JURNAL META-YURIDIS
No. P-ISSN : 2614-2031 / NO. E-ISSN : 2621-6450
Fakultas Hukum Universitas PGRI Semarang
Homepage: http://journal.upgris.ac.id/index.php/meta-yuridis/

Article History: *Received: 2025-01-07* *Accepted: 2024-03-20*
Published: 2024-03-28

DEVELOPMENT OF CYBERCRIME AND INDONESIAN CRIMINAL LAW

Syukron Abdul Kadir
Faculty of Law, Widya Mataram University Yogyakarta, Indonesia.
syukronkadir@gmail.com

Hartanto*
Faculty of Law, Widya Mataram University Yogyakarta, Indonesia.
hartanto.yogya@gmail.com

Abstract: The advancement of information technology and technology has a positive impact, but can also be exploited by (cyber) criminals to carry out their evil intentions, with the potential to cause many victims and spread quickly. Crimes that use or are related to computers and the internet can make a place in cyberspace (computers/internet) a means to commit evil deeds, a target/target of crime, or a place to hide the proceeds of crime. The research method used is a normative research method with a descriptive model that examines aspects of legal regulations related to cybercrime and its development. The results of the study show that the development of computer crime today is not only limited to illegal access, and at a low level has disrupted social relations between communities with the type of defamation/hoax. Further development of the scope of crime and cybercrime requires sophisticated tools for law enforcement, as well as the professionalism of law enforcers. In addition to the criminal law system and imprisonment for cyber criminals, another alternative is restorative justice for low-level crimes. The government "needs to pay attention" to the development of crime in cyberspace, considering the acceleration of its development is very high.

Keywords: ***Cybercrime, Cyberspace, Criminal Law, Internet, Evolving Crime***

INTRODUCTION

In 2021, organizations in Asia experienced the most attacks worldwide. The percentage of attacks on organizations by continent in 2021 was as follows: Asia (26%), Europe (24%), North America (23%), Middle East and Africa (14%), Latin America (13%) (AAG, 2023). Cybercrime is a greater risk when doing business in various parts of the world, internet connectivity is growing rapidly and faster, and in areas with fast internet connections, the potential for internet crime will also spread (operate) quickly. The lack of transparency in certain countries will result in weak cyber regulations and law enforcement, as well as low public awareness in cyberspace activities, no less important is security investment among user companies or electronic service providers. Society will naturally strive to develop and become more advanced, and in this era it is increasingly dependent on telecommunications technology (the internet), so that the relationships that occur cannot be interpreted as between countries, but become more widespread between humans (individuals), resulting in multiple

relations, which give rise to a new world order and at the same time require new areas of law.

The speed or even acceleration of the development of internet information and communication technology is supported by the ease of purchasing devices and using information and communication technology devices, especially through mobile devices (handheld). Daily activities and businesses, which used to be done directly (the real world), are now widely done through cyberspace using gadgets (electronic devices that access the internet). The development of transactions has shifted to electronic communication devices: smartphones, cellphones, i-Pads, notebooks, etc. Accessing information is currently very easy, and can even be done by all ages uncontrollably, to reach the whole world. Nowadays, mobile devices that can access the internet are increasingly affordable, then there are many free wifi/hotspots in various public places, from offices to small Indomie stalls (warmindo). The consequences of the development of technology connected to the internet are also widespread in its misuse; so that it becomes a factor that disturbs the cyber world community, namely the occurrence of cybercrime or what is commonly known as cybercrime (Yusuf DM, et al., 2022). Various crimes, whether we realize it or not, have occurred in cyberspace and caused losses, namely at least making cyberspace a worrying place for its users.

The Indonesian government has anticipated this by revising the Law on Information and Electronic Transactions for the second, to Law No. 19 of 2016 concerning Electronic Transaction Information (ITE), and the third to Law No. 1 of 2024, but has not specifically created a cybercrime law.

