Management of Cybercrime Crimes in Indonesia Viewing from Criminal Law Political Perspective

Roy Adinegoro[1], Faisal Santiago[2]
{dok_oi76@yahoo.com[1] ,faisalsantiago@borobudur.ac.id}

Universitas Borobudur, Indonesia

Abstract. The internet imperfections can possibly cause a worldwide disaster that endangers business, public and global security, conduct, youngster insurance, and government frameworks. While efforts to combat cybercrime continue to be hindered by a variety of factors, it has been demonstrated that cybercrime is harmful to the global community. As a result, a criminal policy to eradicate cybercrime is necessary. In this study, two substances will be discussed: the strategy for eradicating cybercrime and the criminalization of cybercrime in Indonesian law. The Follow up on Data and Electronic Exchanges characterizes the criminalization of cybercrime in Indonesian regulation. Cybercrime annihilation methodologies incorporate both correctional and non-punitive arrangements.

Keywords: cybercrime; criminal policy; criminalization

1 Introduction

The development of the times is also marked by the advancement of technological sophistication which also affects the development of the world of crime. Using the internet and other electronic means, numerous traditional crimes are being transformed into modern cybercrimes (cybercrime). 1] Mamoun Alazab, Steve Chon, Roderic Broadhurst, and Peter Grabosky discussed the characteristics of cybercrime [2] said "Digital lawbreakers might work as free organizations, yet proof recommends that individuals are as yet situated in close geographic nearness in any event, when their assaults are cross-connected. public. For instance, little nearby organizations, as well as gatherings fixated on family members and companions, stay critical entertainers."

The most common goal of cybercrimes is financial gain for the perpetrators. In its turn of events, hoodlums utilize the web to go after somebody's character for monetary profit, either straightforwardly or in a roundabout way. Models incorporate criticism on the web, political hacking, cyberterrorism, cyberbullying, etc. [3]

Despite the fact that Indonesia isn't in the top line of nations that are casualties of cybercrime, it is the nation of beginning where it is regularly perpetrated. Lona Olavia [4] reported, "Indonesia has gotten more noteworthy examination from Cybercrime experts lately, particularly since a 2013 review by Akamai Advances, an IT security firm, detailed that Indonesia had surpassed China as the main wellspring of hacking traffic on the planet." It happens in light of the fact that the culprit

MIC 2022, November 12, Semarang, Indonesia

DOI 10.4108/eai.12-11-2022.2327348

sees a lawful proviso that can be taken advantage of by the culprit to keep away from legitimate trap. A few things become hindrances in beating this wrongdoing, including:[5]

1. Although numerous experts have attempted to define cybercrime at the theoretical level, there is no standard legal definition.
2. Cybercrime continues to grow at a snail's pace that cannot be accommodated by the current legal framework. Like other nations, Indonesia does not yet have a law protecting personal data. Just Regulation No. 11 of 2008 on Electronic Data and Exchanges and Regulation No. 19 of 2016 on Alterations to Regulation No. 11 of 2008 on Electronic Data and Exchanges act as the establishment for transitory individual information insurance.
3. Despite the limited number of international agreements regarding cybercrime law enforcement, the characteristics of cybercrime demonstrate its ability to cross state jurisdictions.
4. Non-penal policies like those for work environments, applications, schools, and so on have not been balanced with penal policies in cybercrime prevention.
5. Law enforcement must deal with billions of internet users who engage in a variety of internet behaviors. Cybercrime can be difficult to combat because of a lack of resources from law enforcement.
6. Insufficient evidence in the case disclosure The police won't be able to obtain evidence from providers because, in many cybercrimes, the apps or media used are located in other countries. In addition, in violation of its banking secrecy obligations, the bank refuses to provide customer information, account modifications, or the flow of funds.[6]
7. Both the right to information and the right to freedom of expression are human rights, and there is no clear line between them in cyberspace.
8. A culture of individuals who are less careful in keeping themselves from becoming casualties of cybercrimes, for instance, simple to give individual character, transfer photographs and recordings that ought not be shared, and simple to believe new individuals known in the internet.

