edunity
Kajian Ilmu Sosial dan Pendidikan

Jurnal Edunity: Kajian Ilmu Sosial dan Pendidikan
Volume 2 Number 1, Januari, 2023
p- ISSN 2963-3648- e-ISSN 2964-8653

LAW ENFORCEMENT AGAINST CYBERCRIME IN ONLINE ACTIVITIES

Novi Hermawati[1], Faisal Santiago[2]
Faculty of Law, Universitas Borobudur
E-mail: hermawatinovi73@gmail.com[1], faisalsantiago@borobudur.ac.id[2]

INFO ARTIKEL
Diterima: 01 Januari 2023
Direvisi: 05 Januari 2023
Disetujui: 15 Januari 2023

ABSTRACT

The development of information and communication technology makes the relationship between individuals and groups with the world not limited to existing norms so that it can cause a change in all fields. The changes also have a major impact on the transformation of values in society. It occurs not only positive but also negative consequences. Information and communication technology used for crime is known as cybercrime. Cybercrime has been confirmed to be adverse to the worldwide community, at the same time as efforts to get rid of cybercrime are nevertheless hampered through numerous factors, therefore, a crook regulation coverage is wanted towards cybercrime crimes. This paper discusses two problems, namely, first, how to enforce the law against cybercrime in the legislation in Indonesia, and second, how the strategy for eradicating cybercrime is formulated in the Law on Information and Electronic Transactions. Law enforcement against cybercrime is performed through criminal and non-criminal policies. Meanwhile, to eradicate cybercrime, it is necessary to prepare appropriate laws and provide legal provisions for law enforcement officers.

Keywords: Law enforcement; cybercrime; crime

INTRODUCTION

Crimes in cyberspace can be carried out without the need for contact between the perpetrator and the victim. Crimes can be committed anywhere, regardless of the distance between the perpetrator and the target of the crime, as long as there is an internet network and adequate equipment.

Crimes committed in cyberspace generally aim to generate financial gain for the perpetrators. (Hatta, 2010) Various measures were taken to attack security systems in cyber space to earn money. Some perpetrators use the internet as a medium to make money, for example using the internet for the illicit trade in weapons and organs, prostitution, and pornography. (Amalia & Prasetyo, 2021) In its development, criminals use the internet to attack someone personally without directly or not aiming for financial gain, for example, defamation through the internet, political hacking, cyberterrorism, cyberbullying, and so on.

Eradication of cybercrime is not easy, this is considering the characteristics of the crime itself. Several things become obstacles in overcoming this crime, including: (Putri, 2020)

a. There is no common legal definition of cybercrime, although at the theoretical level there have been many experts who have tried to define cybercrime.
b. The existing legal formulation has not been able to reach the development of crimes committed in cyberspace. Until now, Indonesia does not yet have a Law on Personal Data Protection like other countries. Temporary personal data protection based on Law Number 11 of 2008 concerning Electronic Information and Transactions and Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions.
c. The characteristics of cybercrime indicate that these crimes can cross state jurisdictions, while international agreements exist regarding law enforcement against cybercrime is still very limited.
d. Penal policies in overcoming cybercrime have not been balanced with non-penal policies such as policies in the work environment, policies in applications, policies in schools, and so on.
e. Law enforcers have to deal with billions of netizens (internet users) with various kinds of internet behavior. Inadequate law enforcement resources are a challenge in tackling cybercrime.
f. Lack of evidence in case disclosure. In several cases in cyberspace, crimes occur in applications or media operated abroad, and that will be difficult for the police to ask the provider for evidence. The bank also refuses to provide customer data, account mutations, and flow of funds in connection with banking secrecy obligations. (Indonesia, 2007)
g. There is no clear boundary between the right to information and the right to freedom of expression in cyberspace, where both rights are human rights.
h. The culture of people who are less vigilant in preventing themselves from becoming victims of cybercrimes, for example, are easy to provide personal identities, upload photos and videos that shouldn't be shared, and easy to trust people they just know in cyberspace. (Soekanto et al., 1981)

RESEARCH METHOD

The research is included in the type of normative juridical research. Normative juridical research is a type of research that seeks to synchronize the legal provisions that apply in law enforcement to other legal norms or regulations. A conceptual approach is also used based on the opinions of legal experts. (Kamilah, 2021) Based on the type of normative juridical research, the research approach in this study uses a statutory approach and a conceptual approach.

