International Journal of Contemporary Sciences (IJCS)
Vol. 1, No. 10, 2024: 635-648

Crimes In Information and Communication Technology Against the Environment

Fajar Khaify Rizky
Universitas Sumatera Utara
Corresponding Author: Fajar Khaify Rizky fajarkhaifirizki89@gmail.com

A R T I C L E I N F O

Keywords: Environmental Crime, Cyber Crime, Information, Communication Technology

Received : 7 July
Revised : 15 July
Accepted: 22 August

A B S T R A C T

This research will discuss the substance relating to environmental crimes contained in Law No. 32 on Environmental Protection and Management, whether Cyber Crime in its application is related to environmental crimes that cause pollution and / or environmental damage, because in the process of activity and management of natural resources whose perpetrators are subjects of environmental law in the form of companies in the form of legal entities or non-legal entities will utilize technology and information via the internet for their activities. This research uses normative legal research methods with qualitative methods. Cybercrime is related to environmental crimes contained in Law Number 32 of 2009 concerning Environmental Protection and Management, including environmental crimes committed by corporations, and falsification of data via the internet on manifest waste and other polluting materials that result in losses to the community and the environment

DOI: https://doi.org/10.55927/ijcs.v1i10.11050
E-ISSN: 3047-4078
https://journal.formosapublisher.org/index.php/ijcs

INTRODUCTION

Changes in the external environment of education, ranging from the social, economic, technological, to political environment require education to rethink how these changes affect it as a social institution and how to interact with these changes. One of the environmental changes that greatly affects the world of education is the presence of information technology (IT).

Information and Communication Technology is an important element in the life of the nation and state. The role of information technology in human activities at this time is so great. Information technology has become the main facility for the activities of various sectors of life where it contributes greatly to fundamental changes in the structure of operations and management of organizations, education, transportation, health and research. Therefore it is very important to improve the ability of ICT human resources (HR), ranging from skills and knowledge, planning, operation, maintenance and supervision, as well as improving the ICT capabilities of leaders in government agencies, education, companies, SMEs (small and medium enterprises) and NGOs. So that in the end it will produce outputs that are very beneficial both for humans as individuals themselves and all sectors of life. (Ibnu Rusydi, 2017, p. 1829-7463).

The tools associated with information technology are computer networks as a medium for providing information, through the internet also the activities of the commercial community become the largest part, and the fastest growth and penetrate various national borders. Even through this network, market activities in the world can be known for 24 hours. Through the internet world or also called cyberspace anything can be done. The positive aspect of this virtual world certainly adds to the trend of world technological development with all forms of human creativity, but the negative impact is inevitable. When pornography is rampant in the Internet media, society cannot do much. (Eliasta Ketaren, 2016, p. 35).

Internet has become one of the obligations in life today. The convenience offered by the Internet is increasingly making people complacent. The Internet connects every user. There are no restrictions on time, region or gender. Information Technology today seems to be a double-edged sword, because in addition to contributing to the improvement of progress, welfare, and human civilization, it is also an effective means of unlawful acts.

LITERATURE REVIEW

The negative impact of internet technology has led to the emergence of a crime called cybercrime or crime through the internet. The emergence of several cybercrime cases, such as credit card theft, hacking several sites, intercepting other people's data transmissions, for example email and manipulating data by setting up unwanted commands into the computer. (Alcianno G. Gani, 2019, p. 17). The definition of cybercrime is the forms of crime that arise due to the use of internet technology. According to Andi Hamzah, cybercrime is a crime in the field of computers, which can generally be interpreted as illegal use of computers. (Andi Hamzah, 1989, p. 67). Cybercrime is a new and unprecedented threat to the global community. Hacking, cracking, defacing, sniffing, carding, phishing, spam, or scamming are some of the most dangerous internet crimes that have caused real harm to many parties. (Andri Winjaya Laksana, 2019, p. 53).

