Mataram Journal of International Law
Volume 1, No. 2, Desember 2023
open access at : https://journal.unram.ac.id/index.php/majil/index
Department of Law, Faculty of Law, University of Mataram

THE URGENCY OF ADOPTING THE NORMA CONVENTION ON CYBERCRIME IN AMENDMENT TO LAW NO 11 OF 2008 CONCERNING ELECTRONIC INFORMATION AND TRANSACTIONS

Sevia Dian Rianita Permadi
Universitas Mataram
seviadian.2001@gmail.com

Muh. Risnain
Universitas Mataram
risnain82@gmail.com

Lalu Guna Nugraha
Universitas Mataram
laluguna@unram.ac.id

ABSTRAK

The purpose of this study is to analyze the urgency of adopting the Convention on Cybercrime in changing Law no. 11 of 2008 concerning Information and Electronic Transactions focuses on forms of legal protection against cybercrime before and after the passage of the Electronic Information and Transaction Law (UU ITE) and the urgency for ratification of The Convention on Cybercrime in Indonesia. In this study using a type of normative research. Based on the results of this study it is known that the Urgency of Adopting the Convention on Cybercrime in Amending Law No. 11 of 2008 concerning Information and Electronic Transactions, especially the form of legal protection against cybercrime before and after the passage of the Electronic Information and Transaction Law and the urgency of ratifying The Convention on Cybercrime in Indonesia, so that in cases of cybercrime or Cybercrime in Indonesia. Based on the provisions of the Convention on Cybercrime, cybercrime offenses are generally regulated in the convention. However, every country is given the opportunity to develop and adapt to the needs of that country without putting aside the interests of the international community. Therefore, the law used is neutral, and the form of punishment regulated in the Convention on Cybercrime is a minimum standard provision. If adopted,The urgency of adopting the norms of the Convention on Cybercrime in changing Law no. 11 of 2008 concerning Information and Electronic Transactions is to complement the weaknesses of the Act regarding international cooperation. This of course can make it easier for the Indonesian government to tackle cyber crime through international cooperation mechanisms.

Keywords: Urgency, Adoption, Norm, Act, Cybercrim.

A. INTRODUCTION

According to the Organization of European Community Development (OECD) cybercrime is: “any illegal, unethical or unauthorized behavior relating to the automatic

DOI : https://doi.org/10.29303/majil

processing and/or the transmission of data".[1]That means, all forms of unauthorized activity in a computer system are included in a crime.

To prevent this, strict and binding laws are needed for everyone to use the internet. One of the efforts that is clearly visible is the Council of Europe in studying and exploring the problem of cybercrime. The Council of Europe has produced an international convention known as The Council of Europe Convention on Cybercrime, 2001 which was made on November 23, 2001 in the city of Budapest, Hungary, by the countries that are members of the European Union (Council of Europe) which was then included in the European Treaty Series with Number 185.

In general, the notion of cybercrime itself is usually interpreted as crimes in the realm of cyberspace that utilize computer technology and internet networks as targets. At the 10th United Nations (UN) Congress in Vienna Austria on 10-17 April 2000, the term cybercrime was divided into two categories. First, cybercrime in a narrow sense is called computer crime. Second, cybercrime in a broad sense (in a broader sense) is called computer-related crime.

1. *Cyber crime in a narrow sense (computer crime): any legal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.*
2. *Cyber crime in a broader sense (computer related crime): any illegal behavior committed by means in relation to a computer system or network, including such crimes as illegal possession, offering or distributing information by means of a computer system or network.*[2]

This convention was formed with the following considerations (in the opening of the EU Convention on Cybercrime), among others:[3]

1. The international community recognizes the need for cooperation between countries and industry in combating cyber crime and the need to protect legitimate interests in the use and development of information technology.
2. The current convention is needed to prevent misuse of computer systems, networks and data to commit criminal acts. Thus there is a need for certainty in the process of investigation and prosecution at the international level. And domestically through a reliable and fast international cooperation mechanism.
3. At present it is increasingly evident that there is a need to ensure a compatibility between the implementation of law enforcement and human rights in line with the Council of Europe Convention for the Protection of Human Rights and the 1966 United Nations Covenant on Political and Civil Rights which provide protection for freedom of opinion such as the right of expression, which includes the freedom to seek, receive and impart information and opinions.