The statutory approach uses laws and regulations related to the rule of advocated immunity rights in defending, while the conceptual approach uses the theories and concepts used in this study that have relevance to the legal issues analyzed regarding the liability of advocates in defending clients.

Normative juridical research uses secondary data sources. Secondary data in this type of normative juridical research is data sourced from legal materials,

consisting of primary legal materials, secondary legal materials, and tertiary legal materials.

Legal materials as secondary data used to analyze legal issues in this study are as follows.

The source of data in the study is the subject from which the data can be obtained. There are two sources of data used by the author, namely:

1. Primary Data Source
   Primary data sources are data sources obtained from parties who are able to provide data directly from the field to researchers. Those parties are limited to the head of the Advocate's office, Indra Syahfri, S.H, and colleagues. Thus, primary data collection is an integral part of the legal research process used for decision-making.

2. Secondary Data Source
   Sources of secondary data in this study are sources of data obtained from books/documents related to this research substantively. The documents include books, the Peradi Secretariat Team, the Book of Indonesian Advocates, Rahmat Rosyadi & Sri Hartini, Advocates in Islamic Perspectives & Positive Law, and other books that support research on the Effectiveness of Advocate Immunity Rights in Client Defense according to Law no 18 2003 concerning advocates (Case Study at the Office of Advocates/Legal Advisers Indra Syahfri, SH and Partners).

RESULT AND DISCUSSION

A. Law Enforcement Against Cybercrime in Indonesian Legislation

Law Number 11 of 2008 concerning Information and Electronic Transactions and Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions regulate several actions that are prohibited and constitute acts of cybercrime. These provisions are also linked to the provisions in the Criminal Code. Cybercrime acts include:

1. Actions that violate decency.
   In Article 27 paragraph (1) of Law Number 11 of 2008 it is stated "Every person intentionally and without rights distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents that have content that violates decency." Law Number 11 of 2008 concerning Information and Electronic Transactions itself does not explain the act of distributing and/or transmitting and/or making accessible Electronic Information and/or Electronic Documents that have contents that violate decency. Acts that violate decency by the internet consult with the Criminal Code. (Bolson, 2016)

a. Gambling

Online gambling is regulated in Article 27 paragraph (2) of the Law on Electronic Information and Transactions. The provision stated that "Every person intentionally and without rights distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents containing gambling content." (Arief, 2005)

b. Insults and/or defamation

Insults and/or defamation in cyberspace are regulated as a prohibition in Article 27 paragraph (3) of Law Number 11 of 2008 concerning Information and Electronic Transactions which stipulates that "Everyone intentionally and without the right to distribute and/or transmit and/or make accessible Electronic Information and/or Electronic Documents containing insults and/or defamation." The law equates humiliation with pollution, while humiliation is a group of actions in which one form of humiliation is pollution. (Hamzah & Marsita, 1987)

Acts of humiliation and/or defamation are regulated in Chapter XVI Book II. The crime of humiliation consists of general insults and special insults. General insults are those with entities of self-respect and personal dignity, including pollution, while specific insults are insults that have communal objects of self-respect, honor, and reputation. (Soejadi, 2017) The qualifications for the offense of contempt in the Criminal Code are as follows:

2. General insult
   a. Pollution
   b. Slander
   c. Mild insult
   d. slander complaint
   e. False guess
   f. Insult to the dead
3. Special insult
   a. Insult to the President or Vice President of the Republic of Indonesia
   b. Insulting the Heads of Friendly States and representatives of foreign countries in Indonesia
   c. Insulting the Head of a Friendly State and representatives of foreign countries in Indonesia by broadcasting, showing, or pasting writings or paintings.
   d. Contempt for the National Flag and Coat of Arms of the Republic of Indonesia
   e. Insult to the Government of Indonesia
   f. Insult to certain population groups
   g. Humiliation in matters related to religion
   h. Contempt for rulers and public bodies.

