INTERNATIONAL JOURNAL OF LAW AND LEGAL ETHICS (IJLLE)
Volume 12, Issue 2022
ISSN 749-9719

THE REVIEW OF CYBERCRIME CASE HANDLING BASED ON INDONESIAN JURISDICTION AND INTERNATIONAL LAW

Fazrul Rahman Mukhsin[1], Aurora Tifani Suci[2], Fadhila Triza Nandrini[3], Achmad Rofiq[4], M. Ongko Khoirurozy[5]

Faculty of Law, Universitas Pembangunan Nasional "Veteran" Jawa Timur,Surabaya, Indonesia[12345]

21071010068@student.upnjatim.ac.id[1],21071010083@student.upnjatim.ac.id[2], 21071010093@student.upnjatim.ac.id[3],21071010099@student.upnjatim.ac.id[4], 21071010139@student.upnjatim.ac.id[5]

Abstract

The purpose of writing this journal is to explain how jurisdictional arrangements in handling cybercrime are governed by national law and international law. The method used in this writing is a library research method using a normative juridical approach and the development of the sources listed in this paper comes from various literature and laws and regulations. The results of the discussion of this journal, international law that regulates state jurisdiction in the Convention on Cybercrime, but the regulation still uses the general concept of jurisdiction in international law. So, it can be concluded from this paper that even though the Cybercrime Convention has not been ratified in Indonesia, the Indonesian people can see from the constitution that we have, namely the ITE Law, that the ITE Law is also a related regulation contained in the Cybercrime Convention. The limitations in this discussion only extend to the discussion regarding jurisdictional arrangements in instruments of international law and national law. Therefore, this article is written to provide understanding to the surrounding community that law enforcement or jurisdiction related to cybercrime has not been implemented either nationally or internationally.

***Keywords*:** cybercrime; international law; ratification; jurisdiction.

Introduction

The use of information technology, media and communication must bring a very significant change. There are changes in both society and technology. World relations will continue to develop without limit, so that it will have an impact on several aspects.

One of technological developments which is frequently used the most is the computer. Nowadays, computers can be used by all people, both children and the elderly. Computers give advantages or benefits to the people when they are working. By using it, the people can finish their work quickly. So, they can save time for doing other work.

Currently, a new legal regime known as cyber law has been born. The term "cyber law" is derived from the word cyber and law which change to cybercrime. Cybercrime is a very serious problem. It is a very detrimental threat to society or local residents. The rapid development of technology, especially the internet, has a huge impact on local residents. These technological advances have both negative and positive impacts. When it's viewed from its positive impact, the internet facilitates easier communication among people in

different places, regions and even countries. Currently, the people even require an internet access to do its job. However, when it's viewed from its negative impact, the internet also has a very dangerous impact for the future. The internet can leak our secrets or personal identities done by people or institutions which are not responsible for doing their work. By leaking people's personal identities, it can spread to other problems which are more dangerous. Cybercrime case certainly will grow up both nationally and internationally.

Cybercrime can occur in the national and international scope. It is a problem which is difficult to be handled because cybercrime belongs to cross border problem. Cybercrime in other countries is certainly happening as well. It even can harm the economic, social and cultural sectors. The development of international crimes which appear in the people's daily life, of course, provides an opportunity for the researcher to conduct research dealing with cybercrime.

The disappearance of space and time boundaries on the Internet changes many things. Developments which occur rapidly when using the internet can even have a negative impact which is commonly referred to cybercrime. Usually, those who commit cybercrimes are named as hackers. They use computer facilities and internet networks. In addition, hackers use internet networks which are changed so that they become cybercrimes. Usually, hackers share the dangerous links to the people who click on these links.

Cybercrime crimes have many types of modes, including:

a. Illegal Contents

In this type of mode, hackers enter or upload data or information which does not match the original or in other words we call it as a fake information (hoax). For the real evidence, the hacker uploads news by looking at the events that occurred, but the contents of the news are all hoaxes, nothing that matches the facts that happened.

b. Data Forgery

Falsification of data surely is a very negative action. This data falsification is usually used to upload data to dangerous websites. Usually the data used is other people's data.

c. Cyber Espionage

Cyber espionage is carrying out spying activities by using the internet network. It's done by entering other devices or computer networks. Usually this crime occurs when there is business competition where important data is stored on a computer of certain group.

d. Infringements of Privacy

This crime is very private and very secret. Usually a person's privacy or data is traded to other people who are not responsible which is of course detrimental to the people whose privacy has been sold.