MAIN PROBLEM

The cyber world has several times raised warnings to the Indonesian government, in terms of illegal access by criminals (hackers). The development of a country will be successful if the country's resilience and support for community authorization are realized, namely a state of avoiding disturbances and threats, including forms of crime. In Indonesia, this era of conventional crime that targets a person or group of people in concrete terms, has changed into abstract/widespread crime by disrupting social development and economic issues in an industrial society whose perpetrators are knowledgeable, educated, and organized people (white collar crime category). Based on the description above, the formulation of the problem in this writing is: how to overcome the development of information technology (crime) in the criminal law system in Indonesia.

METHOD OF RESEARCH

This study uses a normative legal method, using secondary data collected and analyzed from libraries, websites, and so on, then analyzed descriptively (Hartanto, 2023). The aim is to provide a better understanding of the issues studied based on legal documents and published research papers (Firmansyah, 2023).

RESEARCH RESULT AND DISCUSSION

1. Scope of Cybercrime

Cybercrime is a negative impact (dark-side) of technological advances, and can include very broad behavior/victims, where the use of electronic information technology occurs without moral and ethical considerations (Firmansyah, 2017). Cybercrime develops with the focus of the internet or servers, and usually the perpetrators are disguised or anonymous, with crime modes that are actually conventional, namely fraud, extortion, theft, or embezzlement. Although interpreted as cybercrime, several stages of this evil act still require real-world instruments, such as many real accounts or offline communication. Cybercrime is interpreted as a series of actions by people, groups of people, legal entities/business entities that use computers (or other electronic devices) connected to the network/internet, as a facility for evil deeds, and as targets (targets) of cybercrime, or as a place to store the proceeds of crime. The characteristics of "Cybercrime" according to Y. Pratama, (Pratama, 2022) include:

1.1 Illegal, criminal or immoral behaviour occurs on the internet, making it difficult to determine which country's legal authority applies to it.

1.2 This problem can be committed on any device that has an internet connection.

1.3 These acts cause financial and immaterial losses (time, morals, customs, money, opportunities and confidentiality of information), which are likely to be greater than the consequences of traditional pattern crimes.

1.4 The perpetrators are those who have the ability to use/control electronic technology, applications, which are connected to the internet.

1.5 national dividing lines (national jurisdictions and cross-jurisdictional)

2. Cybercrime in Indonesia

The development of cybercrime, began with an attack in the cyber world in 1988 carried out by a student known as Cyber Attack. In 1994, a 16-year-old schoolboy R. Pryce with the nickname/alias "Datastream Cowboy", was arrested for illegally entering a classified computer system, including the Griffiths Air Force data center, NASA, and the Korean atomic research agency Data Center (M.C Dewi, 2022). For people who are accustomed to accessing communication technology media via the internet, cybercrime is not a foreign term. Cybercrime or cybercrime is a phenomenon that cannot be denied. The problems of cybercrime are increasingly diverse and growing every day, especially in countries that are still weak in the field of communication technology law. Crime is a social phenomenon that

has existed in the world, since the beginning of human civilization. Crime is a terminology that has developed because of two large groups, namely the essence of the crime which is indeed new, or the politics of criminal law that an act that was previously not regulated, is regulated in legislation so that it becomes a criminal act. As before the ITE Law, "gossiping" or talking about other people in the real world was commonplace in certain community groups, but when this "gossiping" occurs in cyberspace (social media), it can be qualified as an ITE crime if it has met its elements, namely the simplest/common is defamation or hate speech, and of course with the emergence of real victims (material). On the other hand, there are still many differences in the terminology of hate speech in various countries (Hartanto, et al., 2024). This advanced (modern) crime is actually a form of change in the perpetrator's modus operandi, changing the crime from its original (conventional) form because it uses internet communication technology (A. Raharjo, 2002). The portrait of the crime that was originally hard/rough has metamorphosed into something "smoother" by using internet technology (virtual) in such a way, but in terms of its impact and speed of causing victims, it has become several times higher. Losses in general can occur in a moral and material manner, while victims can be individuals or multiple in the form of netizens (cyberspace residents). Meanwhile, in developing countries which are generally identified with the digital divide, such as Indonesia, they have not accommodated moral losses, such as hoaxes as a form of crime, this can be seen from false news during the campaign period (legislative/presidential elections). In general, the term that is well-known in Indonesia/internationally, namely hackers, using general assumptions referring to real life, there are black and white, some play the role of heroes/guards, and some are like criminals. Furthermore, in understanding cybercrime, we need to understand what are the 5 (five) types of cybercrime in Indonesia (Admin MSI, 2023):