The problem of law enforcement in Indonesia seems to be starting to face obstacles related to the increasingly rapid development of society. Various cases illustrate the difficulty of law enforcement in finding ways to make the law appear to be in line with societal norms.[4]

---

[1]Eddy Djunedi Karnasudiraja. (1993). Computer Crime Jurisprudence, Jakarta: CV Tanjung Agung, p.3

[2]Agus Rahardjo. (2002). Cybercrime: Understanding and Prevention of Technology Crime, Bandung, PT Citra Aditiya Bakti, p. 32 in Widodo, 2011, Legal Aspects of Mayantara Crime, Yogyakarta, Aswindo, p. 7

[3]Sahat Maruli T. Situmeang. (2020). Cyberlaw. Bandung: CV Cakra. p. 14.

[4]Eva Achjani zulfa. (2008). When Age Left the Law. Bandung: Citra Aditya Bakti. page 46

Even though the existence of regulation on cybercrime does not only cover Indonesian Law 11 of 2008 concerning Information and Electronic Transactions, but also includes other special measures outside the Criminal Code, there are still forms of cybercrime that have not been regulated. Particularly with regard to the misuse of advanced technology. One of the principles of criminal law determines that no act can be punished with a criminal penalty and is punishable by a criminal sentence if it has not been stated in a statutory regulation (legality principle). According to Muladi, operationally, criminal legislation has a strategic position in the criminal justice system.[5]

Legally, Indonesia also has a special Cybercrime law, namely Law Number 11 of 2008 concerning Information and Electronic Transactions which discusses computer crimes and penalties imposed for violations. Even though the existence of regulation on cybercrime does not only cover Indonesian Law 11 of 2008 concerning Information and Electronic Transactions, but also includes other special measures outside the Criminal Code, there are still forms of cybercrime that have not been regulated.

Collaborating in investigating cybercrime cases because of its borderless nature and does not recognize regional boundaries, so cooperation and coordination with other countries' law enforcement officials is very important to do. International cooperation also includes cooperation agreements between countries both in extradition and in terms of assistance in efforts to present victims who are outside the territory of the state. For this reason, it is important for Indonesia to be able to adopt the norms written in the Convention on Cybercrime into changes to the Electronic Information and Transaction Law which still has some weaknesses.

A study of the provisions of this Convention is necessary to create harmonization between national law and international law so that the eradication of cybercrime is in harmony with similar efforts at the international level. What's more, through international cooperation designed in this convention system, Indonesia will be able to deal with cyber crime cases more effectively.

Based on the background description, the authors are interested in discussing the new Criminal Code, namely Law No. 1 of 2023 concerning the Criminal Code and Law no. 11 of 2008 concerning Information and Electronic Transactions. Have these two laws adopted the Convention on Cybercrime and do these laws still have deficiencies in terms of norms or are they sufficient to accommodate cybercrime in Indonesia?

Based on the background description provided by the compiler, the problem to be discussed is the importance of implementing the norms of the Convention on Cybercrime in amending Law no. 11 of 2008 concerning Information and Electronic Transactions. Additionally, the mechanism used by the Indonesian government to adopt the norms of the Convention on Cybercrime into the amendments of Law no. 11 of 2008 concerning Information and Electronic Transactions will also be examined.

Based on the main problems as above, this study aims as follows:

a. To analyze Law No. 11 of 2008 concerning Information and Electronic Transactions, it has adopted the norms contained in the Convention on cybercrime
b. To analyze the mechanism of the Indonesian government in adopting the existing norms in the Convention on cybercrime into changes to the ITE Law

The benefits of this research, namely:

[5]Muladi. (1995). Capita Selekta Criminal Justice. Semarang: UNDIP Publisher Agency. P.23

a. Theoretical benefits are expected to add to and can be used as material for study in science, especially in the field of international law so that it can add insight related to legal protection for cyber cases in Indonesia and the urgency of adopting The Convention on Cybercrime in Indonesia.

b. Practical Benefits, it is hoped that it will provide a reference for the government and the DPR in formulating legal policies related to changes to the ITE Law, as well as increasing public knowledge related to legal protection against cybercrime and adding to the author's insight, especially in the field of cyber law.