Therefore, the hackers are very troubling for national and international citizens. The problems related to cybercrime are difficult to be solved because the computer technology, internet networks, gadgets and other telecommunication tools will develop very rapidly by the time.

In addition, there are targets and techniques for cybercrime actors. Usually hackers use devices or tools found on the internet and computers. Then, the tools are executed and used to attack other people's computer systems. Furthermore, the hacker makes his own program to be his target, while the hacker's goals in outline include:

1. Credit card database

2. Bank account database
3. Customer information database
4. Transactions with falsified credit cards
5. Disrupting the system. Usually, hackers disrupt other people's computer systems because of some possibilities. For instance, large company A feels competitive with large company B which has just been inaugurated, thus, these hackers work to disrupt the existing system of company B and maybe the hacker took all personal information about the company for free.

Many hackers are the employees who have worked with the company for a long time, so the company chooses these employees to do this cybercrime. Thus, it brings negative impact to the aggrieved people. These employees are usually paid more by the company's leaders to do cybercrime.

Reporting from the CNBC Indonesia website, the hackers' annual income is around 2.4 billion rupiah. Thus, many teenagers and adults want to be hackers. They usually learn to hijack the systems or other things from online games or even learning from courses.

On the other hand, the occupation in IT (Information Technology) sector become one of the most wanted jobs by large and highly developed companies. The people's income in the IT sector is also very high. There are several types of IT jobs which are most sought after each year. Those are data scientists, web developers, information security analysts and software development engineers. However, it is possible for people who work in a company to sell their abilities for dangerous or illegal things, as we explained in the 4 points above which belongs to the types of cybercrime.

Cybercrime actions are of course very detrimental and also troubling for the internet network users since no more privacy or guaranteed security. Thus, the government of each country should prevent this cybercrime case by giving appropriate punishment for the cybercrime actors because the cybercrime case brings negative impact in various aspects, such as economic, political and socio-cultural aspects. In the future, of course, it will be disruptive in terms of the economic aspect because large companies will emerge which will definitely use the internet network and modern technology.

In addition, the internet network law rules are still new and will continue to develop, and there is global pressure to regulate them, but the enforcement of jurisdiction is still relatively unenforced. It is one of the weaknesses in enforcing the legal basis. It is dealing with the criminal committed by persons and companies based in other countries. The constitution of a country cannot be imposed on other countries, because it is not in accordance with the highest legal basis in a country, and it only applies in each region itself. Thus, every country has its own way in solving or overcoming the cybercrime. One of the main problems in cyber crime is jurisdiction of how far a country can apply its rule of law and how international way is its ability to handle the cases since this is a matter of rights. Legal basis issues in a country can affect its legal sovereignty. In other words, it can affect the country's ability to adjudicate cases with the international way.

Besides, the crimes involving the computer systems, several countries involved can claim jurisdiction over the cybercrime. For example, there are criminal acts such as virus attacks, fraud, and piracy which occur via the Internet, and the victims come from various countries. Thus, to reduce or minimize rivalry between countries in enforcing jurisdiction, countries which are interrelated or have links or cooperation, must negotiate to apply the legal basis to be used. Related negotiations are not required, but it's carried out only when it's necessary. For example, the people with an interest in crimes involving multiple countries are told that other interested people will not prosecute.

Thus, the international cooperation is needed in overcoming this cybercrime problem in the context of its jurisdiction. There are various ways which have been carried out by several countries with the aim of resolving jurisdictional issues in dealing with this cybercrime case. The way which is usually done by some countries is through international cooperation. There are several ways of international cooperation to overcome the cybercrime actors so that they can be tried in the cybercrime's actor 's country by surrendering suspects and isolating cyber actors. If those international collaborations can be conducted properly and thoroughly, the cybercrime actors can be punished as well as possible.

Method

In this paper, the methodology used was the library research method through a normative juridical approach. The development of the sources listed in this paper draws from various literature, laws and regulations. Thus, it is hoped that there will be a combination of data which provides a qualitative analysis based on the sources which have been included.

Result And Discussion

Cybercrime is caused by technology which is increasingly developing in society which then makes people accustomed to life in cyber or virtual worlds. The International Telecommunication Union (ITU) defines Cybercrime as a crime which uses a computer as a medium, destination, or liaison to act maliciously which is harmful[1]. Cybercrime is a serious challenge which must be faced by every country because it has no boundaries since the media used is the internet which has no boundaries as well in both space and time. So that someone can easily explore or exploit because there is no law governing these limits. The difficulties experienced by countries in the world in dealing with this crime are there is no national boundaries which regulate it. It means that this crime can be committed by someone in any country, then can target victims in other countries, and the identity of the cybercrime actors can be hidden in a computer network located in a country in another part of the world.

