International Journal of Social Science And Human Research

ISSN(print): 2644-0679, ISSN(online): 2644-0695

Volume 04 Issue 02 February 2021

DOI: 10.47191/ijsshr/v4-i2-04, Impact factor-5.586

Page No : 141-147

Development of Cyber Crime and its Regulations in Indonesia

Muhammad Iqbal[1], Nyoman Serikat Putra Jaya[2]

[1]Mater of law, Universitas Diponegoro Semarang Jl.Imam Barjo, S.H. No.1-3 Kampus UNDIP Pleburan-Semarang 50241
[2]Faculty of Law, Universitas Diponegoro, Jalan Prof Sudarto, No. 1 Semarang

ABSTRACT: The development of information technology is like "two sides of the sword," because, on the one hand, it brings convenience, speed in doing work. Still, on the other hand, it raises legal problems that are done using information technology. This problem is called Cyber Crime. This article was prepared to discover the development of information technology, the development of Cyber Crime in Indonesia, and its arrangements in Indonesia. The research method used is normative juridical, using secondary data consisting of primary legal material, namely legislation related to Cyber Crime and examples of Cyber Crime cases in Indonesia. This study also uses secondary legal materials, namely books and journals related to Cyber Crime. The legal documents were collected through a literature study and analyzed descriptively analytically. Based on the research results, it is known that the necessary statutory provisions of the Cyber Crime are in the "Criminal Code, Law Number 11 the Year 2008 concerning Information and Electronic Transactions, Law Number 19 the Year 2002 Regarding Copyright, Law Number 15 the Year 2002 Regarding Money Laundering Crimes".

KEYWORDS: Cyber crime, technology development, criminal law.

INTRODUCTION

The practice of human life has always been developing from time to time, one of which is influenced by advances in information technology (information technology), which plays a vital role in human life. Information technology can trigger and spur changes in the social and economic needs of the community, previously towards electronic transactions or socialization (Budi Suhariyanto, 2012). The development of information technology has made society more likely to experience changes in current needs. Many human civilizations have been caused by the development of technology, especially information technology via the internet; human civilizations have been exposed to new phenomena with the presence of information technology (Dikdik M, Arief Mansur dan Elisatris Gultom, 2005). Human civilization is also faced with human needs, which are increasingly developing.

The presence of information technology such as the internet in human life today has had both good and bad impacts; on the one hand, information technology has been able to meet human needs as a place to obtain information to carry out their life activities. But on the other hand, information technology also hurts human life; this makes information technology like "two sides of the sword." The development of information technology, especially internet media technology, not only fulfills the needs and provides comfort for people who want something practical but also causes the emergence of new types of crimes, namely by utilizing computers and internet media as the modus operandi. Through the internet media, several types of criminal acts are easier to do, such as data manipulation, espionage, sabotage, provocation, money laundering, hacking, software theft or hardware destruction and gambling crimes using the internet media (Agus Rahardjo, 2002).

Information technology, which is essentially a tool for humans, has now become an autonomous force that shackles the behavior and lifestyle of humans themselves. Its power is enormous because robust social systems also support it, and at an ever-increasing speed, technology has become the direction of human life. People with low technological capabilities tend to depend and can only react to the impact caused by technological sophistication. The impact of advances in information technology on cybercrime in Indonesia is indeed a serioseverelem. However, to determine an act as a criminal act, a criminal policy must be used, which by Sudarto is a reasonable attempt by the community to overcome crimes. This criminal policy includes a criminal law policy referred to as a crime prevention policy with criminal law (penal policy). In addition to criminal law, it can be done with other means (non-criminal law). Criminal law's function as social control is used to tackle crimes in the form of violations of norms related to the use of potentially criminal information technology to protect the public from the dangers of these crimes (Sudarto, 1981).