The cyber-world is often used by terrorists to include radical ideologies that threaten the integrity of the nation and state. Therefore, in the prevention of crime against cybercrime, criminal law politics is needed. The politics of criminal law is one of the legal efforts in preventing crime in cyberspace.[7]

Based on the description above, the author is interested in studying matters related to Cybercrime. To make it easier to carry out a comprehensive analysis, the author divides into two problem formulations, namely First, how to criminalize Cybercrime in the Legislation in Indonesia. second, what is the strategy for eradicating Cybercrime in Indonesia?

2 Discussion

Cybercrime Criminalization in Indonesian Legislation

Criminalization is a demonstration or assurance of the specialists in regards to specific activities that are viewed as by the local area or local gatherings to be a demonstration that can be rebuffed as a wrongdoing.[8] Demonstrations of cybercrime are illustrated in Regulation No. 11 of 2008, which manages data and electronic exchanges, and Regulation No. 19 of 2016, which alters Regulation No. 11 of 2008, which controls electronic exchanges and data:

1) Actions that violate decency

In Article 27 section (1) of Regulation Number 11 of 2008 it is expressed "Each individual purposefully and without freedoms disseminates or potentially communicates and additionally makes available Electronic Data as well as Electronic Reports that have content that disregards fairness." Guideline Number 11 of 2008 concerning Information and Electronic Trades itself doesn't figure out the exhibition of conveying as well as sending or possibly causing accessible Electronic Information and furthermore Electronic Reports that to have contents that misuse decency. The Lawbreaker Code's Part XIV, Book II, directs moral infringement. The exhibits that are named decency offenses are according to the accompanying:

a. The violation of decency with intent (Article 281 of the Criminal Code).
b. Pornography (the Criminal Code's Articles 282, 283, and 283 bis).
c. Rape (under the Criminal Code's Article 285)
d. Adultery, which is covered by Article 284 of the Criminal Code. e. Having sex with a woman who is not a wife and is unconscious or helpless, which is covered by Article 286 of the Criminal Code.
f. Engaging in child sex
g. Engaging in sexual activity with a woman who has not yet become a wife
h. Obscenity
i. Obscenity directed at an unconscious or helpless individual
j. Obscenity
k. Sexual activities with minors of the same sex
l. Inciting minors to engage in pornographic conduct
m. Obscenity directed at people under his control.
n. Encourage people under his control to commit obscenity
Pimps, as defined by the Criminal Code's Article 296).

Article 27 section 1 of Regulation Number 11 of 2008 concerning Data and Electronic Exchanges incorporates various activities, including digital sexual entertainment and online prostitution, that abuse fairness through electronic media. When it is done to children, this crime is even more serious. The proliferation of websites that feature pornography is one of the issues brought on by advances in information technology. [3]

2) Gambling

Article 27 section 2 of the Law on Electronic Data and Exchanges manages internet betting. "Each individual purposefully and without privileges disperses, communicates, or makes accessible electronic data as well as electronic records containing betting substance," peruses this arrangement."

3) Insults and/or defamation

As per Article 27 section 3 of Regulation Number 11 of 2008 Concerning Data and Electronic Exchanges, affronts or potentially slander in the internet are precluded. "Everybody deliberately and without the option to circulate or potentially communicate as well as make available Electronic Data and additionally Electronic Reports containing affronts and additionally criticism."

4) Cast and/or threats

Pressure and moreover risks in the web are denied in Article 27 segment (4) of Guideline Number 11 of 2008 which states "Everyone deliberately and without honors scatters or possibly sends as well as makes open Electronic Information and also Chronicles Equipment that have coercion and furthermore risks."

5) Stalking/Cyberstalking

Article 29 of Regulation Number 11 of 2008 states "Each individual purposefully and without freedoms sends Electronic Data and additionally Electronic Reports containing dangers of viciousness or terrorizing focused on by and by." Such demonstrations are helped out utilizing or through data and correspondence innovation, for instance by spontaneous disdain mail, indecent or compromising messages, mail bombs, and others. [9]

6) Spread of fake news (hoax)

"Everybody deliberately and without privileges gets out bogus and deluding word that outcomes in shopper misfortunes in Electronic Exchanges," says Article 28 section 1 of Regulation Number 11 of 2008 concerning Data and Electronic Exchanges."