To overcome these problems, countries respond to arrangements regarding limits on freedom in Cyber or what can be called Cyberspace by making legal rules regarding cyberspace in the form of special cyberlaw so that the activities that occur on it can be controlled properly and also as a form of anticipation so that the security of each country is not threatened by the consequences that arise because of increasingly developing technology. An example is the actions taken by European Union countries which created a law in response to regulation of cyberspace which th is called the Convention on Cybercrime[2]. It specifically regulates cyberspace and public relating to the crimes in the cyber sphere. In addition, international institutions such as the UN and ITU also participate in providing responses regarding cyberspace regulations.

Furthermore, the international law should regulate Jurisdiction in handling cybercrime so that it is clearly stated about the extent to which a country can implement or enforce its law and also what are the limits of the competence of a country's court to try criminal acts related to this cybercrime as well as to establish jurisdictional boundaries so that it will not be easy for cybercriminals to move or hide in countries where have not established regulations regarding cybercrime yet. This journal will discuss the state jurisdiction in

[1] ITU, 2009. *Memahami panduan kejahatan dunia maya, Aplikasi ICT dan Divisi Keamanan Siber*, hal 17.
[2] *Dewan Europe: Convention on the Cybercrime, Budapest, 23 October 2001*

dealing with cybercrime regulated by international law, then regarding law enforcement against cybercrime both under national law and international law as well as regarding the international legal arrangements named the Convention on Cybercrime which was adopted or ratified into Indonesian national law.

A. State Jurisdiction in Handling Cybercrime Regulated by International Law

In International Law, there are several principles dealing with the jurisdiction which originate from the expert's opinions or doctrine. The first is the Subjective Territorial principle. It means that the application of a legal provision is determined by looking at the place where an act or criminal act was violated and the handling of the crime was committed in another jurisdiction. Many countries use the Subjective Territorial principle in their rules or criminal laws.

Second, the objective territorial principle is applied if a crime is committed by an actor from the outside jurisdiction of the state, but what gets a more threatening impact from that event is the jurisdiction of the country where the crime occurred.

Third, the principle of universality. It means that the criminals can be punished according to the jurisdiction of each country concerned which is done anywhere, regardless of the nationality of the suspect or victim[3]. This principle is often a concern in terms of law enforcement in cases of cybercrime because the authority to eradicate cybercrime is more focused on protecting the interests of the state. Thus, there is no need to pay attention to the place and also the nationality of the cybercrime actors and victims.

Fourth, the principle of Active Nationality which means that the state is not obliged to hand over its citizens who commit crimes in the territory of other countries. It means that it is the state that has the authority to punish the cybercrime actors rather than the country whose territory is used as a place for committing crimes. This principle gives more attention to the citizenship status in punishing the crime.

Fifth, the principle of passive nationality. It is in contrast to the principle of active nationality. This principle give attention to the citizenship status of victims to punish the crimes, so the state also has the right to provide protection for its citizens outside its territory. Then, if the country where the crime was committed does not prosecute the actors of the crime, then the victim country has the authority to punish them if they enter the territory of their country[4].

Sixth, the principle of protection. It has the authority to deal with crimes that threaten the security and integrity of the country as well as problems with the country's economy. In addition, the principle of protection is applied to protect the country and the interests within it from crimes committed in outside its territory.

As for further arrangements regarding the jurisdiction dealing with cybercrimes which are specifically stated in the Convention on Cybercrime article 22 which has five paragraphs. Each paragraph describes the condition as follows[5]:

- In paragraph (1) it explains that the countries are part of the convention which can take legislative actions or other actions in terms of exercising their jurisdiction over cybercrimes if the crime is committed in: a) The territory of the country, b) On a ship that has the country's flag attached, c) On an airplane whose registration is carried out in that

[3] Pratiwi, Dian K. [2017]. *Pelaksanaan Prinsip Yurisdiksi Universal Mengenai Pemberantasan Kejahatan Perompakan Laut di Wilayah Indonesia*. Jurnal Selat, 5(1), hal. 43.
[4] Starke, J.G. [2000]. *Pengenalan Hukum Internasional*. 9th ed. London. Butterworths, hal. 211.
[5] *European Committee on Crime Problems* (CDPC), 2001. "*Draf Konvensi Akhir tentang Kejahatan Dunia Maya*", Strasbourg, 25 Mei.

country, d) Crimes classified as criminal acts committed by the nationals concerned outside the jurisdiction of that country.