2.1 Carding, is a crime using unauthorized credit card transactions. The perpetrators generally use illegal methods to obtain other people's credit card data, then to make purchases or transactions. Some famous cases in Indonesia: credit card hacking against Awkarin, G. Anastasia, J. Iskandar, T. Mirasih, B. William. and R. Stefanie.

2.2 Phishing, is a crime by deceiving victims through cyberspace. Phishers (perpetrators) generally create fake sites, spread fake links, or send emails to potential victims. The goal is to obtain victim data ranging from personal identity to passwords, PIN codes, and OTPs on their accounts. Phishing cases in Indonesia reach tens of thousands.

2.3 Ransomware, this term is the act of using infiltrated malware to infect computers and take victim data. Then, the perpetrators ask for ransom by threatening the victim for taking the victim's important data. Indonesia is ranked as the country with the highest ransomware threat in ASEAN

2.4 Online Loans, namely online loans that are not registered with the Financial Services Authority (OJK) are

illegal. The perpetrators use the victim's ID card data/photos and "selfie" photos that are sold on the "black market", used for money laundering, or other crimes. Lack of financial understanding (gaptek), can be one of the factors in being trapped in online loans. OJK member F.W. Dewi stated that many people complain about being trapped in online loans. "Previously trapped by loan sharks, now online loans,"

2.5 Illegal content, this type of crime is often found in Indonesia in the form of illegal content. The perpetrators spread information that is incorrect and violates the law, such as slander (hoaxes) and fake news, information containing elements of pornography, and other information regarding state secrets or government propaganda.

Indonesia's delay in following the development of modern communication technology among ASEAN countries is because Indonesia has not succeeded in prioritizing technology development and mastery of strategies, for example in terms of technology transfer from developed to developing countries. Indonesia continues to strive to develop criminal law in the cyber field, but until now it is still a country with a fairly large digital divide. The digital divide that occurs in the form of: the gap in the ability to use communication technology, this is the impact of the gap in education and economic levels in Indonesia; then access to communication technology is not evenly distributed.

3. Cybercrime in Indonesian Criminal Law

The Indonesian criminal law system does not specifically regulate cyber law, but there are laws that have regulated the handling of cyber crimes, such as Law abaout Telecommunications, Law about the Eradication of Terrorism, and Law. No. 11 of 2008 the third amendment to Law No. 1 of 2024 concerning ITE. These laws and regulations have criminalized types of cybercrime and the threat of punishment for each violator. In addition, the criminalization policy written in the cyber crime category in Law No. 1 of 2024 concerning ITE has been reaffirmed in certain articles to follow the formulation in the Criminal Code, this is stated in the Joint Decree of the Minister of Communication and Information of the Republic of Indonesia, the Attorney General of the Republic of Indonesia, and the Chief of Police, No. 229 of 2021, No. 154 of 2021 No. KB / 2 / VI / 2021. This is a government step to respond to the public "noise", about various problems in the ITE Law articles which are called multi-interpretable/rubber articles. Furthermore, cybercrime in the new Criminal Code (Law No. 1 of 2023) Article 5 and its explanation, so that cybercrime can be included in the category of national interests that need to be protected, on par with criminal acts of corruption and money laundering. Cybercrime occupies a strategic position to be studied and regulated in the criminal law system in Indonesia

Cybercrime which is regulated in Law. No. 19 of 2016 concerning Amendments to Law. No. 11 of 2008 concerning Information and Electronic Transactions, as follows:

1) Acts that violate morality.

