WORLD CLASS ISLAMIC CYBER UNIVERCITY
UNISSULA
SULTAN AGUNG ISLAMIC UNIVERSITY
Master of Law Program (S2)
Faculty of Law
Collaboration International Program with Doctoral of Law – UNISSULA 2024
Proceeding of International Conference on The Law Development For Public Welfare
ISSN 2798-9313

Topic: Human Right Issues of Artificial Intelligence (AI) Gaps and Challenges, and Affected Future Legal Development in Various Countries

Cybercrime Regulations as an Instrument of Legal Protection for Victims of Cybercrime in Indonesia

Mujianto
Faculty of Law, Universitas Islam Sultan Agung (UNISSULA) Semarang, Indonesia, E-mail: Mujianto15@gmail.com

Abstract. *Cybercrime Regulations are an important instrument in legal protection for victims of cybercrime in Indonesia. Cybercrime increasingly threatens the peace and security of society, so effective protection of victims is crucial. This research aims to analyze the role of cybercrime regulations as an effort to legally protect victims of cybercrime in Indonesia. Through a normative legal approach and analysis of related laws and regulations, this research identifies the weaknesses and challenges faced in implementing cybercrime regulations in Indonesia. Research findings show the need to increase public legal awareness of cybercrime, increase cooperation between related parties, and strengthen cybercrime regulations that are responsive and adaptive to developments in information technology. It is hoped that the implications of this research can contribute to improving legal protection for victims of cybercrime in Indonesia as well as encouraging improvements in policies and regulations that are more effective in tackling cybercrime.*

Keywords: *Cybercrime; Information; Regulation; Technology.*

1. Introduction

The existence of the internet and information technology has brought significant impacts on the daily lives of society, but it has also opened up opportunities for cybercrime. Cybercrimes such as identity theft, online fraud, malware distribution, and ransomware attacks have become real threats that can harm individuals, companies, and even governments.

In Indonesia, the surge in cybercrime cases continues to occur along with the rapid development of information technology. This necessitates a quick and effective response from the authorities in tackling and preventing cybercrime. Cybercrime regulations become an important tool in enforcing the law and providing protection to victims of cybercrime, as well as preventing the spread of such crimes in society.

However, the implementation of cybercrime regulations in Indonesia still faces various obstacles, such as the lack of public awareness about cybercrime, the lack of cooperation between relevant institutions, and the rapid changes in cybercrime patterns. Therefore, in-depth research and critical analysis of the role of cybercrime regulations in legal protection for victims of cybercrime in Indonesia are important to

improve the effectiveness and responsiveness of these regulations in facing the increasingly complex cybercrime threats in this digital era.

Cybercrime has become a serious threat that confronts not only individuals but also institutions and the nation. In the rapidly developing digital era, cybersecurity challenges are becoming increasingly complex and require a quick and effective response from relevant parties, including regulators and law enforcement agencies. In Indonesia, cybercrime is also increasingly rampant with various modus operandi used by perpetrators to harm victims.

Cybercrime regulations play a very important role in protecting victims of cybercrime and mitigating the risks posed by cybercrime activities. Legal protection for victims of cybercrime is the main focus in efforts to combat cybercrime in Indonesia. However, the implementation of cybercrime regulations still faces various obstacles and challenges that need to be addressed to achieve optimal legal protection for victims of cybercrime.

In this context, this research aims to conduct an in-depth analysis of the role of cybercrime regulations as an instrument of legal protection for victims of cybercrime in Indonesia. By considering various legal, technological, and policy aspects, this research is expected to contribute to a deeper understanding of the challenges and potential solutions in improving the effectiveness of cybercrime regulations in protecting victims of cybercrime in Indonesia."