- Paragraph (2) explains that each country has the right to choose whether to apply the jurisdictional provisions or not, taking into account the circumstances and cases of the crime.
- Paragraph (3) explains that each country where belongs to the convention can take steps to exercise its jurisdiction in the event of a cybercrime, if the actors of the crime are in their country's territory and the extradition is not carried out because of their citizenship status.
- Paragraph (4) explains that the existence of this cybercrime convention cannot leave the application of criminal jurisdiction which has been implemented by the state in its national policy.
- Paragraph (5) explains that if there is more than one country claiming jurisdiction over a crime, then the countries involved are encouraged to negotiate and determine the most appropriate jurisdiction.
- After formulating this convention, the European Union council also explained that in article 22 of the Convention on Cybercrime, there are several crime criteria which oblige convention participants to exercise their jurisdiction in the event of a cybercrime in the form of:
  1. Wiretapping in an illegal manner,
  2. Entering a computer system in an illegal manner,
  3. Intervening with data,
  4. Intervention on the system,
  5. Misusing tools or devices,
  6. Counterfeiting with computer media,
  7. Fraud with computer media,
  8. Pornographic crimes against children,
  9. Violating copyright or other related rights,
  10. Attempted, assisted, or conspired to commit the crimes mentioned above[6].

There are also principles regarding the concept of jurisdiction in International Law stated in Article 22 of the Convention on Cybercrime. Article 22 paragraph (1) explains that there is a territorial principle which means the countries where are part of the convention can punish the cybercrimes' actors in cyberspace which are committed within the territory or outside the territory of the country. However, in line with Article 22 Paragraphs (4) and (5), if there are several countries claiming jurisdiction over a crime, these countries are encouraged to negotiate and determine the most appropriate jurisdiction because in the case of cybercrime, a form of crime involving a computer system and using the internet can target the victims from various countries so it is possible that not only one country will claim jurisdiction over cybercrime. In paragraph (1), letters b and c are territorial principles whose application is escalated. It means that prosecuting criminals who commit their actions on a ship bearing a country's flag or on an airplane registered by a country can only be applied if the ship or aircraft is located outside jurisdiction of that country. Then in Paragraph (1) letter d, there is the principle of Nationality which means that in its application, it is possible that a country can punish its citizens based on the positive law of the country for committing crimes outside the jurisdiction of the country.

In the provisions of Article 22 paragraph (2), it is explained that the countries belong to the convention may make exceptions in the application of paragraph (1) letters b, c,

[6] "*Laporan Penjelasan Konvensi tentang Kejahatan Dunia Maya*", Diadopsi pada November 2001.

also d, but not with paragraph (1) letter a. Then in paragraph (3), it contains a provision that if a country refuses to carry out extradition for reasons of its citizenship status, then that country is still authorized to conduct an investigation of its citizens on condition that the country that refuses must report the results of the interim process that has been carried out.

So, it can be concluded that the Convention on Cybercrime regulating state jurisdiction to eradicate computer crime still uses the general concept of jurisdiction in international law which means that the law established by the European Union council is still immature to be used as a guide for all countries in the world. This is because the computer crime continues to increase, giving rise to the emergence of many cybercriminals whose identities are difficult to identify, and this condition is urgent to create legal regulations regarding cybercrime itself. So that, the regulation regarding state jurisdiction in Article 22 provides legal certainty to every country that is a participant in the convention in applying jurisdiction over this cyber crime even though this jurisdictional arrangement raises possibilities for jurisdictional conflicts which can occur if there is more than one country that claims the jurisdiction of a crime if it is based on territorial principles or where the crime was committed and can also occur if more than one country claiming jurisdiction adheres to the principle of jurisdiction which is not the same as one another[7].