Article 27 paragraph (1) of Law No. 19 of 2016 states "Any person who intentionally & without the right shares/disseminates/makes accessible Electronic Information or Electronic Documents that contain content that violates morality". This element of "violating morality" requires further interpretation of morality and one of the references is the Criminal Code, while in law enforcement it often requires experts to help interpret moral norms/definitions. Acts that violate morality through/using electronic media, in Article 27 paragraph (1) of Law Number 11 of 2008 as amended by Law No. 19 of 2016, include online pornography and online prostitution. If this crime is committed against children, it will become more serious with the addition of aggravation. One of the current problems is the impact of the development of internet technology, namely the proliferation of sites that display pornographic stories/pornographic scenes. The current phenomenon, it is very difficult to protect internet users from commercialization efforts of sexual entertainment (morality) (A. Wahid and M. Labib, 2005).

2) Gambling

Victims of online gambling are very many in Indonesia, criminal acts of online gambling are regulated in Article 27 paragraph (2) of the Electronic Information and Transactions Law. This regulation also states that: "Any person who intentionally and without rights, shares/distributes/makes accessible electronic information/electronic documents that contain gambling content".

3) Insults or defamation

Defamation or insults in cyberspace are prohibited as mandated in Article 27 (3) of Law No. 19 of 2019, which reads: "Any person who intentionally, and without rights, shares/distributes/makes accessible electronic information/electronic documents that contain insults or defamation." Lawmakers equate insults and defamation. Insult itself is an act of humiliation so that people are offended, while one form of insult is defamation. Referring to Chapter XVI Book II regarding acts of insult and defamation. Insults consist of general insults and specific insults.

4) Extortion or threats

Article 27 paragraph (4) of Law No. 11 of 2008 as amended by Law No. 19 of 2016, prohibits extortion/threats in cyberspace; Everyone is prohibited from intentionally and without rights, distributing and/or transmitting and/or making accessible electronic information and/or electronic documents… containing extortion and/or threats.

Article 368 (1) of the Criminal Code includes the qualifications for acts that constitute extortion or threats, namely: “Anyone who intends to benefit himself or another person, in an unlawful (illegal) manner, forces someone to give something belonging to that person, or another person in whole or in part with violence or threats of violence, or creates debt or eliminates debt, will be punished for extortion and can be sentenced to up to 9 years in prison.

5) Stalking (cyberstalking)

Cyberstalking/stalking has not been regulated in Law No. 19 of 2016,

but when it has fulfilled the element of threat, then it can be subject to Article 29, namely: "Any person who intentionally and without right, sends Electronic Information or Electronic Documents containing threats of violence or intimidation that are directed personally". The provisions regarding electronic information and transactions in Article 29 regulate acts of harassment, threats, or other actions carried out to cause fear, including certain words or actions. This concept is called cyberstalking in America, England, Canada and some other countries. This action is carried out by utilizing information and communication technology (S. Suseno, 2012). The threat of punishment in this article has been derived from Law No. 11 of 2008 with Law No. 19 of 2016. This cyberstalking can also develop into cyberbullying, which is a more concrete criminal act (M.R. Azhari, 2019). 6) Spread of fake news (hoax) The spread of fake, untrue, incomplete news is generalized in Law. No. 11/2008 amended by Law No. 19 of 2016, in Article 28 (1), reads: "Any person who intentionally and without rights spreads false/fake and misleading news, which results in consumer losses in Electronic Transactions."