7) Hate Speech

" Each individual deliberately and without freedoms spreads data pointed toward making disdain or aggression certain people and additionally gatherings in light of identity, religion, race, and intergroup," says Article 28 section 2 of Regulation Number 11 of 2008 concerning Data and Electronic Exchanges. A disdain site is one more name for this offense, as characterized in section (2) of Article 28.

8) Illegal Access

In Article 30 of Regulation Number 11 of 2008 concerning Data and Electronic Exchanges, it is managed as follows:

1. Every Individual deliberately and without privileges or illegal gets to PCs and additionally Electronic Frameworks having a place with different People in any capacity.
2. Any Individual deliberately and without privileges or illegal gets to a PC as well as Electronic Framework in any capacity to get Electronic Data or potentially Electronic Reports.
3. Any Individual deliberately and without privileges or illegal getting to a PC or potentially Electronic Framework in any capacity by disregarding, getting through, surpassing, or breaking into the security framework.

9) Interception

Capture is controlled in Article 31 of Regulation Number 19 of 2016 concerning Revisions to Regulation Number 11 of 2008 concerning Data and Electronic Exchanges overseeing block attempt. The demonstrations delegated capture attempt as alluded to in Article 31 are as per the following:

1. Any Individual deliberately and without privileges or illegal captures or catches Electronic Data or potentially Electronic Records in a specific PC as well as Electronic Framework having a place with someone else.
2. Every Individual intentionally and without opportunities or unlawful catches the transmission of Electronic Information or possibly Electronic Records that are not public from, to, and inside a particular PC as well as Electronic System

having a spot with another person, whether it causes no movements or those that cause changes, vanishings, or possibly end of Electronic Information or possibly Electronic Reports that are being imparted.

3. The arrangements as alluded to in sections (1) and (2) don't matter to capture or wiretapping did with regards to policing the solicitation of the police, examiners, or different establishments whose still up in the air by regulation.
4. Further arrangements seeing the capture attempt technique as alluded to in section (3) will be controlled by regulation."

10) Violations of electronic documents or information or data interference

This crime makes it possible for criminals to target electronic documents and/or information. According to Article 32,:

a. Any individual deliberately modifies, adds to, diminishes, sends, harms, eliminates, or conceals electronic data as well as electronic reports that have a place with someone else or general society without consent or disregarding the law.
b. Any individual who deliberately moves electronic data as well as records to someone else's electronic framework without their authorization or disregarding the law.
c. For the actions outlined in paragraph (1) that lead to the public's access to confidential electronic documents and/or information that lacks proper data integrity.

11) Interference with electronic systems

Obstruction with electronic frameworks or framework impedance is a wrongdoing perpetrated by going after the framework as directed in Article 33 which states "Everybody deliberately and without privileges or illegal makes any move that outcomes in disturbance of the Electronic Framework as well as makes the Electronic Framework not work. as it ought to be."

12) Device abuse

According to Article 34, misusing devices or misusing devices is a violation of the law.:

1) Any person who produces, sells, secures for use, imports, conveys, gives, or possesses intentionally and without privileges:
    a. computer software or hardware created specifically to facilitate the actions outlined in Articles 27 through 33;
    b. computer-generated password, access code, or other similar method designed to make the electronic system accessible in order to facilitate the actions outlined in Articles 27 through 33.
2) If the intention is to carry out electronic system testing and research for the purpose of legally safeguarding the electronic system itself, then the action described in paragraph (1) is not a criminal act.

13) Computer-related offenses

Fabrication and misrepresentation are normally dedicated through PC related offenses or PC related offenses.[10] Article 35 states "Each individual purposefully and without privileges or illegal controls, makes, changes, erases, obliterates Electronic Data as well as

Electronic Records with the point that the Electronic Data and additionally Electronic Archives are considered as though the information is valid."