This type of research is normative legal research using a statutory approach (state approach) and conceptual approach (conceptual approach). The sources of legal materials in this study come from primary legal materials, subsidiary and tertiary legal materials. The technique for collecting legal materials uses library research techniques as well as electronic media (internet). Analysis of legal materials using the method of interpretation (interpretation).

B. METHOD

The authors in this study use regulatory research analysis techniques, previous international agreements, and examine new problems that arise. As a step to obtaining conclusions in this study, the author uses the following approach :

a. Statute Approach

The ITE Legislation and International Agreement approach is used with the aim that the problems in this study are reviewed from a legal aspect, namely to what extent international legal rules and regulations that can regulate cybercrime are adopted in Law Number 11 of 2008 concerning Electronic Information and Transactions. In addition, international law in implementing a regulation cannot be separated from political elements that always influence a country in acting with the aim of prioritizing the national interests of its country. This approach is used to review and analyze all laws and regulations related to the legal issue being addressed. This approach is carried out by making the law the main material for guidance in the research conducted. There are still vacancies or shortcomings in the regulations in the law, so this legislative approach is used as the right method to be able to find out whether a law has been implemented appropriately or not.

b. Conceptual Approach

The conceptual approach, namely the conceptual framework, is an illustration of the relationship between the concepts to be studied and expert views and the problems to be discussed. This approach emphasizes the importance of overarching concepts and their interconnections, guiding researchers or problem solvers in formulating hypotheses, designing methodologies, and interpreting findings within a broader theoretical context. By prioritizing theoretical understanding, a conceptual approach allows for a more comprehensive and organized exploration of topics, providing a foundation for insightful analyses and informed decision-making in various fields, including research, problem-solving, and analysis.

C. ANALYSIS & DISCUSSION

A. The Urgency of Adopting Convention on Cybercrime Norms in Amending Law No. 11 of 2008 concerning Information and Electronic Transactions

Computer-related crimes (cybercrime) are regulated by international legal instruments. The only international instrument that regulates computer-related crimes is the Convention on Cybercrime. In Chapter II, the convention regulates substantive criminal law, namely as described in Article 2 to Article 11. Meanwhile, Articles 12-13 regulate provisions for sentencing.

The forms of cyber crime that have been regulated in the Convention on Cybercrime from articles 2-10, namely:[6]

1. Illegal access
2. Illegal interception
3. Data interference
4. System interference
5. Misuse of devices
6. Computer-related forgery
7. Computer-related fraud
8. Offenses related to child pornography
9. Offenses related to infringements of copyright and related rights

However, every country is given the opportunity to develop and adapt to the needs of that country without putting aside the interests of the international community. Therefore, the law used is neutral, and the form of punishment regulated in the Convention on Cybercrime is a minimum standard provision.

International Cooperation Arrangements in the European Convention on Cybercrime in the form of General Principles and Specific Provisions, in the General Principles there are general principles of international cooperation, principles related to extradition, principles related to mutual assistance, and procedures related to mutual assistance in matters there is no international treaty in effect.

There are two aspects of cooperation in law enforcement for extradition issues and the problem of mutual legal assistance in the criminal field. The following explanation is the issue of extradition, namely: including cybercrime as extraditable offenses, expanding the list of crimes that can be extradited, and the need to revise the law on extradition.

A country based on territorial jurisdiction has the right, power, or authority to make or stipulate laws and regulations or decisions to be enforced within its territorial boundaries, carried out against persons and or legal entities and prosecute criminals before law enforcement authorities in their territory.[7]However, this cannot often be done because the perpetrator has already fled or been namedfugitive to the territorial jurisdiction of another country. Therefore, a country cannot arbitrarily enforce its sovereign law in the territory of other countries. When the law enforcement apparatus of a country catches criminals it is almost impossible or difficult because of their territorial jurisdiction, then a collaboration between law enforcement officials of each country is one of the possible solutions to prevent and eradicate criminals who have fled.

[6]Council of Europe, Explanatory Report To The Convention on Cybercrime (ETS No 185)
[7]I Wayan Parthiana. (2002). International Treaty Law – Part 1, Bandung,: Mandar Maju.