7) Hate speech is regulated in Article 28 (2) of Law No. 19 of 2016 concerning ITE, which mandates that: "Any person who intentionally and without rights, spreads information designed to cause hatred or hostility towards certain individuals/community groups based on ethnicity, religion, race, and inter-group (SARA)".

8) Illegal access

Law Number 19 of 2016 in Article 30 essentially stipulates: Any person who intentionally, without rights (against the law), accesses another person's electronic system through any act..

4. Cybercrime Prevention

Cybercrime causes a large number of victims, especially in the financial sector, but not all of them are visible, so it is called the "iceberg phenomenon". On average, victims can only regret the crime that befell them; They hope to learn a lot from their current experience; and what needs to be done now is to prevent possibilities that can harm us as perpetrators of crimes using information technology. This prevention can be in the form of:

4.1 Senate campaigning for "Healthy Internet"

4.2 Socialization/education to internet users, about social media ethics and the dangers of cybercrime.

4.3 Trying for additional security software, either in the form of using antivirus or firewall.

4.4 Socializing the importance of protecting personal data, and recognizing sites that request personal data.

5. Cybercrime Law Enforcement in Indonesia

There are still obstacles in law enforcement efforts against cybercrime perpetrators, even though there is Law No. 19 of 2016 and Joint Ministerial Regulations concerning Electronic Information and Transactions. However, the positive thing in this ITE Law is that there is

something new in the criminal field, namely Article 5 of the Law on ITE, regarding the expansion of relatively new (up to date) evidence, in accordance with the applicable procedural law in Indonesia, namely recognizing electronic information and electronic data or printouts/recordings as valid evidence, and also applies to other laws outside the ITE Law.

The problems of law enforcement against cybercrime perpetrators, as with law enforcement in other criminal fields, are: law enforcement officers lack the skills or quality to conduct cyber patrols, limited latest equipment owned by the Police. Such as tools that should be in every Regional Police/Residential Police to accelerate detection and prediction of the whereabouts (positioning system), of cybercrime perpetrators. Currently only available at the National Police Headquarters and several relatively large Regional Police/Cities, so there are obstacles, delays and high budget requirements in every cybercrime case investigation process in Indonesia; Finally, victims are reluctant to report crimes that have befallen them, for various reasons: privacy (shame), economic (costs), or victims do not trust the expertise and services of the police in uncovering the case (Thantawi, 2014).

6. Legal Protection for Victims of Cybercrime in Indonesia

Law enforcement actions against perpetrators of cybercrime are to protect cyberspace users from crackers who use the internet to commit their crimes. Although Indonesia does not specifically have a law on cyber law or a law on the eradication of cybercrime, Indonesia still needs legal action using existing laws such as: legislation, jurisprudence and international conventions that have been ratified to protect the interests of media users in cyberspace (MR Habibi and I. Liviani, 2020).

Efforts to protect victims of crime are also efforts to restore the losses experienced by the victims. This would make more sense if the victim was involved or participated in the process of resolving the criminal case. Law enforcement is a sustainable development effort that aims to create a safe, peaceful, orderly and dynamic life for the country and the country's environment, in an independent world environment.

In the future, some parties expect criminal law enforcement to be more directed towards a restorative justice system, this is a fair solution to mediate between perpetrators, victims, their families, and other parties involved in the crime, to jointly try to resolve the conflict by reaching a consensus. This is based on several existing regulations, namely: a joint decree of the Supreme Court of the Republic of Indonesia, the Minister of Law and Human Rights (HAM), the Minister of Social Affairs, and the Minister of Women's Empowerment and Child Protection, which emphasizes the restoration of the original state, which we know as restorative justice. The urgency of legal protection for internet users in Indonesia is greatly needed, because it is very possible that the prevalence of cybercrime will be higher than conventional crime, often the dependence of the entire community

and the world on internet technology. Restorative Justice according to the author can only be applied to certain types of cybercrime, especially those that do not have a widespread impact (chaos/riot) and are accompanied by material losses (financial) in a certain amount.