B. Law Enforcement Efforts Against the Cybercrime in International Law and Indonesian National Law to Handle Jurisdictional Issues

The problems in enforcing cybercrime in international law are not far from problems regarding the territory or jurisdiction of the state in prosecuting criminals if the suspect is not in the territory of the country that receives the most serious losses. The method implemented by a country in law enforcement against this crime is by carrying out international cooperation. The forms of international cooperation carried out between countries in the world include:

1. Extradition

Extradition is an act of taking and handing over or bringing back a person who is suspected of having committed an act which constitutes a crime from the country that is used as a place to hide to the country that has jurisdiction to be punished[8]. This practice is carried out by a country to hand over a person who is suspected of being a criminal who has committed a crime in the territory of his country to the country that is entrusted with it because it has the authority to punish the cybercrime's actor. This form of extradition cooperation has the main objective of overcoming the jurisdiction or territorial area which is an obstacle to searching, arresting, detaining, trying and handing over a suspect who has fled to hide[9].

The implementation of extradition efforts in international law is regulated in the Convention on Cybercrime precisely in Article 24 which explains that a crime which can be extradited is a crime that can be punished according to the laws of both countries with a minimum period of one year or a more severe sentence, but if the minimum sentence is differ as stipulated in the law or extradition agreement which applies to two or more parties, then the minimum sentence that can be applied is that of the applicable agreement.

---

[7] Putra, Akbar K. [2016]. *Analisis Hukum Yurisdiksi Tindak Kejahatan Siber (Cybercrime) Berdasarkan Convention on Cybercrime*. Jurnal Ilmu Hukum, 7(1), hal. 39.

[8] Sunarso, S. [2009]. *Ekstradisi Dan Bantuan Timbal Balik Dalam Masalah Pidana Instrumen Penegakan Hukum Pidana Internasional*. Jakarta: Rineka Cipta.

[9] Dewi, Dwi M. N. [2020]. *Ekstradisi Sebagai Upaya Pencegahan Dan Pemberantasan Kejahatan Internasional*. Jurnal Analogi Hukum, 2(1), hal. 18.

The people who are participants in this convention must include the crimes contained in Article 1 of the Convention on Cybercrime to become extraditable offenses in any extradition treaty. Then, if the crime to be extradited is rejected for reasons of the nationality of the cybercrime's actor or if the country that surrenders considers that the violation that occurred is within its jurisdiction, the country that surrenders is obliged to submit a case to the competent authority at the request of the country that is delegated, and also report the final outcome to the entrusted country.

Meanwhile, in Indonesia, this extradition effort has also been implemented for law enforcement against cybercrimes regulated in Law Number 1 of 1979 Concerning Extradition, where the Law contains the conditions for submitting a request for extradition, among others. First, there is prior agreement to carry out extradition based on good relations and desired by the state. Then a person who can be extradited is a person who is a suspect or cybercrime's actor or an accomplice in a crime committed in the territory of Indonesia or in the country to which it has been entrusted. And the crimes that can be punished include crimes that have been mentioned in the Extradition Law, the extradition treaties of Indonesia or other countries, as well as other crimes that have not been regulated but based on the policy of the submitting country, extradition can be carried out. Second, a letter of request for extradition must be addressed to the Minister of Law and Human Rights of the Republic of Indonesia in writing which will then be submitted to the President. In the letter of request submitted to carry out the sentence, there must be an authentic sheet or a copy of the court decision which contains a sentence that has permanent legal force, information on the identity and nationality of the person requested for extradition, and also an authentic sheet or a copy of SP2 from the competent authority in the country[10].

2. Mutual Assistance

This form of mutual assistance cooperation is a mechanism for eradicating international crimes that have begun to emerge in the life of the international community. According to the United Nations, this form of cooperation is that the state requests assistance in finding evidence to be used for the purposes of investigation and prosecution in relation to a case of a crime by tracking, freezing and confiscating the proceeds obtained from the crime[11]. The cooperation in the form of mutual assistance has several principles, including:

- Principle of Cooperation: Cooperation in question is cooperation in law and justice which is regulated in agreements entered into by several countries or can also be in the form of special regulations between two countries.
- The principle of reciprocity according to good relations: The basis of this reciprocity is derived from criminal procedural law, agreements or conventions between one or several countries, as well as international customs.

Indonesian national law also regulates the form of reciprocal cooperation as stated in Law Number 1 of 2006. This cooperation is used in criminal matters. In the law, it is explained that this mutual cooperation occurs when Indonesia requests assistance from outside countries regarding issues related to investigations, prosecutions, as well as court hearings, with the aim that the Indonesian government has a solution on the legal basis to request or provide assistance reciprocally. related to criminal matters with other countries[12].

---

[10] UU No. 1 Tahun 1979 Tentang Ekstradisi.

[11] Peter Langseth, *Buku Pegangan PBB tentang Tindakan Anti Korupsi Praktis untuk Penuntut dan Penyidik* (Vienna; UNDOC,2004), Hal 120.