Discusses why the Indonesian government did not ratify the Convention on Cybercrime (Budapest Convention), even though Indonesia recorded around 1.6 billion cyber attacks from 2021 and it is likely that this will increase.

"There needs to be international cooperation in law enforcement, and this cooperation can be realized by becoming a party that also ratifies the Budapest Convention. This convention seeks to overcome cybercrime by harmonizing provisions in national law, as well as increasing the level of investigation and cooperation between countries. If a country ratifies the Budapest Convention, then the country will be bound by the principle of open source. This principle states that other countries can access data extraterritorially where the data is freely without authorization. This is a contradiction of the principle of data sovereignty, where digital data is subject to the laws of the country where the data is processed.

"This concept is also closely related to the concept of data localization as one of the indicators that requires all data processing activities to be carried out within a country's jurisdiction. Here, the state can control data within its territory or across its territory. Countries such as the UK, Malaysia and Singapore already have provisions regarding cross-border data transfers. The main point of regulation regarding data transfer is to prohibit these activities, unless they have met the requirements in the form of an adequacy decision and an appropriate safeguard"

The regulatory landscape in Indonesia is still unable to reach existing assistance to enforce laws related to cyber crime. Of course ratification of the Budapest Convention will be a solution to these deficiencies, but of course this needs to be looked at considering that this convention adheres to the principle of open source. This will conflict with the principle of data sovereignty, which will have legal implications in the form of transformation of national law, especially in regulating the concept of data localization.

Analysis of the provisions of the Convention is very important to achieve legal harmonization to harmonize and integrate Indonesia's efforts to eradicate cybercrime with similar efforts at the international level. In addition, Indonesia can deal with cyber crimes more effectively through international cooperation mechanisms that are built into the treaty system.

Indonesia has several alternative strategies in the framework of drafting regulations in the field of cyber crime. First, formulating positive legal norms as a form of criminal law development that covers crimes in the field of information technology. Second, making regulations through a model of international legal norms in the form of adopting global cybercrime regulatory principles. Third, regulations are made by first adopting or accessing the EU Convention on Cybercrime, Budapest, 2001 and making implementing regulations (implementing legislation) into national legal instruments.

To anticipate and deal with transnational crimes that arise, a form of cooperation was born in the form of agreements and laws called Mutual Legal Assistance in Criminal Matters (Mutual Legal Assistance in Criminal Matters). As theoretically conceived, Mutual Legal Assistance is an international cooperation mechanism with regard to investigations, prosecutions and examinations before courts in accordance with the provisions of the laws and regulations of the requested country.[8]

[8]Muhammad Rustamaji and Bambang Santoso. (2019). "The Study of Mutual Legal Assistance Model and Asset Recovery in Corruption Affair" . Indonesian Journal of Criminal Law Studies Vol. 4 No. 2 November 30,. p. 158

The background to the formation of MLA was the factual condition that as a result of differences in the criminal law system between several countries which resulted in delays in criminal investigations. As an example of the differences in the legal systems of countries in the world regarding the criminal justice system, namely the "Due Process Model", on the one hand there are those who adhere to the "Crime Control Model" system. The Due Process Model focuses more on the protection of human rights for suspects, causing quite a long bureaucracy in criminal justice. Meanwhile, the Crime Control Model emphasizes the efficiency and effectiveness of criminal justice based on the presumption of innocence.[9]

B. Mechanism of the Government of Indonesia in Adopting Norms in the Convention on Cybercrime into Amending the ITE Law

Obstacles to the Indonesian government in ratifying the Convention on Cybercrime into Law no. 11 of 2008 concerning Information and Electronic Transactions due to Indonesia's status which until now is not part of the European Union which makes Indonesia in responding to cyber problems that exist in the territory of Indonesia and outside the territory of Indonesia is limited.

In the era of globalization, cyberspace has become a basic need for humans that can connect people regardless of their distance. The virtual world itself is a new era brought by the internet.[10]Cyberspace is a real thing even if it is intangible. This is because the shape is a virtual world, which is also considered a world without boundaries. This is why it is called the Borderless World, namely where cyberspace does not need to recognize national borders, which can eliminate the dimensions of space, time and place.[11]

International cooperation is a relationship carried out by a country with other countries to meet domestic needs. Cooperation covers economic, social, cultural and security aspects based on each country's foreign policy.