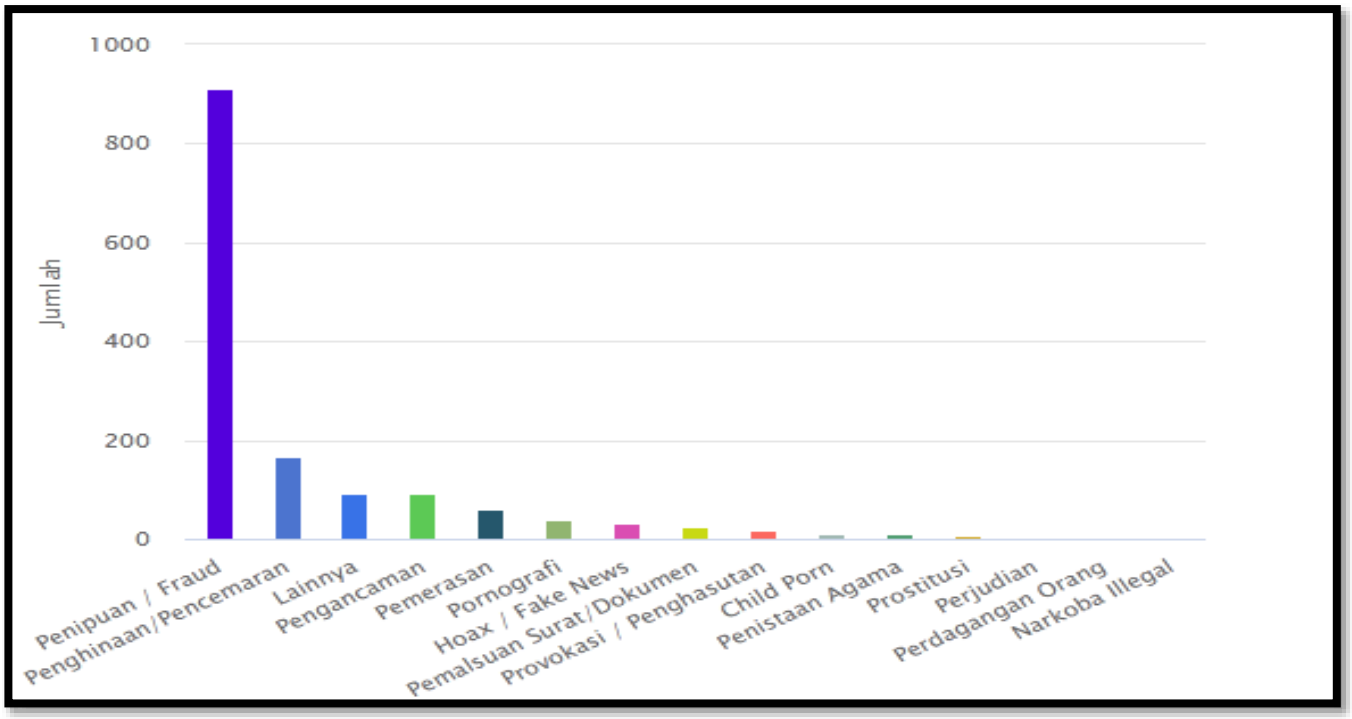
Information technology users in Indonesia are large in number, this can be seen from the data released by APJII (Indonesian Internet Service Provider Association) that the number of internet service users in Indonesia as of September 2019 was 171.2 million users (APJII, 2019). The widespread use of the internet in various life areas often creates legal problems such as fraud, theft, burglary, and data damage by spreading viruses and others. "Users of internet services often experience various problems; this is because the

rules of the game in cyberspace are not clear; besides that, it is also a result of the insecure system in internet settings. In reality, cyberspace development cannot be prevented, not only across regions but also by penetrating national borders. Transactions carried out through the internet are not legally accessible (Iman Sjahputra Tungal, Pandapotan Simorangkir, dan G. Windarto, 2002).

About the development of cyberspace, cybercrime, which occurs in cyberspace, is a severe problem of human life. Cyber Crime is a criminal act committed by utilizing information technology. Experts have put forward various definitions, but there is no uniformity of these definitions. Technically, these crimes can be divided into offline crime, semi online crime, Cyber Crime (Stefano Caneppele dan Marcelo F Aebi, 2019). Each has its characteristics, but the main difference between the three is the connection with the public information network. Cyber Crime is a further development of crimes or criminal acts committed by utilizing computer technology (Harol Agusto Manurung, Nuswantoro Dwi Warno, dan Joko Setiyono, 2016).

