 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

[22] Handayani, P. (2013). Penegakan Hukum Terhadap Kejahatan Teknologi Informasi (Cyber Crime). *Jurnal Dimensi*, *2*(2), 12-24

[23] Herdiana, Y., Munawar, Z., & Putri, N. I. (2021). Mitigasi Ancaman Resiko Keamanan Siber Di Masa Pandemi Covid-19. *Jurnal ICT: Information Communication & Technology*, *20*(1), 42-52.

[24] Ratulangi, P., Nugrahani, H. S. D., & Tangkudung, A. G. (2021). Jenis Kejahatan Pada Masa Pandemi Covid-19 dalam Perspektif Cyber Security Nasional di Indonesia. *Syntax Literate; Jurnal Ilmiah Indonesia*, *6*(2), 987-1001.

[25] Situmeang, S. M. (2021). Fenomena kejahatan di masa pandemi Covid-19: Perspektif Kriminologi. *Majalah Ilmiah UNIKOM*, *19*(1), 35-43.

[26] Rahardaya, A. K. (2021). Studi Literatur Penggunaan Media Sosial Tiktok Sebagai Sarana Literasi Digital Pada Masa Pandemi Covid-19. *Jurnal Teknologi Dan Sistem Informasi Bisnis-JTEKSIS*, *3*(2), 308-319.

[27] Tanthawi, D. (2014). PERLINDUNGAN KORBAN TINDAK PIDANA CYBER CRIME DALAM SISTEM HUKUM PIDANA INDONESIA. *Jurnal Ilmu Hukum*, *2*(1).

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 KUHAP 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 accused.

Furthermore, in addition to legal instruments, special institutions, government-owned and non-governmental organizations (NGOs), are needed as an effort to combat 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 overcoming Cyber Crime [28].

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 [29].

Problems related to Cyber Crime if there is no proper supervision or law enforcement, in any case, this crime will continue to increase. Therefore, an action or role of the government is needed to carry out surveillance both preventively and repressively with the aim of reforming law and public security in the era of globalization and the development of advanced technology as it is today. This is because nowadays, especially in Indonesia, the use of technology-based media has been widely used, therefore it is necessary to carry out strict supervision regarding Cyber Crime so that it does not continue to increase and the people who are harmed do not increase.

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

Technological advances have implications for the development of crime [30]. 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 [31] 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 [32]. Crimes committed in cyberspace generally aim to generate financial gain for the perpetrators [33]. 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 [34.

Indonesia has come under greater scrutiny from Cyber Crime 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 the problems related to Cyber Crime, continue to increase, plus with the Covid-19 which all activities must be carried out at home using electronic media, this requires the government to strengthen regulations to deal with Cyber Crime issues. Furthermore, the problems related to Cyber Crime are related to:

[28] Nugraha, R. (2021). Perspektif Hukum Indonesia (Cyberlaw) Penanganan Kasus Cyber Di Indonesia. *Jurnal Ilmiah Hukum Dirgantara*, *11*(2), 12-25.

[29] Akub, M. S. (2018). Pengaturan Tindak Pidana Mayantara (Cyber Crime) dalam Sistem Hukum Indonesia. *Al-Ishlah: Jurnal Ilmiah Hukum*, *21*(2), 85-93.

[30] Laksana, A. W. (2018). Cybercrime Comparison Under Criminal Law In Some Countries. *Jurnal Pembaharuan Hukum*, *5*(2), 217-226.

[31] Bunga, D. (2019). Politik hukum pidana terhadap penanggulangan cybercrime. *Jurnal Legislasi Indonesia*, *16*(1), 1-15.

[32] Sa'diyah, N. K. (2018). Faktor Penghambat Dalam Pencegahan dan Penanggulangan Cyberporn di Dunia Cyber Dalam Upaya Pembaharuan Hukum Pidana. *Perspektif*, *23*(2), 94-106.

