*Advances in Social Science, Education and Humanities Research, volume 658*
**4th Social and Humanities Research Symposium (SoRes 2021)**

# Law Enforcement of Cyber Crime Jurisdiction in Transnasional Law

Rahmatilla Aryani Putri*
Postgraduate of University of Langlangbuana
Bandung, Indonesia
*rahma.banibandung@gmail.com

Huala Adolf
Professor of International Law
University of Padjadjaran
Bandung, Indonesia
huala.adolf@gmail.com

Jafar Sidik
Lecturer of University of Langlangbuana
Bandung, Indonesia
jafar.fhunla@gmail.com

***Abstract*—The rapid development of information technology has made the world borderless and lead to social change which is significantly fast. These advances are accompanied by negative impacts which threaten and endanger the social and economic development of the Ummah involving more than one country. Law enforcement against cybercrimes in Indonesia is regulated in constitution number 11 of 2008 about Electronic Information and Transaction as amended by constitution number 19 of 2016 about top change constitution number 11 of 2008 about Electronic Information and Transaction. The problem who the researchers do about Application of Law Enforcement Of Cyber Crime Jurisdiction Reviewed From International Law and Obstacles That Occur As Well As Solutions In The Law Enforcement Of Cyber Crime Jurisdiction In Terms Of International Law. The method approach who the writer use in this research is juridical normative, who do the approach with considering the focus problem is revolve to the rules who talk the relation between the rule and other rule and the connection with the application. The specification of this research is descriptive analysis who describe the used rule and connect to the law's theory and the application of the law enforcement about the problem. To analyze the data in this research, the writer used the qualitative analysis according to the legals norm who be found in the rules of law and the court decision and the society's norms. The result of the analysis is make a deductive conclusion, and describe it in narration explanation without using a formula or statistics so that the writer attracted the specific conclusion. The result of this research is showing a conclusion about application of law enforcement jurisdiction in cybercrimes it is not enough to just use national law, but the need for ratification of international agreements in the field of cyber involving between countries. The government has made various efforts to combat cybercrime, but there are still obstacles in its implementation, for this reason there is a need for harmony between laws and regulations, law enforcement, infrastructure, public, and cultural synergy, and implement international conventions and international cooperation in the form of applying international principles that can be recognized as international custom.**

***Keywords—law enforcement, jurisdiction, cyber, international law***

## I. INTRODUCTION

The development of information technology that develops from year to year has resulted in increasingly sophisticated, easy, and fast information flow being absorbed, as well as making it easier for people to communicate without being constrained by space and time limits. In addition, the development of information technology has caused the world to become borderless and has led to significant social changes taking place so quickly [1].

For example Indonesia cases about cyber crime, first Court ruling No.11/Pid.Sus/2018/PN.Sgr 21 Mei 2018 [2], at Pengadilan Negeri Singaraja, with defendants Boris Georgiev Rusev and Marian Bogidarof Serafimof they are Foreign Citizens Nationality of Bulgaria. Their modus operandi is skimming (act of theft information credit/debit card by ilegal). Second, Court ruling No.1567/Pid.Sus/2020/PN.Sby 5 Oktober 2020 [3] at Pengadilan Negeri Surabaya, with defendants Sergio Chondro and Mira Deli Rubi Permata they are Indonesian citizens. Their modus transact using a foreigner's credit card (Japanese Citizen). Of these cases, these cases have foreign elements where the first case is the perpetrator is a foreign citizen but the locus delictie is carried out in Indonesia, while in the second case is carried out by an Indonesian citizen, the locus delictie is in Indonesia but the victim in this case is a foreign citizen who is a Japanese citizen.

As far as the researcher's knowledge and searches regarding the problems studied, based on preliminary research from researchers at the Library of the Faculty of Law,

 

Langlangbuana University, the researchers found a similar title, namely "Legal Protection against Bank Customers of Cyber Crime Victims in Internet Banking based on Law Number 11 of 2008 concerning Information and Electronic Transactions" by Meslik Anin in 2020, however, this research only focuses on protecting victims of cybercrimes. Researchers also found a similar title at Purna Cita Nugraha's Padjadjaran University with the title Political Law for the Establishment of an Extraterritorial Jurisdiction Regime in Cyberlaw associated with the Conception of State Sovereignty "but the study focuses more on legal politics, the establishment of an extraterritorial jurisdiction regime, and the conception of State sovereignty. The problems raised in this analysis are certainly different from the problems raised in the research analysis whose object of research focuses on law enforcement, the jurisdiction of cybercrime which is reviewed in International Law.

From this description, the researcher wants to know more and understand and analyze further about the enforcement of cybercrime jurisdiction in transnational law.

## II. Research Methods

Legal research method is a scientific activity based on certain methods, systematics, and thoughts, which aims to study something or certain legal phenomena, by analyzing them. In addition, an in-depth examination of the legal factors is also carried out, in order to then seek a solution to the problems that arise in the phenomenon in question [4]. Based on this, the researcher must determine and choose the right method so that the research objectives can be achieved optimally. The research method consists of:

### *A. Approach Method*

The approach method used in this research is normative juridical. Normative juridical research is library research on secondary data in the field of law consisting of primary legal materials and secondary legal materials, laws based on statutory regulations through the interpretation of the articles that regulate the matters that are problematic. The approach method is used keeping in mind that the problem under study revolves around legislation, namely the relationship between one regulation and another and its relation to its application in practice [5].

### *B. Research Specification*

The research used in this research is analytical descriptive, which describes the applicable laws and regulations related to legal theories and law enforcement practices concerning the above problems) [5], namely regarding the implementation of criminal jurisdiction enforcement against cybercrimes in international law.