This crime can also be qualified by material offences and formal offences. The material offence is the act of any person who causes harm to another person, and the formal offence is the act of any person in this case entering another person's computer without permission. The legal consequences of such crimes will be a threat to stability, so that in the settlement process it is very difficult to keep up with the techniques of crimes committed with computers, especially internet and intranet networks. (Alcianno G. Gani, 2019, p. 17).

In the face of the outbreak of cybercrime in Indonesia, the Government of the Republic of Indonesia on 2 January 2024 ratified the enactment of the Law on Electronic Information and Transactions (ITE) Law Number 1 of 2024 concerning Electronic Information and Transactions which aims to provide 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 utilizing information technology. This paper will discuss cybercrime with environmental crimes contained in Law Number 32 of 2009 concerning Environmental Protection and Management, whether the two forms of crime complement each other.

METHODOLOGY

The research method used in this paper is normative legal research, where normative legal research is a scientific research procedure to find the truth based on scientific logic viewed from its normative side. Normative legal research is also a scientific activity, which is based on certain methods, systematics and thoughts that aim to study one or several certain legal symptoms by analyzing them.

This research is conducted by collecting and examining library materials and secondary data in the form of legal materials consisting of laws and regulations, books, papers, journals, scientific works, the internet and so on relating to crimes in information and communication technology against the environment.

Data collection techniques and tools in this paper use data collection techniques through library research. Data collection tools from data collection techniques through library research, namely analyzing legal materials obtained through library research in the form of tabulated secondary data which is then systematized by selecting legal instruments that are relevant to the object of research. Furthermore, the legal materials analyzed are synchronized with the topics and problems in this research related to crimes in information and communication technology against the environment.

The data analysis method used in testing and finding answers to the problems of this paper is a qualitative data analysis method, after the research data or legal materials needed in this research are collected properly, then further analysis will be carried out.

RESULTS AND DISCUSSION

Cyber Crime

As has been stated, cybercrime is a form of crime that arises from the utilization of internet technology. There are several opinions about cybercrime, namely:

a. Cybercrime is a criminal act committed using computer technology as the main crime tool. It is a crime that utilizes the development of computer technology, especially the internet.
b. Cybercrime as an act that violates the law and the actions taken can threaten and damage information technology infrastructure, such as illegal access, attempts or actions to access part or all parts of a computer system without permission and the perpetrator does not have the right to access. (Nurul Puspita Dewi, 2009, p. 3).
c. The US Department of Justice defines computer crime as … "any illegal act requiring knowledge of computer technology for its perpetration, investigation or prosecution". Another definition is given by Organization of European Community Development, i.e.: "any illegal, unethical or unauthorized behavior relating to the automatic processing and/or the transmission of data". Andi Hamzah in his book Criminal Aspects in the Computer Field (1989) defines: "crimes in the field of computers can generally be interpreted as illegal use of computers". (NCB-Interpol Indonesia, 2019).

From some of the above definitions, it can be seen that cybercrime is an unlawful act, related to unlawful acts regulated in Article 1365 of the Civil Code, namely: "Every act that violates the law and brings harm to another person, obliges the person who causes the loss due to his fault to replace the loss", which is carried out using the internet based on the sophistication of computer and telecommunications technology is a tort as in the Civil Code.

Characteristics of Cybercrime

Cybercrime is a crime, which has its own characteristics that are different from conventional crime. Conventional crime is known for 2 types of crime, among others: (Etika Profesi IT, 2020).

a. *Blue collar crime*
   This type of crime is a conventional type of crime or criminal offence, such as robbery, theft, and others. The perpetrators of this type of crime are usually portrayed as having certain stereotypes, such as being from a lower social class, less educated, and so on.
b. *White collar crime*
   This type of crime is divided into 4 groups of crimes: corporate crime, bureaucratic crime, malpractice, individual crime.
   The perpetrators are usually the opposite of blue collar criminals, they have high income, are educated, hold honorable positions in society.