Based on data from the Directorate of Cyber Crime, Bareskrim Polri, the total number of public complaints regarding Cyber Crime acts up to July 2020 is 1,475 complaints. The details regarding public complaints can be seen in Figure 1.

Figure 1. Public Complaints



Source: Directorate of Cyber Crime, Bareskrim Polri

It can be seen that the most frequently complained of cybercrime is fraud or fraud, and the second most is defamation or defamation. The data show that "as the progress and development of science and technology in society, so doe's crime development. The crimes committed have taken advantage of and exploited the opportunities provided by modern instruments' convenience with sophisticated equipment, no longer traditionally. Such crimes are crimes with new dimensions (Sabar Slamet, 2015). This term is to indicate a crime related to the development of society in the economic sector in industrial society; the perpetrators consist of the wealthy, intellectual, organized (including white-collar crime) (Clinten Trivo Loah, 2020). High crime mobility is carried out within an area and between regions, even crossing regional and transnational boundaries. The modes of operation use sophisticated equipment, taking advantage of the legal system's weaknesses, management system.

Currently, Cyber Crime has developed not only as a criminal act in the national scope. Still, it has entered the category of international criminal acts because Cyber Crime knows no jurisdiction boundaries to escape lawsuits for crimes committed (Roni Gunawan Raja Gukguk dan Nyoman Serikat Putra Jaya, 2019).

Such actions can complicate efforts to investigate, prosecute, and examine in court proceedings or even implement court decisions. This criminal act has even resulted in the emergence of legal problems from one country to another, so that efforts to overcome and eradicate it are difficult to do without cooperation and harmonization of policies with other countries (Bambang Hartono dan Recca Ayu Hapsari, 2019). So that the prevention and eradication of Cyber Crime, international cooperation must be carried out, and there is a need for good relations between countries in the world to work hand in hand in the context of mitigating and eradicating Cyber Crime, which is transnational; this, of course, must be based on their respective laws country.

Cyber Crime is a sour fruit for the advancement of human civilization in modern times like today. The existence of Cyber Crime endangers and threatens the lives of modern humans in general, including Indonesian society. "The bad result of the rapid

advancement of information technology is the increase in incidents of computer crime, pornography, digital terrorism, junk information, biased information or hoaxes, hackers, crackers, and so on." Therefore, the rapid development of information technology must be regulated and monitored to prevent the emergence of various kinds of crimes that exploit and result from the development of information technology.

RESEARCH PROBLEM

Based on the explanation above, the problem's formulation can be as follows: How is the development of Cyber Crime in Indonesia? How is the Cyber Crime legal arrangement in Indonesia?

RESEARCH METHOD

This research is a normative legal research, using secondary data consisting of primary legal materials. (Kornelius Benuf dan Muhamad Azhar, 2020). Namely, the laws and regulations regarding Cyber Crime in Indonesia and other related laws and regulations. This study also uses secondary legal materials, namely books and journals on Cyber Crime. This study's data and legal materials are collected through a literature study, then analyzed descriptively and analytically (Soerjono Soekanto dan Sri Mamudji, 2001), to answer research problems.

DISCUSSION

Development of Cyber Crime in Indonesia

The development of Cyber Crime begins with discovering computers until discovering information technology, namely the internet, the internet's existence, creating a new world for humans to interact with besides the real world, namely the virtual world. The real world has a mechanism of interaction between humans that is different from the virtual world. If humans interact directly in the real world, namely between humans and humans, in the virtual world, human interaction is carried out between machine-to-machine (Ikhsan Yusda PP , 2015). The development of information technology, in this case, computers and the internet, has changed communication between humans; if it was done face to face or in-person, now with the development of information technology, humans can interact through cyberspace.