2. Research Methods

The issue addressed in this research utilizes a research method. This research employs a normative legal approach to analyze the role of cybercrime regulation as an instrument of legal protection for victims of cybercrime in Indonesia. The normative legal approach is used to examine and evaluate the legal aspects related to cybercrime and cybercrime regulation in Indonesia. The research steps include: Literature Study: Tracing legal literature, regulations, and information sources related to cybercrime regulation and cybercrime in Indonesia.

Topic: Human Right Issues of Artificial Intelligence (AI) Gaps and Challenges, and Affected Future Legal Development in Various Countries

3. Results and Discussion

3.1. Cybercrime Regulations in the Indonesian Criminal Law System

The Indonesian legal system does not specifically regulate cyber law. However, several laws have been enacted to prevent cybercrime, including Law No. 36 of 1999 concerning Telecommunications, Law No. 19 of 2002 concerning Copyright, Law No.

15 of 2003 concerning the Eradication of Terrorism, and Law No. 11 of 2008 concerning Electronic Information and Transactions. These laws and regulations have criminalized various types1 of cybercrime and established penalties for offenders. Furthermore, the criminalization policy for cybercrime is formulated in the Draft Criminal Code (RKUHP), specifically in Book Two (Chapter VIII): Crimes Endangering Public Security for People, Goods, and the Environment. Section Five: Articles 373-379 concerning Crimes against Informatics and Telematics regulates the following criminal offenses: Illegal access, Illegal interception, Data interference,

System interference, Domain name misuse, Child pornography. In the discussion of the future development of criminal law, the resolution and prevention of cybercrime must be balanced with the regulation and development of the entire criminal justice system, which includes the development of the structure, culture, and substance of criminal law. In such a condition, criminal law policy occupies a strategic position in the development of modern criminal law. Criminal law policy aims to achieve peace and welfare for all people.

The following cybercrime acts are regulated in Law No. 11 of 2008 concerning Electronic Information and Transactions and Law No. 19 of 2016 concerning Amendment to Law No. 11 of 2008 concerning Electronic Information and Transactions, as follows:

a) Acts that violate morality.

Article 27(1) of Law No. 11 of 2008 states that "Any person who intentionally and without the right distributes or disseminates or makes accessible Electronic Information or Electronic Documents that contain content that violates morality". However, the act of distributing/disseminating/making accessible electronic information/electronic documents that violate decency (morality) is not explicitly explained in Law No. 11 of 2008. Violations of ethics/morality through the internet itself refer to the Criminal Code. In the context of acts that violate morality through electronic media, Article 27(1) of Law No. 11 of 2008 regulates electronic information and transactions, including online pornography and online prostitution. If this crime is committed against children, it will become even more serious. One of the

problems caused by the development of information technology through the internet is the abundance of websites displaying pornographic scenes. It seems that it is very difficult to protect the Internet from the interference of entertainment merchants selling pornography.[2]

b) Online Gambling

Online gambling is regulated by Article 27 paragraph (2) of the Electronic

Information and Transactions Law. This regulation also states that: "Any person who intentionally and without authorization distributes/shares/makes accessible electronic.

c) Insult or defamation of character

Defamation and insult in cyberspace are prohibited under Article 27 paragraph (3) of Law No. 11 of 2008, which states: "Any person who intentionally, and without the right, distributes/spreads/makes accessible electronic information/electronic documents containing defamation or slander. The legislator equates defamation and insult. Insult itself is an act, and one form of insult is defamation. The legislator seems to want to direct the act of insult through the internet as defamation. Chapter XVI of Book II regulates acts of insult and defamation. The crime of insult consists of public insult and specific insult. Public insult refers to the object of the dignity and degree of a person, including defamation. Specific insult refers to insults that have the object of public (general)3 dignity, honor, and reputation. Acts of insult or defamation can be found in various comment sections in cyberspace, especially when the victim scans their identity, photos, or personal videos. Perpetrators may also write insulting or defamatory text on statement walls, publish statements, or link the statements to the victim.