Cybercrime itself, as a crime that arises as a result of the existence of a virtual community on the internet, has its own characteristics that are different from the two models above. The unique characteristics of cybercrime include the following five things:

a. Scope of crime
   Due to the global nature of the internet, the scope of this crime is also global. Cybercrime is often committed transnationally, across national borders, making it difficult to ascertain the jurisdiction of state law that applies to the perpetrator. The characteristics of the internet where people can pass by anonymously allow for various malicious activities that are untouched by the law.
b. Nature of the crime
   Non-violence, or not causing visible chaos. While conventional crime is often chaotic, internet crime is the opposite.
c. Perpetrators of crime
   More universal in nature, it has a special characteristic that crimes are committed by people who master the use of the internet and its applications. The perpetrators of these crimes are not limited to a certain age and stereotype, those who have been caught are teenagers, and some are even children.
d. Modes of crime
   The uniqueness of this crime is the use of information technology in the modus operandi, which is why the modus operandi in the cyber world is difficult to understand by people who do not master the knowledge of computers, programming techniques and the ins and outs of the cyber world.
e. Types of losses incurred
   It can be material or non-material. Such as time, value, services, money, goods, self-esteem, dignity and even confidentiality of information.

Based on this, in describing the types of activities it carries out, cybercrime can be classified into several types as follows: (Hinca IP Panjaitan et al, 2005, p. 32).

a. *Unauthorized Access to Computer System and Service*
   Crimes committed by entering / infiltrating a computer network system illegally, without permission or without the knowledge of the owner of the computer network system it enters. Hackers usually do this with the intention of sabotage or theft of important and confidential information. However, there are also those who do it just because they feel challenged to try their skills to penetrate a system that has a high level of protection.
b. *Illegal Contents*
   It is a crime to put data or information on the internet about something that is untrue, unethical, and can be considered unlawful or disturbing public order. For example, the posting of false or slanderous news that will destroy the dignity or self-esteem of others, matters related to pornography or the posting of information that is a state secret, agitation and propaganda against the legitimate government and so on.

c. *Data Forgery*
It is a crime to falsify data on important documents stored as scripless documents via the internet.

d. *Cyber Espionage*
It is a crime that utilizes the internet network to spy on other parties, by entering the target party's computer network system. This crime is usually aimed at business rivals whose documents or important data (data base) are stored in a computerized system (connected to a computer network).

e. *Cyber Sabotage and Extortion*
This crime is committed by disrupting, damaging or destroying data, computer program or computer network systems connected to the internet. Usually this crime is committed by infiltrating a logic bomb, computer virus or a certain program, so that data, computer programs or computer network systems cannot be used, do not run properly, or run as desired by the perpetrator.

f. *Offense against Intellectual Property*
This crime is aimed at intellectual property rights owned by other parties on the internet. For example, illegally copying the appearance on a web page of a site owned by someone else, broadcasting information on the internet that turns out to be someone else's trade secrets, and so on.

g. *Infringements of Privacy*
This crime is usually aimed at a person's personal information stored on computerized personal data forms, which if known by others can harm the victim materially or immaterially, such as credit card numbers, ATM PIN numbers, disabilities or hidden diseases and so on.

h. *Cracking*
Crimes using computer technology that are committed to damage the security of a computer system and usually commit theft, anarchic acts once they gain access. Usually we often misinterpret between a hacker and a cracker where hackers themselves are synonymous with negative actions, even though hackers are people who like to program and believe that information is something very valuable and some are public and confidential.

i. *Carding*
Carding is a crime using computer technology to make transactions using another person's credit card so that it can harm that person both materially and non-materially.

Based on Activity Motive

Motive is the intention to commit a criminal offence or crime, the motives for cybercrime activities can be classified as follows: (Bapenda Jabar, 2017).

a. *Cybercrime as a purely criminal act*
Pure crime is a criminal act committed for criminal motives. These crimes usually use the internet as a means of crime.