The increase in the benefits gained from the use of information technology has led to an increase in the number of users of information technology, increasing the value of the virtual world economy (Sri Redjeki Hartono, 1995). The number of requests and strong desires for the use and utilization of information technology makes information technology a place to reap profits, thus opening up opportunities for some people to use all the means they can to get by seizing others' rights for personal gain. The method in question is, for example, committing fraud through information technology (Melisa Sumenge, 2013)., spreading fake news through social media (Ahmad Budiman, 2017), theft of personal data for interests that are detrimental to the owner of personal data (Kornelius Benuf, Siti Mahmudah, dan Ery Agus Priyono, 2019)., etc. In addition to pursuing material or monetary gain, Cyber Crime perpetrators commit crimes to get a challenge; what the perpetrator thinks is how to trick the computer system into enjoying the results (Muhammad Prima Ersya , 2017).

Because people's activities in cyberspace are not orderly and even tend to be detrimental to one another, the Government "responds to this that the government has begun to enact laws and regulations to curb community activities. "These regulations, known as cyberlaw, are expected to serve as legal and moral boundaries for all cyberspace, known as cyber law is expected to serve as legal and moral boundaries for all cyber users, to protect them from all forms of Cyber Crime (Nandang Sutrisno, 2001). The existence of a computer network that connects all parts of the world is a human effort to overcome limitations because the time and space of the world are Flat is the right line in describing our world's condition. The virtual world knows no national boundaries, and all activities that occur in space occur in real-time (Fredy Susanto, Muhammad Nur Rifai, dan Adlah Fanisa, 2017). Countries take advantage of this opportunity to advance their economic interests of national value. Increased regional and international trade is carried out in cyberspace to get higher profits. Indonesia, as a member of the international community, is influenced by the same conditions as the Indonesian government, therefore, must start preparing various things that can ensure good and safe cyber interactions by the values and norms that are embraced by the Indonesian people.

The development of information technology has encouraged the emergence of new crimes. Types of crime are growing and varying; many new crimes are emerging with the development of technology, especially internet technology (Rudi Hermawan, 2013). Cybercrime is a new form or dimension of crime today caused by the rapid development of technology. This crime has even become an international concern. Cybercrime is one of the dark sides of technological progress, which has a far-reaching negative impact on all areas of modern life today (Ineu Rahmawati, 2017). Cyber Crime stems from hacking activities that have existed for more than a century. In the 1870s, several teenagers had tampered with the country's new telephone system by changing authorities. The following will show you how busy hackers have been over the last 35 years. Early 1960 University facilities with a large computer mainframe, such as MIT's artificial intelligence laboratory, became an experimental stage for hackers". In the early days, the word "hacker" meant positively for a computer-savvy person who could create a program beyond what it was designed to do its job. Research on the forms of cybercrime was also carried out by Stanford Research International (SRI) in the United States from 1971

to 1985. The research found 1600 cases that occurred since 1958 and public and government reactions to them, including settlement based on civil law. In 1979 SRI obtained more valid data, namely stating that of the 244 cases that occurred, 191 could be brought to court, and the defendant from 161 cases could be convicted. The studies conducted in the 1970s were unable to show the data regarding the regulation of criminal law clearly, so they had not been included in the criminal statistics (Suroso, 2007).

In Indonesia, in January 2000, several sites Indonesia were scrambled by a cracker called Fabian Clone and naisedoni. Sites that were attacked include the Jakarta Stock Exchange, BCA, Indosatnet. Apart from these large sites, many other sites are not reported (Dodo Zaenal Abidin , 2017). Later in the same year, an Indonesian cracker was caught in Singapore while trying to break into a Singapore company. In September and October 2000, after successfully breaking into Bank Lippo, the Fabian Clone was back in action by breaking into the Bank's web. Please note that both of these banks provide internet repair services (Internet Banking). In September 2000, the police received many reports from abroad about Indonesian users trying to deceive other users on websites that provide auction transactions such as eBay. Then on 24 October 2000, two internet cafes (warnet) in Bandung were attacked by the police because they used a stolen dialup account from the Centrin ISP. One of the internet cafes was online using the stolen account. June 2001 An Indonesian internet user-created several websites similar to the klikbca.com site, which BCA used to provide internet banking services. Sites created using a domain name similar to klikbca.com, and many other examples(Dodo Zaenal Abidin , 2017). The impact of credit card crimes committed through online transactions by Indonesian carders has made several online merchants in the US and Australia blacklist Indonesia (Sri Wulandari, 2019). There is even a strong suspicion that the FBI (Federal Bureau of Investigation) targets several cities in Indonesia as direct monitoring. This happens because carders are on par with hackers and crackers, harming some foreign parties, as happened in Yogyakarta. The Yogyakarta Special Region Police arrested five carders and secured evidence worth tens of millions obtained from overseas merchants (Yuslia Naili Rahmah, 2018).