[12] Putra, Akbar K. [2016]. *Analisis Hukum Yurisdiksi Tindak Kejahatan Siber (Cybercrime) Berdasarkan Convention on Cybercrime*. Jurnal Ilmu Hukum, 7(1), hal. 48-50.

3. Diversion of Cases

Cooperation in this form is regulated in international law and is set forth in the only existing convention, namely the European Convention on Transfer of Process in Criminal Matters. Transfer of cases means cooperation in the international scope where each country may ask another country to use its criminal law rules to try someone who is suspected of being the cybercrime's actor of a crime[13].

An analysis of the Convention on Cybercrime needs to be carried out in order to harmonize laws in Indonesia, this is because in several articles in the Criminal Code law enforcement is considered not in accordance with the level of loss or criminal threats as if it creates discrimination against law enforcement.

In the Convention on Cybercrime, there are several articles that classify cybercrime crimes as regulated in Articles 2 to 5, while the types of crimes are as follows:

1. **Illegal Access**

   Regulated in the Convention on Cybercrime (article 2), it's stated:
   "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system."

2. **Illegal Interception**

   Regulated in the Convention on Cybercrime (article 3), it's stated:
   "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system."

3. **Data Interception**

   Regulated in the Convention on Cybercrime (article 4), it's stated:
   "1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right."
   "2) A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm."

4. **System Disturbance**

   Regulated in the Convention on Cybercrime (article 5*)*, it's stated:
   "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by

[13] *European Convention on Transfer of proceedings Explanatory Report*

inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data."

5. Device Misuse

Regulated in the Convention on Cybercrime (article 6), it's stated:

"Each Party shall take legislative and other measures which may be required to constitute a criminal offense under its domestic law, if it is done willfully and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i *a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;*

ii *a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and*

b *the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. "*

From the several articles above, it is the basis for Indonesia to make arrangements related to cybercrime named the ITE Law where in the Convention on Cybercrime acts are divided into two classifications while in the ITE Law it is not explicitly classified related to the arrangements. The need for ratification of the Convention On Cybercrime for law in Indonesia itself is strongly driven by the fact that Indonesia is one of the countries with the largest internet users in the world, but Indonesia is also one of the countries that is included in the blacklist of the world of trading via the internet, this happens because many internet users in Indonesia are abusing the internet network, as well as transactions via on line.

The Convention on Cybercrime contains several actions that include cybercrime, namely as follows:

1. Offenses against the confidentiality, integrity and availability of data and computer systems. Those are as follows:
a. illegal access;
b. illegal interception;
c. data interception;
d. system disturbance;
e. device misuse.
2. Computer-related offenses, fraud, and counterfeiting
3. Offenses containing child pornographic content

The ITE Law has made the Convention on Cybercrime a reference for regulating cybercrime crimes in Indonesia, which include the following:

1. Illegal Access,

Regulated in article 30 of the ITE Law, as follows:

"(1) Every person intentionally and without right or unlawfully accesses another person's computer and/or electronic system in any way."

"(2) Everyone intentionally and without rights or against the law accesses Computers and/or Electronic Systems in any way with the aim of obtaining Electronic Information and/or Electronic Documents."
"(3) Everyone intentionally and without rights or against the law accesses Computers and/or Electronic Systems in any way by violating, bypassing, exceeding, or breaking through the security system."
2. Illegal Interception
Regulated in article 31 UU ITE, as follows:
"(1) that every person intentionally and without rights or against the law intercepts or intercepts electronic information and/or electronic documents in computer and/or certain electronics belonging to other people;"
"(2) that every person intentionally and without rights or against the law intercepts the transmission of electronic information and/or electronic documents that are not public in nature from, to and in a computer and/or certain electronic documents belonging to other people, whether which does not cause any changes or causes changes, omissions and/or termination of electronic information and/or electronic documents that are being transmitted."
3. Data Interruption
Regulated in article 32 paragraph 1 UU ITE, as follows:
"(1) Everyone intentionally and without rights or against the law in any way changes, adds, subtracts, transmits, destroys, deletes, moves, hides electronic information and/or electronic documents belonging to other people or public property."
4. System Disturbance
Regulated in article 33 UU ITE, as follows:
"Every person intentionally and without right takes any action which results in disruption of the Electronic System and/or causes the Electronic System to not work properly"
5. Device Misuse
Regulated in article 34 of the ITE Law, as follows:
"Anyone who intentionally and without rights produces, sells, procures for use, imports, distributes, provides or owns computer hardware or software specifically designed or developed to facilitate prohibited actions and passwords via computers, access codes, or other things. similar to that, which is intended to make electronic systems accessible with the aim of facilitating prohibited acts."