The main issue of international cooperation can be seen from the extent to which benefits can be obtained jointly through cooperation, as well as supporting the conception of unilateral and competitive action interests.[12]

As a developing country, Indonesia is lagging behind in terms of maintenance and development of information technology. In fact, the use of information technology for destructive purposes is a threat to a national defense. The threat can be in the form of military or non-military. A military threat to national defense is a threat to defense and security. Meanwhile, non-military threats to national defense are threats to ideological, political, economic, social and cultural resilience. Sooner or later, the existence of technological progress will affect various fields of human life, be it the social, cultural, or political fields.[13]

Therefore, cybercrimes that act against territorial and time boundaries need proper protection in order to avoid potential harm to individuals, organizations, and even the

[9]Herbert L. Packer, "Two Models of The Criminal Process". Reprinted from The Limits of the Criminal Sanction by Herbert L. Packer. Stanford University Press. 1968, p. 4-8

[10]A. Mahzar. (1999). "Cyberspace Spirituality: How Computer Technology Affects Human Diversity" Mizan Publishers, Bandung, p. 9.

[11]OW Purbo, Development of Information Technology and the Internet in Indonesia, Kompas, 2000, p. 50.

[12]Anak Agung Banyu Perwita and Yanyan Mochamad Yadi. (2017). Introduction to International Relations. Bandung : PT Remaja Rosdakarya. p. 34.

[13]J. Sudarsono. (1992). Science, Technology, and Professional Ethics: Socio-Political Views. Sociology Journal Society. Jakarta: FISIP UI-Gramedia. p. 4.

country. Cyber security is an action to protect computer system operations or internal data integration from criminal actions. Cyber security can also be interpreted as protecting the loss of the ability of the computer owner (the party authorized to control his computer) to control the computer system so that it does not function properly due to an intruder attack that enters the computer system or through malware.[14]

As an effective solution, the emphasis is on legal apparatus to cooperate (mutual assistance) with other countries' law enforcement officers in uncovering a criminal act and this interest must be justified by the laws and regulations in Indonesia. Therefore, many countries add other principles so that their criminal legislation remains in force in conditions that cannot be reached by the principle of territoriality, especially in conditions like the one above. This principle is better known as the extraterritoriality principle.

From this it can be concluded that the Electronic Information and Transaction Law adheres to the principle of extraterritorial jurisdiction. This is contained in article 2 of the ITE Law. The ITE Law applies to any person who commits an unlawful act as stipulated in this ITE Law, both within the jurisdiction of Indonesia and outside the jurisdiction of Indonesia, which has legal consequences in the jurisdiction of Indonesia and/or outside the jurisdiction of Indonesia and is detrimental Indonesian interests.

Extradition is based on the principles of reciprocity, comity and mutual respect for differences in jurisdictions and the legal system aims to enhance international cooperation and extend the application of national law beyond territorial boundaries.[15]

In practice, what makes extradition ineffective is because each country is not bound by bilateral agreements in extradition and is not prioritized in relationsinternational law and extradition are not included as important issues that can force a country to implement the treaty.[16]

The seriousness of the Indonesian government in enforcing and eradicating cyber crime is evidenced by the promulgation of the Electronic Information and Transaction Law (UU ITE). Although the definition of cybercrime is not explicitly stated in the ITE Law, it categorizes several types of cybercrime based on the Budapest Convention on Cybercrime dated November 23, 2001. Based on Article 2 of the ITE Law, it is stated that the law applies to anyone who commits a criminal act as stipulated in the law. this law, both within and outside the jurisdiction of Indonesia, and which is detrimental to the interests of Indonesia.

The scope of jurisdiction of the ITE Law is not limited to acts committed in Indonesia by Indonesian citizens, but also includes acts committed by foreign citizens or legal entities that have legal consequences in Indonesia. Utilization of information technology for information and electronic transactions can be cross-regional or universal, so that "harmful to the interests of Indonesia" includes not only national economic interests but also strategic data protection, national dignity, defense and security, state sovereignty, citizens and Indonesian legal entities. .

---

[14]Yani YM, Ian Montrama, Emil Wahyudin. (2007). Introduction to Security Studies. Malang: Intrans Publishing. p. 73.