d) Blackmail or threats

Extortion or Threat Article 27 paragraph (4) of Law No. 11 of 2008 prohibits extortion or threats in cyberspace. This article states: "Any person who intentionally and without right distributes and/or transmits and/or makes accessible electronic information and/or electronic documents containing extortion and/or threats". Article 368 (1) of the Criminal Code lists the qualifications of acts that constitute Extortion or Threat, namely: "Anyone who intends to benefit himself or another person in an unlawful (illegal) manner, by forcing someone to give something belonging to that person or another person, in whole or in part, by violence or threat of violence, or by creating debt or erasing debt, shall be punished for extortion and may be sentenced to imprisonment for up to 9 years."

e) Cyberstalking

The Indonesian Law No. 11 of 2008, Article 29, stipulates that: "Any person who intentionally and without the right sends Electronic Information or Electronic Documents containing threats of violence or intimidation addressed personally to another". The provisions concerning electronic information and transactions in Article 29 regulate acts of harassment, threats, or other actions that cause fear, including certain words or actions. This provision is similar to the regulation of cyberstalking in the United States, Canada, England, and other countries. These acts are carried out by utilizing information and communication technology, such as mail bombs, unsolicited hate mail, obscene or threatening emails, and others.[4]

f) The spread of fake news (hoax)

The dissemination of (hoax) news is regulated in Law No. 11/2008 Article 28 paragraph (1), which reads: 'Any person who intentionally and without right disseminates false/fake news and is misleading, resulting in consumer losses in Electronic Transactions.

g) Hate speech

“Article 28 paragraph (2) of Law Number 11 of 2008 concerning Electronic Information and Transactions regulates the crime, which reads: “Everyone who intentionally and without right disseminates information designed to cause hatred or hostility towards individuals/groups of people based on ethnicity, religion, race, and inter-group relations (SARA)

h) Illegal Access

Law No. 11 of 2008, in Article 30, regulates the following:

a) Anyone who intentionally, without right or illegally (illegally) accesses another person's computer or electronic system in any way.

b) Anyone who intentionally, without right or illegally (illegally) accesses (opens) a computer or electronic system in any way with the intention of obtaining electronic information or electronic documents.

c) Anyone who violates, breaks through, exceeds, or breaks the security system intentionally, without right or illegally (illegally) accesses a computer or electronic system.

Topic: Human Right Issues of Artificial Intelligence (AI) Gaps and Challenges, and Affected Future Legal Development in Various Countries

2. Prevention and control of cyber crime

Cybercrime victimizes a massive number of people, especially financially. Most victims can only regret what has happened. They hope to learn a lot from their current experiences, and what needs to be done now is to prevent the possibilities that can harm us as IT actors. This prevention can be in the form of 5:

a. Educate users (providing new knowledge about b. Cybercrime and the internet world)

b. Use the hacker's perspective (using the hacker's thinking to protect your system)

c. Patch the system (closing the weaknesses in the system)

d. Policy (setting policies and rules to protect your system from unauthorized people)

e. IDS (Intrusion Detection System) bundled with IPS (Intrusion Prevention System) g. Firewall. h. Antivirus.

Some important steps that must be taken in responding to Cybercrime are:

a. Conduct national criminal and procedural law updates in accordance with international agreements related to such crimes.

b. Improve national computer network security systems in accordance with international standards.

c. Enhance the knowledge and expertise of law enforcement officials in preventing, investigating, and prosecuting cybercrime cases.

d. Increase public awareness about cybercrime issues and the importance of preventing such crimes.

e. Strengthen cooperation between countries, including bilateral, regional, and multilateral cooperation, in tackling cybercrime, including through extradition treaties and mutual assistance treaties.