Based on the court's decision, Cyber Crime had occurred in Indonesia since 1983, namely the Bank Rakyat Indonesia (BRI) branch of Brigadier General Katamso Yogyakarta in 1986 when Bank Negara Indonesia (BNI 1946) was burglary by using computer facilities. In 1989, the Bali bank burglary occurred with the suspect, Budiman Hidayat. In 1990 there was Cyber Crime in Bandung, which was an illegal copy of the Word Star version 5.0 program, (Aloysius Wisnubroto , 1999), in the following years in Indonesia, there were many Cyber Crimes, for example, cracking, namely "accessing computers without permission by the owner credit card fraud (Hardianto Djanggih , 2013).

Theft of personal data these days is an issue that is widely discussed by legal practitioners and legal academics. Along with the development of information technology in Indonesia, many digital business actors carry out their business activities by utilizing personal data without the owner's consent. However, witnesses against business actors who did this were limited to administrative sanctions in the form of; Oral warnings, written warnings, temporary suspension of activities, announcements on websites in the network (online website) (Laksono Daniel Christian Hutagalung, 2019). The development of Cyber Crime in Indonesia in terms of personal data theft in Indonesia cannot be subject to criminal witnesses. Even though there are regulations in the Criminal Code regarding "Theft," there is a specialist lex principle that overrides general law by using special laws.

Regulation of Cyber Crime in Indonesia

The regulation of Cyber Crime in Indonesia, specifically in the law, does not exist. However, several favorable laws in Indonesia can be used to trap cybercrime perpetrators in Indonesia. These favorable laws will be described in the following sections, from the most general to the most specific, but not to the extent that they specifically regulate Cyber Crime. The favorable laws are as follows; First, namely, the "Criminal Code," the articles in the Criminal Code are usually used more than one Article because it involves several actions as well as the Articles that can be imposed in the Criminal Code on Cyber Crime, namely:

a. Article 362 of the Criminal Code is imposed for carding cases where the perpetrator steals another person's credit card number, even though not physically because only the card number is taken by using card generator software on the Internet to make transactions e-commerce. After the transaction is made and the goods are shipped, the seller who wants to withdraw the bank's money is rejected because the card owner is not the person who made the transaction.
b. Article 378 of the Criminal Code can be imposed for fraud by pretending to offer and sell a product or goods by placing an advertisement on one of the websites to be interested in buying it and then sending money to the advertiser. But, in reality, the item doesn't exist. This is known after the money is sent and the goods ordered do not arrive so that the buyer is deceived.
c. Article 335 of the Criminal Code can be imposed for cases of threats and extortion carried out via e-mail sent by the perpetrator to force the victim to do something according to what the perpetrator wants. If it is not implemented, it will have a dangerous impact. This is usually done because the perpetrator knows the victim's secret.
d. Article 311 of the Criminal Code can be imposed for cases of defamation using Internet media. The mode is that the perpetrator spreads an email to the victim's friends about a story that is not true or sends an email to a mailing list so that many people know the story.
e. Article 303 of the Criminal Code can be imposed to ensnare gambling games conducted online on the Internet with Indonesia organizers.

f. Pasal Article 282 of the Criminal Code can be imposed to distribute pornography and pornographic websites that are widely circulated and easily accessible on the Internet. Even though they are in Indonesian, it is tough to take action against the perpetrators because they register the domain abroad where pornography featuring adults is not a prohibited thing or illegal.
g. Articles 282 and 311 of the Criminal Code can be applied to cases of spreading vulgar personal photos or films on the Internet, for example, cases of pornographic videos of students, workers, or public officials.
h. Articles 378 and 262 of the Criminal Code can be applied to carding cases because the perpetrator commits fraud as if he wants to buy an item and pay with his credit card whose credit card number is stolen.
i. Article 406 of the Criminal Code can be imposed in cases of defacing or hacking that make someone else's system, such as a website or program, become malfunctioning or can be used properly.