Even though the Convention On Cybercrime is not ratified in Indonesia, if we analyze it, we can see that what is contained in the Convention On Cybercrime is also contained in the ITE Law where the ITE Law makes the Convention On Cybercrime the basis for its regulation, maybe there are only differences in the order or in the arrangement layout for each regulated cybercrime act. This explains that the norms contained in the Convention on Cybercrime have been applied to Indonesian law, namely the ITE Law. The ITE Law also regulates the types of acts and criminal sanctions regulated in different articles.

Conclusion

The use of media facilities both communication media and information media has made major changes to people's lives both regionally and globally. Currently, the development of technology has made human beings without boundaries to communicate, causing rapid social, cultural and economic changes. The rapid development of technology, especially the internet, has had a huge impact on local residents. These technological advances have impacts both negative and positive impacts. When it's viewed from its positive impact, the internet facilitates easier communication among people in different

places, regions and even countries. Currently, the people even require an internet access to do its job. However, when it's viewed from its negative impact, the internet also has a very dangerous impact for the future. The internet can leak our secrets or personal identities done by people or institutions which are not responsible for doing their work. By leaking people's personal identities, it can spread to other problems which are more dangerous. This crime is called cybercrime.

Cybercrime is a serious threat to the world and is very detrimental to society so that it is the duty of the state to cause cyberlaw to emerge in world countries. It can occur in the national and international scope. It is a problem which is difficult to be handled because cybercrime belongs to cross border problem.

Cybercrime crimes have many types of modes, including:

a. Illegal Contents

In this type of mode, hackers enter or upload data or information which does not match the original or in other words we call it as a fake information (hoax). For the real evidence, the hacker uploads news by looking at the events that occurred, but the contents of the news are all hoaxes, nothing that matches the facts that happened.

b. Data Forgery

Falsification of data surely is a very negative action. This data falsification is usually used to upload data to dangerous websites. Usually the data used is other people's data.

c. Cyber Espionage

Cyber espionage is carrying out spying activities by using the internet network. It's done by entering other devices or computer networks. Usually this crime occurs when there is business competition where important data is stored on a computer of certain group.

d. Infringements of Privacy

This crime is very private and very secret. Usually a person's privacy or data is traded to other people who are not responsible which is of course detrimental to the people whose privacy has been sold.

To overcome these problems, countries respond to arrangements regarding limits on freedom in Cyber or what can be called Cyberspace by making legal rules regarding cyberspace in the form of special cyberlaw so that activities that occur on it can be controlled properly and also as a form of anticipation so that the security of their country is not threatened by the consequences of technology that is experiencing very rapid development. An example is the actions taken by European Union countries which created a law as a response to the regulation of cyberspace, namely the Convention on Cybercrime which specifically regulates cyberspace and is public in nature with regard to crimes in the cyber sphere. In addition, international institutions such as the UN and ITU also participate in providing responses regarding cyberspace regulations.

As for further arrangements regarding jurisdiction in dealing with cyber crimes that are specifically stated in the Convention on Cybercrime. However, the Convention on Cybercrime governing state jurisdiction to resolve computer crimes still uses the concept of jurisdiction in general in international law, which means that the law established by the European Union council is still immature to be used as a guideline for all countries in the world. This is because computer crime continues to increase, giving rise to the emergence of many cybercriminals whose identities are difficult to identify, and this condition is urgent to create legal regulations regarding cybercrime itself.

The legal efforts taken by Indonesia are by issuing the ITE Law and also taking several steps to cooperate with countries and international agencies for crimes committed outside the territory of Indonesia, forms of cooperation between Indonesia and the world such as:

1. Extradition

Extradition is an act of taking and handing over a person suspected of having committed a crime from a country outside the territory of Indonesia to be tried under the jurisdiction of the aggrieved country. Indonesia itself has also implemented this extradition effort for law enforcement against cybercrimes as stipulated in Law Number 1 of 1979 concerning Extradition.

2. Mutual Assistance

This form of mutual assistance cooperation is a mechanism for eradicating international crimes that have begun to emerge in the life of the international community. According to the United Nations, this form of cooperation is the state requesting assistance and also receiving assistance to search for evidence to be used for the purposes of investigation and prosecution related to crime cases by searching, freezing and confiscating evidence obtained against crimes.