Some other examples of mitigation measures include:

a. IDCERT (Indonesia Computer Emergency Response Team) One way to make security issues easier to handle is to establish a unit to report security incidents. With the emergence of the

"sendmail worm" (around 1988), security issues of this kind began to be recognized abroad. When the worm shut down the Internet email system of that era, a Computer Emergency Response Team (CERT) was formed. Since then, other countries have also begun to establish CERTs as a point of contact for people to report security problems. IDCERT is Indonesia's CERT6.

b. Security device certification the equipment used to ensure security must have a certain level of characteristics. Of course, the equipment used for personal purposes is different from that used for military purposes. However, so far in Indonesia, there is no institution that deals with the problem of evaluating security devices.

3. Law Enforcement Against Cybercrime Perpetrators in Indonesia

The enforcement of law against cybercrime perpetrators still faces obstacles even though the Electronic Information and Transactions Law (UU ITE) has been enacted as Law No. 11 of 2008. This law concerns Information and Electronic Transactions. Article 5 of this law expands the scope of evidence in accordance with Indonesian procedural law, accepting electronic information and data or printed copies as valid evidence. This law adds facts about cybercrime that were previously not regulated in the Criminal Procedure Code (KUHAP), such as the contents of this article. However, the law enforcement against cybercrime perpetrators still faces several obstacles. These obstacles include: Lack of Skills and Resources of Law Enforcement Officers Law enforcement officers often lack sufficient training and expertise to effectively combat sophisticated cybercriminals.

Limited Equipment: Many law enforcement agencies lack access to the latest technology and tools necessary for investigating cybercrime, such as cybercrime laboratories, which are crucial for detecting and predicting the whereabouts of cybercriminals during their activities.

These labs are only available at the National Police Headquarters and in police departments in major cities, leading to delays and high costs in investigations. Reluctant Victims Many victims of cybercrime hesitate to report the crimes due to concerns about privacy, financial implications, or a lack of trust in the ability and commitment of law enforcement to solve the cases

3.2 Protection for Victims of Cybercrime in the Indonesian Criminal Justice System

Law enforcement actions against cybercrime perpetrators aim to protect cyberspace users from crackers who use the internet as a medium for their crimes. Although Indonesia does not yet have a "cyberlaw" that specifically targets the interests of victims, Indonesia still needs to take

legal action using existing laws such as: legislation, jurisprudence, and international conventions that have been ratified to protect the interests of the virtual population in Indonesia.

Various efforts can be taken to resolve internet crime, both preemptively, preventively, and repressively. Preemptive efforts can be carried out by ratifying international cybercrime agreements into the legal system in Indonesia. The Council of Europe agreement is one form of international agreement, and part of its covenant has been ratified into the legal system in Indonesia. Handling cybercrime preventively can be done by developing security, increasing energy for computer features, the ability, and discipline in using these features in cyberspace. These activities can take the form of actions that can be carried out individually, nationally, or globally. Meanwhile, repressive cybercrime control measures can be carried out by ensnaring perpetrators of criminal acts to be handled in accordance with the law. The law determines the interests of victims by providing restitution, compensation, or assistance, which is the responsibility of the perpetrator with the State as the

provider.

Efforts to protect victims of crime are an effort, Efforts to protect victims of crime are an attempt to recover the losses already suffered by the victim. This makes more sense if the victim is involved in or participates in the process of resolving the criminal case. Law enforcement is an effort of sustainable development that aims to create a safe, peaceful, orderly, and dynamic life for the country and its environment in the environment of the free (independent) world community.

In the future, criminal law enforcement should pay more attention to the restorative justice system, which is a fair solution to connect the perpetrator, the victim, their families, and other parties involved in the crime to work together to resolve the crime. This is based on a joint decree between the Chief Justice of the Republic of Indonesia, the Minister of Law and Human Rights (HAM), the Minister of Social Affairs, and the Minister of Empowerment of Women and Child Protection of the Republic of Indonesia, which emphasizes restoration to its original state.