Second, namely Law No. 19 of 2002 concerning Copyright, According to Article 1 number (8) of Law No. 19 of 2002 concerning Copyright, a computer program is a set of instructions that are manifested in the form of language, code, scheme or other forms When combined with media that can be read by a computer, it will be able to make the computer work to perform particular functions or to achieve extraordinary results, including preparation in designing these instructions. Copyright for computer programs is valid for 50 years (Article 30).

The very high price of computer programs/software for Indonesian citizens is a promising opportunity for business people to duplicate and sell pirated software at low prices. For example, a $ 50 antivirus program can be purchased for IDR 20,000.00. Compared to the original software, sales at low prices resulted in enormous profits for the actors because the capital issued was not more than Rp. 5,000.00 per chip. The rise of software piracy in Indonesia, which seems understandable, is, of course, very detrimental to copyright owners. The act of pirating a computer program is also a criminal offense as regulated in Article 72 paragraph (3), namely, anyone who deliberately and without rights reproduces the use of a computer program for commercial purposes shall be punished with imprisonment of 5 (five) years and a maximum fine. A lot of IDR 500,000,000.00 (five hundred million rupiah).

The third is Law Number 11 of 2008 concerning Electronic Information & Transactions. This law, which was ratified and promulgated on April 21, 2008, although to date there has not been a PP regulating the technical implementation of it, it is hoped that it can become a cyber law or cyberlaw to ensnare Cyber Crime perpetrators irresponsible and become a legal umbrella for people who use information technology to achieve legal certainty.

a. Article 27 of the 2008 ITE Law: Everyone knowingly and without right distributes and/or transmits and / or makes accessible electronic information and / or electronic documents that have contents that violate decency. The criminal threat of article 45 (1) of the Criminal Code. The maximum imprisonment is 6 (six) years and / or a maximum fine of Rp. 1,000,000,000.00 (one billion rupiah). It is also regulated in the Criminal Code Article 282 concerning crimes against decency.
b. Article 28 of the 2008 ITE Law: Every person knowingly and without right spreads false and misleading news that results in consumer losses in electronic transactions.
c. Article 29 of the 2008 ITE Law: Anyone who knowingly and without rights sends electronic information and / or electronic documents containing threats of violence or intimidation, directed personally (Cyber Stalking). Criminal threat article 45 (3) Every person who fulfills the elements referred to in article 29 shall be sentenced to imprisonment of up to 12 (twelve) years and / or a maximum fine of Rp. 2,000,000,000.00 (two billion rupiah).
d. Article 30 of the ITE Law of 2008 paragraph 3: Every person intentionally and without rights or against the law accesses computers and / or electronic systems in any way by violating, breaking through, bypassing, or breaking into security systems (cracking, hacking, illegal access). Every person who complies with the elements referred to in Article 30, paragraph 3, shall be punished with imprisonment for a maximum of 8 (eight) and / or a maximum fine of Rp. 800,000,000.00 (eight hundred million rupiah).
e. Article 33 of the 2008 ITE Law: Every person intentionally and without rights or against the law takes any action which results in disruption of the electronic system and/or results in the electronic system not working correctly.
f. Article 34 of the 2008 ITE Law: Everyone knowingly and without rights or against the law produces, sells, procures for use, imports, distributes, supplies, or owns.
g. Article 35 of the 2008 ITE Law: Every person intentionally and without right or against the law manipulates, creates, changes removes, destroys electronic information and / or electronic documents to make the electronic information and / or electronic documents appear to be authentic (phishing = site fraud).