Acts of humiliation and/or defamation can be found in various comment fields online, especially when the victim is scanning his or her personal status, photos, or videos. (Laksana, 2019) Perpetrators can also write insulting and/or defamatory words on their account wall, either with or linking the statement to the victim.

B. Extortion and/or threats.

Extortion and/or threats in cyberspace are prohibited in Article 27 paragraph (4) of Law Number 11 of 2008 which states "Everyone intentionally and without rights distributes and/or transmits and/or makes accessible Electronic Information and/or Documents Electronics that have extortion and/or threats." The qualifications for acts classified as extortion and/or threats in Article 368 paragraph (1) of the Criminal Code states:

Any person with the intent to unlawfully benefit himself or another person forces a person by force or threat of violence to give something, which wholly or partly belongs to that person or another person, or to make a debt or write off a debt, is threatened with extortion, with a maximum imprisonment of nine years.

Article 369 of the Criminal Code is also stated as follows:

1. Whoever with the cause to gain himself or others unlawfully with the risk of defamation both verbally or in writing, or with the risk of disclosing a secret, forcing someone to present something that totally or partially belongs to that man or woman or any other man or woman, or to make money owed or write off money owed, will be punished through the most imprisonment of 4 years.
2. This crime is not prosecuted except upon the complaint of the person affected by the crime. This crime can be committed when the perpetrator forces the victim through cyberspace to provide an item, otherwise, the perpetrator will take certain actions against the victim.

C. Stalking/Cyberstalking

Article 29 of Law Number 11 of 2008 states "Every person intentionally and without rights sends Electronic Information and/or Electronic Documents that contain threats of violence or intimidation aimed at personally." Such acts are carried out using or through information and communication technology, for example by unsolicited hate mail, obscene or threatening emails, mail bombs, and others. (Mansur, 2005)

D. Spreading fake news (hoax)

The spread of false news is regulated in Article 28 paragraph (1) of Law Number 11 of 2008 concerning Information and Electronic Transactions which states "Everyone intentionally and without rights spreads false and misleading news that results in consumer losses in Electronic Transactions."

E. Hate Speech

This crime is regulated in Article 28 paragraph (2) of Law Number 11 of 2008 concerning Electronic Information and Transactions which states "Every person intentionally and without rights disseminates information aimed at causing hatred or hostility to certain individuals and/or groups of people based on ethnicity, religion, race, and intergroup (SARA). “The crime as regulated in Article 28 paragraph (2) is also called a hate site.

F. Illegal Actions

In Article 30 of Law Number 11 of 2008 concerning Information and Electronic Transactions, it is regulated as follows:

1) Every Person intentionally and without rights or against the law accesses Computers and/or Electronic Systems belonging to other Persons in any way.
2) Any Person intentionally and without rights or against the law accesses a Computer and/or Electronic System in any way with the aim of obtaining Electronic Information and/or Electronic Documents.
3) Any person intentionally and without rights or against the law accessing a Computer and/or Electronic System in any way by violating, breaking through, exceeding, or breaking into the security system.

G. Interception

Interception is regulated in Article 31 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions governing interception. The acts classified as interception as referred to in Article 31 are as follows:

1) Any person intentionally and without rights or against the law intercepts or intercepts Electronic Information and/or Electronic Documents in a certain Computer and/or Electronic System belonging to another Person.
2) Any man or woman deliberately and without rights or a crime intercepts the transmission of Electronic Information and/or Electronic Documents that aren't public from, to, and inside a positive Computer and/or Electronic System belonging to some other man or woman, whether or not it does now no longer motive any adjustments or people who motive adjustments, disappearances, and/or termination of Electronic Information and/or Electronic Documents which can be being transmitted.
3) The provisions as referred to in paragraphs (1) and (2) do not apply to interception or wiretapping carried out in the context of law enforcement at the request of the police, prosecutors, or other institutions whose authorities are determined by law.
4) Further provisions regarding the interception procedure as referred to in paragraph (3) shall be regulated by law.”