4. Conclusion

Communication technology has tremendous power to change human communication behavior. In addition to bringing the benefit of easy communication, technology can also bring disadvantages, one of which is making it easier for "criminals" to commit crimes. Advances in technology allow cybercriminals to prey on their victims. Some common cybercrimes are hacking, cracking, carding, defacement, and phreaking. Hackers are usually not from the lower

class, they are generally educated people, who at least have received formal education to a certain level and can use or operate a PC. Crackers are also educated people, not technologically illiterate, financially capable, and not included in the lower class. Based on cases and conditions of cybercrime occurring in Indonesia, it can be seen that cybercrime is a serious threat to non-traditional security departments. In Indonesia, computer and internet crime (cybercrime) is one of the highest crimes in the world. The Indonesian legal system does not specifically regulate cyber law (cybercrime), but several laws have regulated cybercrime prevention, such as Law No. 36 of 1999 concerning Telecommunications, Law No. 19 of 2002 concerning Copyright, Law No. 15 of 2003 concerning Counter-Terrorism, and Law No. 11 of 2008 concerning Information and Electronic Transactions.". In the discussion of the above description about the development of criminal law in the future, the prevention and handling of cybercrime must be balanced with the improvement and development of the entire criminal justice system, which includes the development of structure, culture, and substance of criminal law. In such conditions, criminal law policy occupies a strategic position in the advancement of modern criminal law. As well as the enforcement of criminal law should pay more attention to the restorative justice system, it seems that this is a fair solution to connect the perpetrators, victims, their families, and other parties involved in the crime to work together to resolve the crime.

5. References

Abdul Wahid and Mohammad Labib, 2005. Cybercrime (Kejahatan Mayantara). Bandung: Refika Aditama.

Adami Chazawi, 2013. Positive Criminal Law of Insult, Revised Edition. Malang: Media Nusa Creative.

Cicut Sutiarso, 2011. Implementation of Arbitration Awards in Business Disputes. Jakarta: Yayasan Pustaka Obor Indonesia.

Dwi Rezki Sri Astarini, 2020. Court Mediation: A Form of Dispute Resolution Based on the Principle of Fast, Simple, and Low-Cost Justice. Bandung: Penerbit Alumni.

Maria Farida Indrati, 2020. Science of Legislation: Types and Materials of Content. Sleman Yogyakarta: Penerbit Kanisus.

Mukti Fajar ND and Yulianto Achmad, 2019. Dualism of Normative and Empirical Legal Research. Yogyakarta: Penerbit Pustaka Pelajar.

Sigid Suseno, 2012. Jurisdiction of Cybercrime. Bandung: Refika Aditama. Soerjono Soekanto and Sri Mamudji, 2019. Normative Leg

al Research: A Brief Review. Depok: Penerbit PT Rajagrafindo Persada.Dista Amalia Arifah, "Cybercrime Cases in Indonesia," Journal of Business and Economics (JBE) 18, no. 2 (September 2011).

Thantawi, "Protection of Victims of Cybercrime in the Indonesian Criminal Law System," Journal of Legal Science, Postgraduate Program, University of Syiah Kuala 2, no. 1 (February 2014).

Ucuk Agianto, "Law Enforcement in Indonesia: Exploring the Concept of Justice in the Dimension of Integrity," Proceedings of the 2018 National Seminar: Transcendental Law Development and Law Enforcement in Indonesia.

Zulfia Hanum Alfi Syahr, "Dynamics of Digitalization of Court Service Management," Proceedings of the 3rd National Expert Seminar 2020, Book 2: Social Humanities, 2020.

Mahkamah Agung Republik Indonesia, Blueprint for Judicial Reform 2010-2035, Mahkamah Agung RI, Jakarta, 2010, pp. iii and iv.

Tim Pokja Laporan Tahunan Mahkamah Agung Republik Indonesia, Annual Report 2020 Mahkamah Agung Republik Indonesia: Long-Term Modern Justice Optimization, Mahkamah Agung RI, Jakarta.