Strategies for Eradicating Cybercrime in Indonesia

Cybercrime must be combated comprehensively through both criminal and non-criminal channels. An integrated approach between penal and non-penal policies is used to control crime.[11] The corrective strategy has a couple of limits and defects, for example, being practical, individualistic (wrongdoer situated), more severe, and requiring a significant expense framework to help it. Along these lines, bad behavior expectation is better wrapped up by using non-remedial game plans that are preventive in nature.[12] Approaches in cybercrime avoidance can be done in two ways, to be specific:

a) Penalty Policy
b) Non-penal policy

The reformatory strategy is an arrangement connected with the utilization of criminal assents in the settlement of criminal cases in the internet. Punishment strategy should be possible in the accompanying ways:

a. Making legal actions criminal, including cyberspace-related offenses.

   Criminalization can happen due to the improvement of society, which is maintained by drives in science and advancement.[14] Criminalization permits mayhem in the legitimate construction of telematics. Indonesia, as a condition of regulation, establishes that law and order ensures state request and public request.[13] According to Jonathan Mayer of Strictly [15],

   Two distinct types of redundancy are possible because of the structure of cybercrime law. Initial, a cybercrime offense might cover with other cybercrime offenses inside a similar legal plan, making it inside repetitive. Second, a cybercrime offense might cover with common cases or criminal allegations that are not connected with cybercrime.

   Legislators need to draw a line somewhere between personal safety and freedom of speech when deciding whether or not an action should be classified as a crime. Flare's Zubair Kasuri states: 16] "Activists for common and basic liberties contend that the law would superfluously confine opportunity of articulation on the web." They guarantee that it will give policing examination specialists unhindered position to annoy guiltless people for the sake of public safety. Basic liberties and social equality advocates contend that the law will deny web opportunity of articulation limitations. They guarantee that it would allow outlandish powers to experts in policing examination to disturb blameless individuals for public safety.

b. Harmonization of public legitimate arrangements with worldwide regulation in annihilating Cybercrime.

   Sigid Suseno [17] depicts that there has been a philosophy between the overall procedure and the groundbreaking system which delivered a compromise approach that is by the characteristics and request of Cybercrime. PC related offenses are separated from customary crook acts that are represented by extraordinary regulations outside the Lawbreaker Code by adjusting the non-criminal equation, both as far as the item and how they are carried out. By making new game plans in unambiguous regulations, a worldwide

methodology is taken to the privacy, honesty, and accessibility of PC information, PC frameworks, or electronic frameworks.

The Public Legitimate Improvement Office (BPHN) in its last report on "EU Show on Cybercrime Study related with Data Innovation Wrongdoing Administrative Endeavors" expressed that in drafting guidelines in the Cybercrime field, Indonesia has a few elective procedures that can be done, specifically by [18]

1. Foster criminal regulation through the arrangement of positive legitimate standards that can arrive at wrongdoings in the field of data innovation.
2. incorporating into national legislation the global principles of cybercrime regulation from a model of international legal norms.
3. In Budapest, ratify or access the EU Cybercrime Convention of 2001, and then draft and implement national legal regulations..

c. Law implementation through the inconvenience of criminal approvals for cybercrime culprits

By including legislators in the detailing of approvals for of policing, regulation purposes regulation as a device for local area designing (regulation as an instrument for social designing). The reason for policing to effectuate social change [9]. It likewise maintains the worth of equity, especially for casualties. The idea of equity assumes a pivotal part in the turn of events, execution, and maintaining of the law. The beliefs of Pancasila regulation make the worth of equity a flat out prerequisite for society, country, and state life. [19] Non-corrective approaches and the governmental issues of criminal regulation should be adjusted to overcome cybercrime through discipline. Coming up next are non-corrective approaches that can be carried out: [20]

a. Develop approaches beyond criminal regulation that help Cybercrime counteraction endeavors, like through enemy of disdain arrangements, hostile to harassing strategies, and solid web strategies through the school system.
b. Spreading awareness of cybercrimes by instructing internet users not to use personal identities, conducting business in areas with secure internet access, and so on.
c. Work with the private sector to create a cyberspace security system.
d. Establishing institutional networks for the purpose of international and national cybercrime prevention. Given that cybercrime is an organized transnational crime, international cooperation to combat it is crucial.