In the Elucidation of Article 31 paragraph (1) of Law Number 19 of 2016, what is supposed by "interception or wiretapping" is a pastime to listen, document, deflect, change, inhibit, and/or document the transmission of Electronic Information and/or Electronic Documents that aren't public, the use of both a stressed out conversation community or a wired community, which includes electromagnetic radiation or radio frequency.

H. Crimes against Electronic Information and/or Electronic Documents or Data interference.

This crime makes Electronic Information and/or Electronic Documents a target for committing crimes. In Article 32 it is stated as follows:

1) Every Person intentionally and without rights or against the law in any way alters, adds, reduces, transmits, destroys, removes, transfers, or hides Electronic Information and/or Electronic Documents belonging to other Persons or public property.

2) Every Person intentionally and without rights or against the law in any way transfers or transfers Electronic Information and/or Electronic Documents to the Electronic Systems of other people too who are not entitled.

3) For the actions as referred to in paragraph (1) which result in the disclosure of confidential Electronic Information and/or Electronic Documents being accessible to the public with improper data integrity. (Nasional, 2009)

I. Interference in the Electronic Systems

Gangguan terhadap sistem elektronik atau system interference adalah kejahatan yang dilakukan dengan menyerang sistem sebagaimana diatur dalam Pasal 33 yang menyatakan “Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.”

J. Devices Abuse

Misuse of devices or misuse of devices is an act against the law as regulated in Article 34, namely: (1). Any person who knowingly and without rights or unlawfully produces, sells, procures for use, imports distributes, provides, or owns:

1) Computer hardware or software designed or specifically developed to facilitate the actions as referred to in Article 27 to Article 33;

2) password via a Computer, Access Code, or something similar to make the Electronic System accessible to facilitate the actions as referred to in Article 27 to Article 33.

3) The action as referred to in paragraph (1) is not a criminal act if it is intended to carry out research activities, Electronic System testing, for the protection of the Electronic System itself legally and not against the law.

K. Computer related Offense

Computer-related offenses or computer-related offenses are usually used to commit forgery and fraud. (Makarim, 2004) In Article 35 it is stated, "Every person intentionally and without rights or against the law manipulates, creates, changes, deletes, destroys Electronic Information and/or Electronic Documents with the aim that the Electronic Information and/or Electronic Documents are considered as if authentic data."

Strategies in Eradicating Cybercrime Formulated in the Law on Information and Electronic Transactions Cybercrime is one of the products of the globalization of crime, where crimes are committed without being limited to space and time. In tackling the crime of cybercrime, comprehensive efforts are needed both through criminal law and outside criminal law. (Wahid, 2005) Crime prevention and control is carried out with an integrated approach between penal policies and non-penal policies. The penal policy has several limitations and weaknesses, namely, it is pragmatic, individualistic (offender oriented), more repressive, and must be supported by an infrastructure that requires high costs. Thus, crime prevention is better done by using non-penal policies that are preventive in nature. (Taib, 2017) Policies for overcoming cybercrime can be carried out in two ways, namely:

1) Penalty policy.
2) Non-penal policy.

The politics of criminal law in overcoming cybercrime through penal means needs to be balanced with non-penal policies. Non-penal policies that can be implemented are as follows: (Dewi & Suteki, 2017)

1) Develop policies outside of criminal law that support cybercrime prevention efforts, such as through anti-hate policies, anti-bullying policies, and healthy internet policies through the education system.
2) Conducting socialization of potential crimes in cyberspace by educating the internet user community not to include personal identities, transact in places with safe internet facilities, and so on.
3) Build cooperation with the private sector to build a security system in cyberspace.
4) Establishing institutional networks in preventing cybercrime, both at the national and international ranks. International cooperation in overcoming cybercrime is very much needed considering that cybercrime is an organized transnational crime.