[33] Jeronimo, A. (2019). THE GLOBALIZATION EFFECT OF LAW AND ECONOMIC ON CYBERCRIME. *Jurnal Pembaharuan Hukum THE GLOBALIZATION EFFECT OF LAW AND*, *6*(3), 12-27.

[34] Sumarwani, S. (2014). Tinjauan Yuridis Pemidanaan Cybercrime Dalam Perpektif Hukum Pidana Positif. *Jurnal Pembaharuan Hukum*, *1*(3), 287-296.

1. Characteristics of crime in cyberspace show that this crime can cross state jurisdiction, while the existence of international agreements regarding law enforcement against Cyber Crime is still very limited.
2. Penal policies in cybercrime prevention 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 and 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 should 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 [35].

Criminal policy is used as an alternative in solving social policies [36]. 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 wide and complex crime, therefore crime prevention is carried out by means of penalizing (the use of criminal law) and balanced with non-penal means [37]. 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 war making 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 [38]. 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 dealing with Cyber Crime can be carried out in two ways, namely:

a. 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 cybercrime 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.

b. Non-Penal Policy (Role of the Prosecutor's Office)

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

1) Develop policies outside of criminal law that support cybercrime prevention efforts, such as through anti-hate policies, anti-bullying policies and healthy internet policies through the education system;
2) 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;
3) Build cooperation with the private sector to build a security system in cyberspace;
4) Establish an institutional network in preventing Cyber Crime both at the national and international levels. International cooperation in overcoming Cyber Crime is very much needed considering 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 cybercrime. Legal politics in tackling Cyber Crime is carried out by developing a global strategy in preventing and enforcing laws against crimes in cyberspace, compiling responsive legal

[35]Sumarwani, S. (2014). Tinjauan Yuridis Pemidanaan Cybercrime Dalam Perpektif Hukum Pidana Positif. *Jurnal Pembaharuan Hukum*, *1*(3), 287-296.

[36]SW, M. M., Soponyono, E., & Mulasari, L. (2016). Kontribusi Hukum Pidana Islam Dalam Upaya Penanggulangan Tindak Pidana Cybersex Dalam Rangka Pembaharuan Hukum Pidana Indonesia. *Diponegoro Law Journal*, *5*(2), 1-19.

[37] Muladi, S. H., Diah Sulistyani, R. S., & SH, C. (2021). *Kompleksitas Perkembangan Tindak Pidana dan Kebijakan Kriminal*. Penerbit Alumni.

[38]Hafidz, J. (2014). Kajian Yuridis Dalam Antisipasi Kejahatan Cyber. *Jurnal Pembaharuan Hukum*, *1*(1), 32-40.

formulations and preparing institutions that can take quick action when problems occur in cyberspace.

Legal reform is an attempt to further improve and perfect 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.

CONCLUSION

Based on the results of research related to the Problems of Overcoming Cyber Crime during the Covid-19 Pandemic, it can be concluded that 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. In the midst of the outbreak of the Covid-19 pandemic, various countries are faced with cybercrime or Cyber Crime which is increasing and targeting groups related to Covid-19. The Corona virus pandemic is being used to influence the global cyber threat landscape. Problems that arise in relation to Cyber Crime are how to eradicate or enforce the law can be done with the politics of criminal law.