Fourth, namely Law Number 15 of 2002 concerning the Crime of Money Laundering is the most powerful law for an investigator to obtain information on suspects who have committed fraud via the Internet, because it does not require lengthy and time-consuming bureaucratic procedures, because fraud is one of the types of crime included in money laundering (Article 2 Paragraph (1) Letter q). Investigators can ask the bank retro receive transfer to provide the suspect's identity and banking data without ha following the regulations as stipulated in the Banking Law. In the Banking Law, identity and banking data are part of bank secrecy. suppose the investigator needs such information and data. In that case, the procedure that must be done is to send a letter from the Kapolda to

the Chief of Police to be forwarded to the Governor of Bank Indonesia. This procedure takes a long time to obtain the desired data and information.

CLOSING

Conclusion

Cyber Crime has occurred in Indonesia since 1983, namely the case of the Bank Rakyat Indonesia (BRI) branch of Brigadier General Katamso Yogyakarta, in 1986 the Bank Negara Indonesia (BNI 1946) burglary occurred by using computer facilities until now the development of Cyber Crime is increasingly rapid, many types of new crimes that have arisen due to developments in information technology such as; Hoaxes, fraud, insults, threats, theft of personal data, pornography, and more. There is no specific regulation on Cyber Crime; there are rules in general, namely in the Criminal Code Article 282, article 303, article 311, article 335, article 362, article 378, and article 406. Law Number 11 of 2008 regarding information: article 1 number 8, article 72 paragraph 3 and Electronic Transactions, Law Number 19 the Year 2002 concerning Copyright, Law Number 15 the Year 2002 Concerning the Crime of Money Laundering.

Recommendation

Based on the research and discussion results described above, the authors provide suggestions to two parties, namely, to all Indonesian people and the government as the regulator. Suggestion to all Indonesian people is to use information technology for beneficial and not detrimental things by the values that develop in Indonesian society. To the government as the regulator, the author suggests that the regulation of Cyber Crime in Indonesia is still behind the development of information technology and the types of crimes in cyberspace today, so it is necessary to establish a broad and flexible rule so that it can continue to be relevant to the times.

BIBLIOGRAPHY

Book

M, Dikdik, Mansur, Arief dan, Elisatris Gultom. Cyber Law Aspek Hukum dan Teknologi Informasi. Bandung: Tiga Serangkai, 2005.

Rahardjo, Agus. Cyber Crime-Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi. Bandung: Citra Aditya Bakti, 2002.

Suhariyanto, Budi. Tindak Pidana Teknologi Informasi (Cyber Crime). Jakarta: PT. RajaGrafindo Persada, 2012.

Tungal, Iman Sjahputra, Pandapotan Simorangkir, dan G. Windarto. Problematika Hukum Internet Indonesia. Jakarta: Prenhallindo, 2002.

Wisnubroto, Aloysius. Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer. Yogyakarta: Penerbitan Universitas Atma Jaya, 1999.

Skripsi/Thesis/Disertasi

Suroso. Kebijakan Kriminal Cyber Crime Terhadap Anak (Tinjauan Dalam Prespektif Hukum Dan Pendidikan Moral). Thesis. Semarang: Magister Ilmu Hukum Universitas Diponegoro, 2007.

Journal

1) Abidin, Dodo Zaenal. "Kejahatan dalam Teknologi Informasi dan Komunikasi." Jurnal Processor 10, no. 2 (2017): 509-516.
2) Benuf, Kornelius dan Azhar, M. "Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer." Gema Keadilan 7, no. 1 (2020): 20-33.
3) Benuf, Kornelius, Mahmudah, Siti dan Priyono, Ery Agus. "Perlindungan Hukum Terhadap Keamanan Data Konsumen Financial Technology di Indonesia." Refleksi Hukum: Jurnal Ilmu Hukum 3, no. 2 (2019): 145–160.
4) Budiman, Ahmad. "Berita bohong (hoax) di media sosial dan pembentukan opini publik." Majalah Info Singkat Pemerintahan Dalam Negeri Isu Aktual 9, no. 1 (2017): 17-20.
5) Caneppele, Stefano dan Aebi, Marcelo F. "Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes." Policing: A Journal of Policy and Practice 13, no. 1 (2019): 66-79.
6) Djanggih, Hardianto. "Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana Cyber Crime di Bidang Kesusilaan." Jurnal Media Hukum I, no. 22 (2013): 57-77.
7) Ersya, Muhammad Prima. 2017. "Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia." Journal of Moral and Civic Education 1, no. 1 (2017): 50-62.
8) Hartono, Bambang dan Hapsari, Rebecca Ayu. "Mutual Legal Assistance pada Pemberantasan. Cyber Crime Lintas Yurisdiksi di Indonesia." Jurnal Sasi 25, no. 1 (2019): 59-71.