As a developing country, Indonesia must be swift in adapting to legal developments and strategies for dealing with cybercrime. Legal politics in tackling cybercrime is finished with the aid of using growing an international method in stopping and imposing legal guidelines in opposition to crimes in cyberspace, compiling responsive criminal formulations, and getting ready

establishments that could take brief movement whilst troubles to arise in cyberspace.

CONCLUSION

Cybercrime in Indonesian legislation is contained in Law Number 11 of 2008 concerning Information and Electronic Transactions and Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions. In eradicating cybercrime and law enforcement through the imposition of criminal sanctions for cybercrime perpetrators similar to non-penal policies, namely formulating policies outside of criminal law that support law enforcement efforts. By socializing the potential for cybercrime, building cooperation with the private sector to build a security system in cyberspace, and establishing an institutional network in preventing the occurrence of increasingly sophisticated cybercrime.

REFERENCES

Amalia, D. A. R., & Prasetyo, M. H. (2021). Kebijakan Hukum Pidana Dalam Upaya Penanggulangan Cyber Terorism. *Jurnal Pembangunan Hukum Indonesia*, *3*(2), 228–239. Google Scholar

Arief, B. N. (2005). *Pembaharuan hukum pidana dalam perspektif kajian perbandingan*. Citra Aditya Bakti. Google Scholar

Bolson, A. P. (2016). Flawed but Fixable: Section 230 of the Communications Decency Act at 20. *Rutgers Computer & Tech. LJ*, *42*, 1. Google Scholar

Dewi, N. S., & Suteki, S. (2017). Obstruksi Pelaksanaan Lisensi Wajib Paten Dalam Rangka Alih Teknologi Pada Perusahaan Farmasi Di Indonesia. *Law Reform*, *13*(1), 1–17. Google Scholar

Hamzah, A., & Marsita, B. D. (1987). *Aspek-aspek pidana dibidang komputer*. Sinar Grafika. Google Scholar

Hatta, M. (2010). *Kebijakan politik kriminal: Penegakan hukum dalam rangka penanggulangan kejahatan*. Pustaka Pelajar. Google Scholar

Indonesia, P. A. (2007). *Kitab Advokat Indonesia, Bandung: PT*. Alumni. Google Scholar

Laksana, A. W. (2019). Pemidanaan Cybercrime Dalam Perspektif Hukum Pidana Positif. *Jurnal Hukum*, *35*(1), 52–76. Google Scholar

Makarim, E. (2004). Kompilasi Hukum Telematika, PT. *Raja Grafindo Persada*. Google Scholar

Mansur, D. M. A. (2005). *Cyber Law: Aspek Hukum Teknologi Informasi*. Tiga Serangkai. Google Scholar

Nasional, B. P. H. (2009). Kajian EU Convention on Cybercrime dikaitkan dengan Upaya Regulasi Tindak Pidana Teknologi Informasi. *Departemen Hukum Dan Hak Asasi Manusia Republik Indonesia, Jakarta*. Google Scholar

Putri, P. (2020). Konvergensi Hukum Informasi Dan Transaksi Elektronik Dalam Kejahatan Korporasi (Coorporate Crime) Menurut Undang-Undang Nomor 11 Tahun 2008 Jo Undang-Undang Nomor 19 Tahun 2016. *Lex Et Societatis*, *7*(11). Google Scholar

Soejadi, H. R. (2017). Refleksi mengenai hukum dan keadilan, aktualisasinya di Indonesia. *Jurnal Ketahanan Nasional*, *8*(2), 1–18. Google Scholar

Soekanto, S., Liklikuwata, H., & Kusumah, M. W. (1981). *Kriminologi: Suatu Pengantar*. Ghalia Indonesia. Google Scholar

Taib, M. (2017). *Dinamika perundang-undangan di Indonesia*. Refika Aditama. Google Scholar

Wahid, A. (2005). *Kejahatan Mayantara (cyber crime)*. Google Scholar