3. Diversion of Cases

Cooperation in this form is regulated in international law and is set forth in the only existing convention, namely the European Convention on The Transfer of Proceedings in Criminal Matters. Transfer of cases means cooperation in the international sphere, where each country may ask another country to use its criminal law rules to try someone who is suspected of being the cybercrime's actor of a crime.

Even though the Convention On Cybercrime is not ratified in Indonesia, if we analyze it, we can see that what is contained in the Convention On Cybercrime is also contained in the ITE Law, where the ITE Law makes the Convention On Cybercrime the basis for its regulation, maybe there are only differences in the order or in the arrangement layout for each regulated cybercrime act, this explains that the norms contained in the Convention On Cybercrime have been applied to Indonesian law, namely the ITE Law. The ITE Law also regulates the types of acts and criminal sanctions regulated in different articles.

References

2000. Starke, J.G. [2000]. *Introduction to International Law*. 9th ed. London. Butterworths, hal. 211.

2001. "*Expalantory Report of Convention on Cybercrime*", Diadopsi pada November 2001.

Chaidar, AC, & Kristiani, D (2021). *Peran Perguruan Tinggi Dalam Sosialisasi*

2001. *European Committee on Crime Problems* (CDPC), 2001. "*Final Draft Convention onCybercrime*", Strasbourg, 25 Mei.

2001. *The Council of Europe: Convention on the Cybercrime, Budapest, 23 October 2001*

2009 Sunarso, S. [2009]. *Ekstradisi Dan Bantuan Timbal Balik Dalam Masalah Pidana Instrumen*

2009. ITU, 2009. *Understanding cybercrime guide, ICT Application and Cybersecurity Division*, hal17.

2011. Dista Amalia, *Kasus Cybercrime di Indonesia,* Vol.18, Jurnal Bisnis dan Ekonomi, 2011, 4-5

2016. Hardianto2018, D. (2016). Pertimbangan Hakim Dalam Perkara Pencemaran Nama BaikMelalui Media Sosial. *Jurnal Penelitian Hukum Dejure Akreditasi LIPI: No*, *740*.

2016. Putra, Akbar K. [2016]. *Analisis Hukum Yurisdiksi Tindak Kejahatan Siber (Cybercrime)Berdasarkan Convention on Cybercrime*. Jurnal Ilmu Hukum, 7(1), hal. 39.

2016. Putra, Akbar K. [2016]. *Analisis Hukum Yurisdiksi Tindak Kejahatan Siber (Cybercrime)Berdasarkan Convention on Cybercrime*. Jurnal Ilmu Hukum, 7(1), hal. 48-50.

2017. Pratiwi, Dian K. [2017]. *Pelaksanaan Prinsip Yurisdiksi Universal Mengenai PemberantasanKejahatan*

2020. Dewi, Dwi M. N. [2020]. *Ekstradisi Sebagai Upaya Pencegahan Dan PemberantasanKejahatan Internasional*. Jurnal Analogi Hukum, 2(1), hal. 18.

2020. Ketaren, E. (2016). Cybercrime, Cyber Space, dan Cyber Law. *Jurnal Times*, *5*(2), 35-42. Marufah, N., Rahmat, H. K., & Widana, I. D. K. K. (2020). Degradasi Moral sebagai Dampak

2021. Situmeang, S. M. T. (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk KejahatanSempurna Dalam Perspektif Hukum Siber. *SASI*, *27*(1), 38-52.

Council of Europe Covention on Cybercrime

European Convention on Transfer of proceedings Explanatory Report

Kejahatan Siber pada Generasi Millenial di Indonesia. *NUSANTARA: Jurnal Ilmu Penegakan Hukum Pidana Internasional*. Jakarta: Rineka Cipta.

Pengetahuan Sosial, *7*(1), 191-201.

Perompakan Laut di Wilayah Indonesia. Jurnal Selat, 5(1), hal. 43.

Peter Langseth, *United Nations Handbook on Practical Anti Corruption Measures forProsecutors and Investigators* (Vienna; UNDOC,2004), Hal 120.

Undang Ite Nomor 19 Tahun 2016 Tentang Cyber Crime-Bullying Di Dukuh .... JurnalEkonomi, Sosial & ..., jurnalintelektiva.com, https://www.jurnalintelektiva.com/index.php/jurnal/article/view/457

UU No. 1 Tahun 1979 Tentang Ekstradisi.