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

- Abdul, K. M. (2004). Hukum dan penelitian Hukum, *Bandung : Citra Aditya Bakti*, 32.
- Akub, M. S. (2018). Pengaturan Tindak Pidana Mayantara (Cyber Crime) Dalam Sistem Hukum Indonesia. *Al-Ishlah, Jurnal Ilmiah Hukum*, 21(2), 85-93.
- Barda, N. A. (2005). Pembaharuan Hukum Pidana; Dalam Perpekstif Kajian Perbandingan, *Citra Aditya Bakti, Bandung*, 102.
- Barda, N. A. (2006). Tindak Pidana Mayantara dan Perkembangan Kajian Cyber Crime di *Indonesia, Jakarta: Rajawali Pers*, hal 25.
- Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies*, *23*(sup1), S47-S59.
- Bunga, D. (2019). Politik hukum pidana terhadap penanggulangan cybercrime. *Jurnal Legislasi Indonesia*, 16(1), 1-15.
- Collier, B., Horgan, S., Jones, R., & Shepherd, L. (2020). 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*.
- Fontanilla, M. V. (2020). Cybercrime pandemic. *Eubios Journal of Asian and International Bioethics*, 30(4), 161-165.
- Hafidz, J. (2014). Kajian Yuridis Dalam Antisipasi Kejahatan Cyber. *Jurnal Pembaharuan Hukum*, 1(1), 32-40.
- Handayani, P. (2013). Penegakan Hukum Terhadap Kejahatan Teknologi Informasi (Cyber Crime). *Jurnal Dimensi*, 2(2), 12-24.
- Hawdon, J., Parti, K., & Dearden, T. E. (2020). Cybercrime in America amid COVID-19: The initial results from a natural experiment. *American Journal of Criminal Justice*, *45*(4), 546-562.
- Herdiana, Y., Munawar, Z., & Putri, N. I. (2021). Mitigasi Ancaman Resiko Keamanan Siber Di Masa Pandemi Covid-19. *Jurnal ICT: Information Communication & Technology*, *20*(1), 42-52.
- Hilmy, M. I., & Azmi, R. H. N. (2021). Konstruksi Pertahanan Dan Keamanan Negara Terhadap Perlindungan Data Dalam Cyberspace Untuk Menghadapi Pola Kebiasaan Baru. *Jurnal Lemhannas RI*, *9*(1), 579-591.
- Jeronimo, A. (2019). THE GLOBALIZATION EFFECT OF LAW AND ECONOMIC ON CYBERCRIME. *Jurnal Pembaharuan Hukum THE GLOBALIZATION EFFECT OF LAW AND*, *6*(3), 12-27.
- Kashif, M., Javed, M. K., & Pandey, D. (2020). A surge in cyber-crime during COVID-19. *Indonesian Journal of Social and Environmental Issues (IJSEI)*, *1*(2), 48-52.
- Kemp, S., Buil-Gil, D., Moneva, A., Miró-Llinares, F., & Díaz-Castaño, N. (2021). Empty streets, busy internet: A time-series analysis of cybercrime and fraud trends during COVID-19. *Journal of Contemporary Criminal Justice*, *37*(4), 480-501.
- Laksana, A. W. (2018). Cybercrime Comparison Under Criminal Law In Some Countries. *Jurnal Pembaharuan Hukum*, *5*(2), 217-226.
- McGuire, M., & Dowling, S. (2013). Cyber-crime: A review of the evidence Summary of key findings and implications Home Office Research Report 75, Home Office, United Kingdom. *October*. *30p*.
- Mufid, F. L., & Hariandja, T. R. (2019). Efektivitas Pasal 28 Ayat (1) UU ITE tentang Penyebaran Berita Bohong (Hoax). *Jurnal Rechtens*, *8*(2), 179-198.