An example of this type of crime is Carding, which is the theft of credit card numbers belonging to other people to be used in trading transactions on the internet.

b. *Cybercrime as grey crime*
The type of activity on the internet that falls into the "grey" area, it is quite difficult to determine whether it is a crime or not regarding the motive of the activity is sometimes not for crime.
Example: Probing or port scanning is the name for a kind of reconnaissance of someone else's system by collecting as much information as possible from the system being monitored, including the operating system used, open and closed ports and so on.

By Target of Crime

Based on the target of the crime, cybercrime can be grouped into the following categories:

a. *Cybercrime that attacks individuals* (*againts person*)
This type of activity, the target of the attack is aimed at individuals or individuals who have certain characteristics or criteria according to the purpose of the attack, examples of this crime include pornography, cyberstalking, cyber-trespass.
b. *Cybercrime attacks property rights* (*againts property*)
Activities undertaken to interfere with or invade the property of others, such as unauthorized accessing of computers through cyberspace.
c. *Cybercrime attacks the government* (*againts government*)
Conducted with the specific purpose of attacking the Government. Such activities include cyber terrorism as an act of threatening the government including cracking into official government sites or military sites.

Cybercrime Case Example

Quite a number of cases have occurred in Indonesia in relation to cybercrime, including:

a. In 1982 there was an embezzlement of money in a bank through a computer as reported in the 10 January 1991 edition of "Voice of Reform" about two students who broke into a private bank in Jakarta to the tune of Rp. 372,100,000.00 using a computer. In this case, the modus operandi was purely criminal; this type of crime usually uses the internet only as a means of crime. The settlement, because this crime included embezzlement of money from a bank by using a computer as a means of committing a crime. In accordance with Indonesian law, this person is punishable under Article 362 of the Indonesian Penal Code or Article 378 of the Indonesian Penal Code, depending on the mode of offence committed. (Andin Rusmini, 2017, p. 30-31).
b. The domestic banking world was also shocked by Steven Haryanto's actions in creating a real but fake website for BCA's internet banking services. Through the "Aspal" sites, if customers mistyped the original site and entered the sites, their user IDs and personal identification numbers (PINs) could be captured. 130 customers had their data stolen, but according to Steven's confession on the Indonesian Web Master

website, his aim in creating the spoof sites was to draw attention to the public's mistyping of the site address, not to make a profit. (Ning April, 2020).

c. Based on data from the Directorate of Cyber Crime of the Police Bareskim during 2023, namely January-October, the ranks of the Police in Indonesia handled 1,763 cybercrime cases. Of this figure, the Police have at least resolved 835 cybercrime cases (crime clearance). The settlement of the case is categorized from the case file declared complete (P21) or the letter of request for termination of the investigator's process (SP3), in the data the highest cybercrime is fraud. (Okezone News, 2023).
d. North Sumatra Polda handled 95 cybercrime crimes, with details of one pornographic content, one online gambling, 53 cases of insult and defamation, 30 cases of fraud, two spreading hostility, 6 cases of threatening, 3 cases of illegal access, out of a total of 45 cases have been resolved. (Okezone News, 2017).

Cybercrime and Environmental Crime

The Government of the Republic of Indonesia has passed Law No. 32/2009 on Environmental Protection and Management which consists of 127 articles. The criminal law provisions in the law are regulated from Article 97 to Article 120. The Law on Environmental Protection and Management explicitly stipulates that environmental crimes are crimes. A crime is a breaking the law, which is an act that although not specified in the law as a criminal act has been declared as injustice, as an act that is contrary to the legal system. (Moelyatno R, 1987, p. 7).

In detail, Law No. 32/2009 contains 19 forms of acts or actions that can be sanctioned by criminal law, which can be categorized into material offences and formal offences.

Material offences are offences or acts prohibited by law that are considered to be complete or fulfilled when the act has caused the consequences, which are formulated in Article 98, Article 99 and Article 112 of the law.

Article 98 reads as follows:

(1) (1) Any person who intentionally commits an act that results in the exceeding of ambient air quality standards, water quality standards, sea water quality standards, or environmental damage standard criteria shall be sentenced to imprisonment for a minimum of 3 (three) years and a maximum of 10 (ten) years and a fine of at least Rp.3,000,000,000.00 (three billion rupiah) and a maximum of Rp.10,000,000,000.00 (ten billion rupiah).
(2) ..... etc.
(3) ..... etc.