9) Harol Agusto Manurung, Warno, Nuswantoro Dwi dan Setiyono, Joko. "Analisis Yuridis Kejahatan Pornografi (Cyber Porn) Sebagai Kejahatan Transnasional." Diponegoro Law Review 3, no. 5 (2016): 2.
10) Hartono, Sri Redjeki. Perspektif Hukum Bisnis Pada Era Teknologi. Semarang: Undip Pers, 1995.
11) Hermawan, Rudi. "Kesiapan Aparatur Pemerintah Dalam Menghadapi Cyber Crime di Indonesia." Faktor Exacta 6, no. 1 (2013): 43-50.
12) Loah, Clinten Trivo. "Penegakan Hukum Terhadap Pelaku Tindak Pidana White Collar Crime." Lex Crimen 8, no. 12 (2020): 82-89.
13) PP, Ikhsan Yusda. "Analisis Terhadap Cyber Crime Dalam Kaitannya Dengan Asas Territorialitas." Jurnal TEKNOIF 3, no. 1 (2015): 48.
14) Rahmah, Yuslia Naili. "Pengaruh Penggunaan Internet Banking Dan Perlindungan Nasabah Pengguna Fasilitas Internet Banking Terhadap Cyber Crime Di Daerah Istimewa Yogyakarta." Jurnal Pendidikan dan Ekonomi 7, no. 6 (2018) : 580.
15) Rahmawati, Ineu. "The Analysis of Cyber Crime Threat Risk Management to Increase Cyber Defense." Jurnal Pertahanan & Bela Negara 7, no. 2 (2017): 37-52.
16) Roni Gunawan Rajagukguk dan Nyoman Serikat Putra Jaya. "Tindak Pidana Narkotika Sebagai Transnasional Organized Crime." Jurnal Pembangunan Hukum Indonesia 1, no. 3 (2019): 337-351.
17) Slamet, Sabar. "Politik Hukum Pidana Dalam Kejahatan Perkosaan." Yustisia Jurnal Hukum 4, no. 2 (2015): 478.
18) Soekanto, Soerjono dan Mamudji, Sri. Penelitian Hukum Normatif Suatu Tinjauan Singkat. Jakarta: Raja Grafindo Persada, 2001.
19) Sudarto. Hukum, dan Hukum Pidana. Bandung: Alumni, 1981.
20) Sumenge, Melisa. "Penipuan Menggunakan Media Internet Berupa Jual-Beli Online." Lex Crimen 2, no. 4 (2013): 102
21) Susanto, Fredy, Rifai, Nur Muhammad dan Fanisa, Adlah. "Internet of Things Pada sistem keamanan ruangan, studi kasus ruang server Perguruan Tinggi Raharja." Semnasteknomedia Online 5, no. 1 (2017): 4.
22) Sutrisno, Nandang. "Cyberlaw: Problem dan Prospek Pengaturan Aktivitas Internet." Jurnal Hukum IUS QUIA IUSTUM 8, no. 16 (2001): 34
23) Sri Wulandari. "Perlindungan Hukum Bagi Nasabah Perbankan Terhadap Kejahatan Kartu Kredit." Hukum dan Dinamika Masyarakat 17, no. 1 (2019): 30.

Internet or website

1) APJII. "Pengguna Internet di Indonesia," 2019. http://apjii-jumlah-pengguna-internet-di-indonesia-tembus-171-juta-jiwa.
2) Laksono Daniel Christian Hutagalung. "Langkah Hukum terhadap Pencurian Data Pribadi (Identity Theft)." Hukumonline, 5 November 2019. https://www.hukumonline.com/klinik/detail/ulasan/lt5d904597bfa6e/langkah-hukum-terhadap-pencurian-data-pribadi-iidentity-theft-i/