7. Obstacles in Handling Cybercrime

Cybercrime perpetrators have been prosecuted using existing laws, but there are still obstacles in law enforcement, including:

1) Investigator capabilities

In general, the knowledge and understanding of the operation of computers by Polri investigators against cybercriminals, as well as the ability to investigate these cases, are still very minimal. In the cocept of law enforcement on cybercrime, it is greatly influenced by five elements, namely: Law, law enforcement officers (mentality), community behavior, legal facilities & culture (Y. Amrozi, 2021). The same perception of the articles in the Criminal Code as the backbone of criminal law in Indonesia, among investigators (especially the Polri), in interpreting the elements of cybercrime, and the need for a special law on cybercrime law.

2). Supporting equipment/equipment for law enforcement in the field of cybercrime, for example adequate electronic system equipment, for example a cyber laboratory. One of the most striking things in this field is the difficulty that occurred in the case of the murder of "Mirna" which was declared to have originated from coffee containing cyanide in 2016, while the electronic evidence (direct evidence) that existed was inadequate to prove the perpetrator's actions, as a result the perpetrator was convicted based on a series/syllogism/relevance of circumstantial evidence, and the judge's conviction; The emergence of a documentary entitled Ice Cold: Murder, Coffee and Jessica Wongso, which was broadcast on Netflix in 2023, was the trigger; and currently the case is being debated again by experts, including Otto Hasibuan, Eddy OSH, Djaja Surya Atmadja, Reza Indragiri, and Winardo Wongso. Of course, cybercrime will be much more complicated to prove than just CCTV evidence.

CONCLUSION

Cybercrime has the meaning of an individual activity, a group of people, a legal entity using computer facilities to commit crimes, as a target, and can also be used to store the proceeds of crime. Another definition by Wisnubroto in Habibi, means that computer crime is an act that is against the law, which is committed using a computer as a means/tool, or a computer as an object, to gain profit or not, but has consequences that are detrimental to other people (causing victims).

Communication technology has a tremendous influence in changing human communication behavior, in addition to bringing benefits in the form of ease of communication, technology can also bring losses, one of which is making it easier for "criminals" to commit crimes. The ease of accessing technology and its sophistication, allows people to be influenced to misuse it, in addition to those who do have evil intentions (mens rea) to commit cybercrime.

Based on the cases and conditions of cybercrime that occur in Indonesia, it can be seen that cybercrime is a serious threat to society and state security and Indonesia does not seem to have built a cyber security system. In Indonesia, crimes using computer devices and the internet (cybercrime) are one of the highest crimes in the world. The Indonesian legal system specifically does not yet have a cybercrime law, but is currently using several laws related to cybercrime, such as Law about Telecommunications, Law about the Eradication of Terrorism; however, this concept can still develop with the regulation of norms in the Human Rights Law & the Law on Anti-Monopoly & Unfair Business Competition, even the Law on the Eradication of Corruption.

The development of criminal law in cyberspace requires 2 (two) substantial things, namely sophisticated devices (equipment) and human resources (law enforcers/investigators). The current reality shows that criminal law policy has a dominant/strategic position in developing modern law.. Legislation must be updated periodically, to keep up with the threat of cybercrime which continues to increase along with the progress and dependence on the latest technology. Countries should cooperate regionally and internationally to build consensus on common cyber security standards, for more effective collaboration or establish joint mechanisms to exchange information and combat cybercrime threats.