Article 99 Any person whose negligence results in the exceedance of the ambient air quality standard ... etc.

Article 112 is a material offence that applies to government officials authorized in the field of environmental supervision.

Formal offences are offences or acts prohibited by law that are considered perfect or fulfilled once the act is committed without requiring the existence of the consequences of the act. There are 16 (sixteen) formal offences in Law Number 32 Year 2009 on Environmental Protection and Management.

Based on the types of criminal offences that have been put forward as environmental crimes when linked to cybercrime, both are crimes whose objects are through information technology through the internet network, while environmental crimes are in the form of pollution and/or environmental damage. Both have resulted in losses to society and the environment. In conventional crime, the perpetrator is a corporation, (B. Cinard & Peter C. Yeager retrieved Muladi, 1992, p. 39) often called white-collar crime.

In Law Number 32 of 2009 concerning Environmental Protection and Management regarding criminal provisions relating to legal entities, it is regulated in Article 116 which reads as follows:

(1) Where an environmental criminal offence is committed by, for, or on behalf of a business entity, criminal prosecution and criminal sanctions shall be imposed upon:
    a. Business entity; and/or
    b. The person who gives the order to commit the criminal offence or the person or persons who act as the leader of the activities in the criminal offence.
(2) ... etc.

In practice, some of the laws that are often used by law enforcement officers to ensnare allegations of certain criminal offences committed by corporations as well as their management, through Law Number 41 of 1999 concerning Forestry, especially Article 78 paragraph (14), Law Number 32 of 2009 concerning Environmental Protection and Management, especially Article 116, Article 117, and Article 119. (Syamsul Arifin, 2014, p. 217-226).

Related to cybercrime, are production activities that cause environmental pollution, in the form of manifest liquid waste, dust and sound by using inaccurate data through the internet network, presenting balance sheet figures that are not true or made in such a way as if the corporation or company has good and strong capabilities.

Solutions to Prevent Cybercrime

a. From computer devices, including:
    1) Routine updates, upgrades and patches to the operating system and applications in use;
    2) Recheck and correct configurations on operating systems, web servers and other applications;
    3) Re-analyze the active services, disable them if not necessary;
    4) Organize a schedule for backing up important data;
    5) Protect servers with firewalls and IDS. These two tools are powerful for dealing with denial of service (DoS) attacks; and
    6) Use security software that is up to date.

b. Through Legislation

The regulation of cybercrime offences in Indonesia can be seen in a broad and narrow sense. Broadly speaking, cybercrime offences are all criminal offences that use the means or with the help of electronic systems, meaning all conventional criminal offences in the Criminal Code as long as they use the help or means of Electronic Systems, such as murder, trafficking in persons.

However, in a narrower sense, the regulation of cybercrime is regulated in Law Number 11/2008 on Electronic Information and Transactions ("ITE Law").

There are several articles that prohibit and can be applied in the event of cybercrime, including:

1) Article 27 of the 2008 ITE Law: Every person intentionally and without the right to distribute and/or transmit and/or make accessible;
2) Along with violating decency. Criminal punishment Article 45 paragraph (1) of the Criminal Code. Imprisonment for a maximum of 6 (six) years ... etc;
3) Article 28 of the ITE Law of 2008: Every person intentionally and without the right to spread false and misleading news that results in consumer harm in electronic transactions;
4) Article 29 of the ITE Law of 2008 intentionally and without the right to send electronic information and / or electronic documents containing threats of violence aimed personally (cyber stalking) ... etc;
5) Article 30 of the 2008 ITE Law paragraph (3): Every person intentionally and without right or unlawfully accesses a computer and/or electronic system in any way by violating, breaking through, exceeding or breaching the security system (cracking rights, illegal access) ... etc;

Article 33, Article 34 and Article 35 of the ITE Law of 2008.