3 Conclusion

Regulation No. 11 of 2008 on Electronic Data and Exchanges and Regulation No. 19 of 2016 on Corrections to Regulation No. 11 of 2008 on Electronic Data and Exchanges lay out the criminalization of cybercrime in Indonesian regulation. The procedure for killing cybercrime comprises of a punitive strategy, explicitly condemning demonstrations to incorporate cybercrime, orchestrating public legitimate arrangements with global regulation, and policing the inconvenience of criminal assents for cybercrime culprits. Non-reformatory arrangements, then again, incorporate creating strategies beyond criminal regulation that help endeavors to forestall cybercrime, directing

socialization of likely violations in the internet, building participation with private gatherings to assemble security frameworks in the internet, and shaping institutional organizations in.

References

[1] Fredy Haris, Cybercrime Dari Perspektif akademis, Lembaga Kajian Hukum dan Teknologi Universitas Indonesia, Jakarta, 2004.

[2] Roderic Broadhurst, Peter Grabosky, Mamoun Alazab dan Steve Chon, "Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime", International Journal of Cyber Criminology Vol 8 Issue 1 January - June 2014.

[3] Abdul Wahid dan Mohammad Labib, Kejahatan Mayantara (Cyber Crime), Refika Aditama, Bandung, 2005.

[4] Lona Olavia, "Cybercrime Threat a Growing Concern: Police", http://www.jakartaglobe.beritasatu.com/news/cybercrime-threat-growing-concern-police/.

[5] Mardjono Reksodiputro, Eric J. Sinrod, William P. Reilly, Pendekatan Hukum pada Teknologi dan Informasi, Surya Cipta Karya, Jakarta, 2005.

[6] Wirjono Prodjodikoro, Tindak-tindak Pidana Tertentu Di Indonesia, PT Refika Aditama, Bandung, 2015.

[7] Ali Zaidan, Menuju Pembaruan Hukum Pidana, Sinar Grafika, Jakarta, 2015.

[8] Soekanto, Soerjono, Kriminologi: Suatu Pengantar, Cetakan Pertama, Ghalia Indonesia, Jakarta, 1981.

[9] Sigid Suseno, Yurisdiksi Tindak Pidana Siber, Refika Aditama, Bandung, 2012.

[10] Edmon Makarim, Kompilasi Hukum Telematika, Cet. 1, PT RajaGrafindo Persada, Jakarta, 2003.

[11] Sutanto, Hermawan Sulistyo, Tjuk Sugiarso, Ed., Cybercrime: Motif dan Penindakan, Cet. 1, Pensil-324, Jakarta, 2005.

[12] Hatta, Kebijakan Politik Kriminal; Penegakan Hukum dalam Rangka Penanggulan Kejahatan, Pustaka Pelajar, Yogyakarta, 2010.

[13] Sri Widoyati Wiratmo Soekito, Anak dan Wanita dalam Hukum, LP3ES, Jakarta, 1983.

[14] Andi Hamzah, Aspek-aspek Pidana di Bidang Komputer, Sinar Grafika, Jakarta, 1987.

[15] Jonathan Mayer, "Cybercrime Litigation", University of Pennsylvania Law Review, Vol. 164, 2016.

[16] Adami Chazawi dan Ferdian Ardi, Tindak Pidana Informasi dan Transaksi Elektronik, Bayu Media Publishing, Malang, 2011.

[17] Zubair Kasuri, Karachi Flare, "Cybercrime Prevention Law Takes Effect", Karachi Vol. 12, Iss. 11, (Aug 2016).

[18] https://yuliatwn.wordpress.com/2015/12/05/pengertian-jenis-jenis-dan-contoh-kasus-cyber-crime/

[19] Badan Pembinaan Hukum Nasional (BPHN), 2009, "Kajian EU Convention on Cybercrime dikaitkan dengan Upaya Regulasi Tindak Pidana Teknologi Informasi", Departemen Hukum dan Hak Asasi Manusia Republik Indonesia, Jakarta.

[20] Marco Gercke, Understanding Cybercrime: Phenomena, Challenges and Legal Response, ITU Telecommunication Development Bureau, 2012.

[21] Adami Chazawi, Hukum Pidana Positif Penghinaan (Edisi Revisi), Media Nusa Creative, Malang, 2013.