REFERENCE

[1] AAG, The Latest 2023 Cyber Crime Statistics (updated Dec. 2023), https://aag-it.com/the-latest-cyber-crime-statistics/, diakses 3 Mei 2024

[2] Admin MSI. (2023). There Are 5 Types Of Cybercrime In Indonesia, https://www.hypernet.co.id/en/2023/03/11/cybercrime-ada-5-jenis-di-indonesia-2/, diakses 5 Juni 2024

[3] Amrozi, Y. dkk. (2021). Tantangan Security Dan Kehandalan Sistem Dalam Aplikasi Bergerak. *Jurnal Jukanti*, 4(2), 8. DOI: 10.37792/jukanti.v4i2.253

[4] Azhari, Muhammad Redha. (2019). Aspek Pidana Mayantara (Cyberstalking). *Badamai Law Journal*, 4(1), 152. http://dx.doi.org/10.32801/damai.v4i1.9234

[5] Dewi, M.C. (2022). Cyber Espionage in National and Global Perspective: How Indonesia Deal with this issue?, *International Law Discourse in Southeast Asia* 1 , 1(2), 2. https://doi.org/10.15294/ildisea.v1i1.56874

[6] Firmansyah. (2017). Problematika Tindak Pidana ITE Dalam Persfektif Sistem Hukum, *MalRev*, 1(2), 105. https://doi.org/10.31850/malrev.v1i2.31

[7] Firmansyah. (2023). Fenomena Demostrasi Anarki Diindonesia,

Sebuah Tinjauan Kritis Persfektif Sosiologi Hukum. *MalRev*, Vo.7(1), 27. https://doi.org/10.31850/malrev.v7i1.2433

[8] Habibi, M R., Isnatul Liviani. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Al-Qanun*, 23(2), 407. https://doi.org/10.15642/alqanun.2020.23.2.400-426

[9] Hartanto, dkk. (2024). Perbandingan Hukum Pidana Tentang Ujaran Kebencian Di Indonesia, Malaysia Dan Norwegia, *HUKMY*, 4(1), 519. https://doi.org/10.35316/hukmy.2024.v4i1.518-534

[10] Hartanto. (2023). Meaningfull Justice Decision of Grant Funding Criminal Corruption Cases. *Pakistan Journal of Criminology,* 15(4), 697. -

[11] Indonesia, R. (1946). Kitab Undang-undang Hukum Pidana (KUHP) – *WvS*

[12] Indonesia, R. (1999). UU. No. 36 tentang 1999 tentang Telekomunikasi

[13] Indonesia, R. (2016). UU. No.19 Tahun 2016 tentang Perubahan UU. No 11 Tahun 2008 tentang ITE

[14] Indonesia, R. (2018). UU. No. 5 Tahun 2018 tentang Pemberantasan Terorisme

[15] Indonesia, R. (2021). Keputusan Bersama Menteri Komunikasi Dan Informatika RI, Jaksa Agung RI, Dan Kapolri, No. 229 Tahun 2021, No. 154 Tahun 2021 No. KB/2/VI/2021 Tentang Pedoman Implementasi Pasal Tertentu

[16] Indonesia, R. (2023). UU No. 1 Tahun 2023 tentang KUHP

[17] M. Moh. Yusuf D., Addermi, A., Jasmine Lim. (2022). Kejahatan Phising dalam Dunia Cyber Crime dan Sistem Hukum di Indonesia. *Jurnal Pendidikan dan Konseling*, 4(5), 8018-8019. https://doi.org/10.31004/jpdk.v4i5.7977

[18] Pratama, Y. dkk. (2022). Cybercrime: The Phenomenon of Crime through the Internet in Indonesia. *International Conference Restructuring and Transforming Law*, 1(1), 298. DOI -

[19] Raharjo, A. (2002). *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi Tinggi*, Bandung: Citra Aditya Bakti, 29

[20] Suseno. S. (2012). *Yurisdiksi Tindak Pidana Siber*. Bandung: Refika Aditama, 125

[21] Thantawi, “Perlindungan Korban Tindak Pidana Cyber Crime - Sistem Hukum Pidana Indonesia,” *Jurnal Ilmu Hukum*, Vol.2, No.1. 2014

[22] Wahid, A. dan M. Labib. (2005). *Kejahatan Mayantara (Cyber Crime)*, Bandung: Refika Aditama, 146