CONCLUSIONS AND RECOMMENDATIONS

Along with the development of internet technology has had a positive impact on humans in processing sectors in life, but there are also negative impacts, namely cybercrime. Cybercrime is an unlawful act committed using the internet based on the sophistication of computer and telecommunications technology.

This cybercrime is also related to environmental crimes contained in Law Number 32 of 2009 concerning Environmental Protection and Management, including environmental crimes committed by corporations, and falsification of data via the internet on waste manifests and other polluting materials that result in losses to the community and the environment.

Some important steps that every country must take in countering cybercrime are:

1) Modernizing the national criminal law and its procedural laws;
2) Improving the national computer network security system in accordance with international standards;
3) Improve the understanding and expertise of law enforcement officials regarding the prevention of investigation and prosecution of cybercrime-related cases;
4) Increase citizen awareness of cybercrime issues and the importance of preventing such crimes from occurring; and

Enhance cooperation between countries, both bilateral, regional and multilateral in efforts to handle cybercrime.

ADVANCED RESEARCH

This research only discusses environmental crimes contained in Law Number 32 concerning Environmental Protection and Management, using normative legal research methods. It is hoped that future researchers will add case studies related to Environmental Protection and Management.

ACKNOWLEDGMENT

On this occasion the researcher would like to thank all parties who have helped the researcher in completing this article. Hopefully in the future we can collaborate on more in-depth research.

REFERENCES

Alcianno G. Gani, Cybercrime (Computer Based Crime), (2019).

Andi Hamzah, Criminal Aspects of the Computer Field, Sinar Grafika, Jakarta, (1989).

Andin Rusmini, Criminal Offences of Misuse of Credit Cards and Efforts to Combat Credit Card Misuse, Al'Adl, Vol. IX, No. 1, (2017).

Andri Winjaya Laksana, Cybercrime Punishment in the Perspective of Positive Criminal Law, Journal Hukum UNISSULA, Vol. 35, No. 1, (2019).

Bapenda Jabar, Types of Cybercrime Based on Motive and Activity, https://bapenda.jabarprov.go.id/2017/11/10/jenis-cybercrime-berdasarkan-motif-dan-aktivitasnya/, (2017).

Eliasta Ketaren, Cybercrime, Cyber Space, and Cyber Law, Journal Times, Vol. V, No. 2, (2016).

Etika Profesi IT, Characteristics of Cyber Crime, https://danrayusuma.weebly.com/karakteristik-cybercrime.html, (2020).

Hinca IP Panjaitan dkk, Building a democratic Indonesian Cyber Law, IMLPC, Jakarta, (2005).

Ibnu Rusydi, The Role of the Development of Information and Communication Technology in Learning Activities and the Development of the World of Education, Journal Warta Edition: 53, (2017).

Marsall B. Cinard & Peter C. Yeager retrieved Muladi, Corporate Crime, New York: The Free Press, Bunga Rampai Hukum Pidana, Bandung, (1992).

Moelyatno R, Principles of Criminal Law, Bina Aksara Mutiara, Jakarta, (1987).

NCB-Interpol Indonesia, Cybercrime: A Cyberspace Phenomenon, https://interpol.go.id/kejahatanduniamaya2.php, (2019).

Ning April, Examples of Cyber Crime Cases in Indonesia, https://www.academia.edu/37863747/Contoh_kasus_Cyber_crime_di_indonesia, (2020).

Okezone News, In 2023, Police Handle 1,763 Cyber Crime Cases, https://nasional.okezone.com/read/2017/12/21/337/1833784/tahun-2017-polisi-tangani-1-kasus-kejahatan-siber?page=all, (2023).

Okezone News, Police Handle Cyber Crime Cases, https://news.okezone.com/read/2017/12/337/1833784/tahun-2017-polisi-tanganikasusu-kejahatan-siber, (2017).

Syamsul Arifin, Environmental Protection and Management Law in Indonesia, Sofmedia, Medan, (2014).