- Mukti, F. D. Y. A. (2010). Dualisme Penelitian Hukum Normatif & Empiris, *Yogyakarta, Pustaka Pelajar*, 34.
- Muladi, D. D. S. R. S. (2016). Kompleksitas Perkembangan Tindak Pidana dan Kebijakan Kriminal, *Alumni, Bandung*, 24.
- Nugraha, R. (2021). Perspektif Hukum Indonesia (Cyberlaw) Penanganan Kasus Cyber Di IndonesiA. *Jurnal Ilmiah Hukum Dirgantara*, 11(2), 12-25.
- Panggabean, M. L. (2020). *Memahami Kebijakan Kriminal Tentang Penghinaan dan/Atau Pencemaran Nama Baik dalam Transaksi Elektronik*. 49-63.
- Peter, M. M. (2011). Penelitian Hukum, *Kencana Prenada Media Group, Jakarta*, 35.
- Rahardaya, A. K. (2021). Studi Literatur Penggunaan Media Sosial Tiktok Sebagai Sarana Literasi Digital Pada Masa Pandemi Covid-19. *Jurnal Teknologi Dan Sistem Informasi Bisnis-JTEKSIS*, 3(2), 308-319.
- Ratulangi, P., Henny, S. D. N., & Audrey, G. (2021). Tangkudung. Jenis Kejahatan Pada Masa Pandemi Covid-19 dalam Perspektif Cyber Security Nasional di Indonesia. *Syntax Literate; Jurnal Ilmiah Indonesia*, 6(2), 987-1001.
- Sa'diyah, N. K. (2018). Faktor Penghambat Dalam Pencegahan Dan Penanggulangan Cyberporn Di Dunia Cyber Dalam Upaya Pembaharuan Hukum Pidana. *Perspektif* , 23(2), 94-106.
- Sari, N. W. (2019). Kejahatan Cyber Dalam Perkembangan Teknologi Informasi Berbasis Komputer. *Jurnal Surya Kencana Dua: Dinamika Masalah Hukum Dan Keadilan*, 5(2), 56-78.
- Sidik, S. (2013). Dampak Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) terhadap Perubahan Hukum dan Sosial dalam Masyarakat. *Jurnal Ilmiah Widya*, 1(1), 1-7.
- Situmeang, S. M. (2021). Fenomena Kejahatan Di Masa Pandemi Covid-19: Perspektif Kriminologi. *Majalah Ilmiah UNIKOM*, 19(1), 35-43.
- Soetrisno. (1978). Metodologi Research, *UGM, Yogyakarta*, 49.
- Sumarwani, S. (2014). Tinjauan Yuridis Pemidanaan Cybercrime Dalam Perpektif Hukum Pidana Positif. *Jurnal Pembaharuan Hukum*, 1(3), 287-296.
- Suryani, K. (2017). *Sanksi Bagi Pelaku Perdagangan Perempuan Melalui Prostitusi Online (Analisis Hukum Positif dan Hukum Islam)* (Doctoral dissertation, IAIN Raden Intan Lampung).
- SW, M. M., Soponyono, E., & Mulasari, L. (2016). Kontribusi Hukum Pidana Islam Dalam Upaya Penanggulangan Tindak Pidana Cybersex Dalam Rangka Pembaharuan Hukum Pidana Indonesia. *Diponegoro Law Journal*, *5*(2), 1-19.
- Tanthawi, D. (2014). PERLINDUNGAN KORBAN TINDAK PIDANA CYBER CRIME DALAM SISTEM HUKUM PIDANA INDONESIA. *Jurnal Ilmu Hukum*, *2*(1).
- Wicaksana, R. H., Munandar, A. I., & Samputra, P. L. (2020). Studi Kebijakan Perlindungan Data Pribadi dengan Narrative Policy Framework: Kasus Serangan Siber Selama Pandemi Covid-19 (A Narrative Policy Framework Analysis of Data Privacy Policy: A Case of Cyber Attacks During the Covid-19 Pandemic). *JURNAL IPTEKKOM (Jurnal Ilmu Pengetahuan & Teknologi Informasi)*, *22*(2), 143-158.
- Winarno, W. A. (2011). Sebuah Kajian Pada Undang-Undang Informasi Dan Transaksi Elektronik (UU ITE). *Jurnal Ekonomi Akuntansi dan Manajemen*, *10*(1), 23-35.
- Zulkifli, N. F. R. (2021). Perlindungan Hukum Terhadap Korban Penipuan Jual Beli Online Pada Masa Pandemi Covid-19 Di Polrestabes Surabaya. *Jurnal Syntax Transformation*, *2*(5), 638-649.