[15]Law Number 1 of 1979 concerning Extradition

[16]Rusdianto. (2023). " Implementing the Principle of Extraterritorial Jurisdiction in Combating Cybercrime. Mataram.

Various methods have been taken by countries to resolve jurisdictional issues, but if the perpetrators of cybercrime are outside the territory of the country that is most affected, then they must find a way to bring the perpetrators to that country. The way that is usually taken by countries is through international cooperation. Following are the forms of international cooperation adopted by countries to bring cybercrime perpetrators to justice in their countries:

a. Extradition and Deportation
b. Mutual Legal Assistance
c. Transfer of Cases (Transfer of Proceedings)

D. CONCLUSION

The urgency of adopting the norms of the Convention on Cybercrime in changing Law no. 11 of 2008 concerning Information and Electronic Transactions is to complement the weaknesses of the Act regarding international cooperation.To anticipate and deal with transnational crimes that arise, the principles of cooperation were born in the form of agreements and laws adopted by Indonesia, namely extradition and Mutual Legal Assistance.However, in practice, what makes these two principles ineffective is because to carry out these principles cooperation between countries is required, whereas not all countries are bound to this agreement and are not prioritized in relations. international. So that it cannot force other countries to implement the agreement.The strategy that must be carried out by Indonesia is to first make regulations by adopting the Convention on Cybercrime into national legal instruments.This of course can make it easier for the Indonesian government to tackle cyber crime through international cooperation mechanisms. Then, the Indonesian government's mechanism for adopting the Convention on Cybercrime norms is by amending Law No. 11 of 2008 concerning ITE. Indonesia has several alternative strategies in the framework of drafting regulations in the field of cyber crime. First, formulating positive legal norms as a form of criminal law development that covers crimes in the field of information technology. Second, making regulations through a model of international legal norms in the form of adopting global cybercrime regulatory principles. Third, regulations are made by first adopting or accessing the Convention on Cybercrime, Budapest.

Bibliography

Book

Herbert L. Packer. 1968. "Two Models of The Criminal Process". Reprinted from The Limits of the Criminal Sanction by Herbert L. Packer. Stanford UniversityPress.

Karnasudiraja, Eddy D. 1993, Computer Crime Jurisprudence, CV Tanjung Agung, Jakarta

Parthiana, I Wayan, 2002, International Treaty Law – Part 1, Mandar Maju, Bandung.

Situmeang, Sahat Maruli T. Cyberlaw, CV Cakra, Bandung, 2020

Zulfa, Eva Achjani. 2008, When Age Left the Law, Citra Aditya Bakti. Bandung

Muladi, 1995, Capita Selekta Criminal Justice, UNDIP Publisher Agency, Semarang.

Mahzar A., Cyberspace Spirituality: How Computer Technology Affects the Life of Human Diversity, Mizan Publishers, Bandung, 1999

Purbo, OW Development of Information Technology and the Internet in Indonesia, Kompas, 2000

Banyu Perwita, Anak Agung and Yadi, Yanyan Mochamad. Introduction to International Relations, PT Juvenile Rosdakarya, Bandung, 2017

Sudarsono, J. Science, Technology, and Professional Ethics: Socio-Political Views, Society Journal of Sociology, FISIP UI-Gramedia, Jakarta, 1992

YM Yani, Montrama, Ian, Wahyudin, Emil. Introduction to Security Studies. Malang: Intrans Publishing, 2007

Journal

Rusdianto. 2023. Implementing the Principle of Extraterritorial Jurisdiction in Combating Cybercrim. Mataram Journal of International Law. Vol. 1 No.1

Muhammad Rustamaji and Bambang Santoso. 2019. The Study of Mutual Legal Assistance Model and Asset Recovery in Corruption Affair, Indonesian Journal of Criminal Law Studies Vol. 4 No. 2.

Constitution

Council of Europe, Explanatory Report To The Convention on Cybercrime (ETS No 185)

Indonesia, Law no. 11 of 2008 concerning Information and Electronic Transactions

Law of the Republic of Indonesia Number 1 of 2023 concerning the Criminal Code

Law Number 1 of 1979 concerning Extradition

E-ISSN : XXXX-XXXX

E-ISSN : XXXX-XXXX