### *C. Research Stage*

This study uses secondary data types, secondary data, namely data obtained from library research and documentation which is the result of research and processing belonging to other people who are already available in the form of books and documentation. Secondary data consists of:

*1) Primary legal material:* Primary legal materials are laws and regulations relating to the object of research, namely: Kitab Undang-Undang Hukum Pidana, Undang-Undang Nomor 8 Tahun 1981 about Hukum Acara Pidana, Undang-Undang Nomor 36 Tahun 1999 about Telekomunikasi, Undang-Undang Nomor 11 Tahun 2008 about Informasi dan Transaksi Elektronik, Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi, Undang-undang Nomor 8 tahun 2010 about Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, Undang-Undang Nomor 19 tahun 2016 about Perubahan Atas Undang-Undang Nomor 11 tahun 2008 about Informasi dan Transaksi Elektronik, Peraturan Pemerintah Nomor 82 Tahun 2012 about Penyelenggaraan Sistem dan Transaksi Elektronik.

*2) Secondary legal material:* Secondary legal materials are legal materials that provide explanations for primary legal materials, including books on legal science and the writings of experts related to the subject matter.

*3) Tertiary legal materials:* legal materials are materials that provide instructions or explanations for primary and secondary law, including books, journals, internet, dictionaries, and other scientific disciplines that provide explanations that have relevance to the object of the problem being studied [6].

### *D. Data Analysis*

Data analysis used in writing is a qualitative analysis method, namely research that refers to legal norms contained in laws and regulations and court decisions as well as norms that live and develop in society [6]. From the results of the analysis carried out, deductive conclusions are then drawn, which are described in narrative form without using formulas or statistical figures to then draw specific conclusions.

## III. Results and Discussion

### *A. Application of Law Enforcement of Cyber Crime Jurisdiction Reviewed From Transnasional Law*

Law enforcement against cybercrimes in Indonesia is regulated in constitution number 11 of 2008 about Electronic Information and Transaction as amended by constitution number 19 of 2016 about top change constitution number 11 of 2008 about Electronic Information and Transaction.

The example of the case that the researcher describes about cybercrimes is concrete evidence that cybercrimes are still prevalent even though there are laws that regulate this. The examples of cases that the researcher describes about cybercrimes are concrete evidence that cybercrimes are still common even though there are laws that regulate this. New problems arise when this crime involves more than one country (transnational crime), then how is the application of the law to

enforce the jurisdiction of transnational crime in international law. The researcher examines the issue of cybercrime jurisdiction through the approach of jurisdictional principles by Huala Adolf:

1. Territorial Principle, according to this principle, the state has jurisdiction over all matters or events within its territory
2. Personal Principle, is state jurisdiction based on the nationality of the perpetrator of the crime committed.
3. Protection Principle, based on this principle, a state can exercise its jurisdiction over foreign nationals who commit crimes abroad which are suspected to threaten the security interests or vital interests of the state
4. Universal Principle, according to this principle every state has jurisdiction over crimes that threaten the international community.

The implementation of the criminal jurisdiction of a country is closely related to the place where the crime occurred (locus delicti). The means of cyber crime and its media are computers that often use internet media that can be accessed by all human beings in the world, so the determination of locus delicti is the place where the act was committed, the place where the impact of the crime occurred and the tools used in committing the crime. Researchers analyzed using locus delicti theories from Moeljatno who divided this theory into two streams, that is:

1. The flow that determines a place, namely the place where the defendant acts. The theory of the place where the behavior occurs is extended to the theory of the place where the tool is used.
2. Flow that determines in several places, namely the place of behavior and the place where the effect occurs.

The locus delicti theories have an equally important position and can be used to determine the place where the crime occurred according to the characteristics of the crime. The first theory, which is a decisive flow somewhere, is applied to the case examples described in the previous chapter, namely the decision Number 11/Pid.Sus/2018/PN.Sgr and the decision Number 1567/Pid.Sus/2020/PN.Sby. In this example, both of them were tried and decided based on national law without applying international rules/conventions even though the case involved more than one country. So that in the second theory with a decisive stream in several places it is not involved in handling cyber criminal cases, even though in international law there are international conventions that can be used as a basis for reference for cyber crimes involving more than one country.

Legal issues involving more than one country or international legal issues involving countries between countries are covered by law, including the International Court of Justice (ICJ) and the International Criminal Court (ICC). The International Court of Justice (ICJ) was established in 1945, after World War II, in The Hague, Netherlands. Meanwhile, the International Criminal Court (ICC) was established in 2002, and is also domiciled in Den Haag.

In the field of cybercrimes, a regional convention has been established that regulates the need for a criminal policy (legal policy) against cybercrimes. The regional convention is the Convention on Cybercrime produced by the Council of Europe/the convention on telematics crimes in 2001 or referred to as the 2001 Council of Europe Convention.

The solution for non member countries who want to adapt the 2001 Council of Europe Convention, can pay attention to the convention in Chapter III of International Cooperation. Where in the section on general principles concerning international cooperation, the state parties must cooperate with each other in accordance with the requirements through the application of relevant international instruments, agreements agreed on the basis of similar and reciprocal laws, and legislation. domestic, to the widest possible extent for the purpose of investigation or proceedings concerning violations relating to computer systems and data, or for the collection of data in electronic form of a violation

### *B. Obstacles That Occur as Well As Solutions in the Law Enforcement of Cyber Crime Jurisdiction in Terms of Transnasional Law*

The problem of law enforcement against cyber crimes that the researchers examined was not only limited to that, the researchers found significant differences regarding the evidence in conventional crimes with evidence in cyber crimes. The application of evidence, electronic data or electronic evidence has several problems, such as locus delicti (the crime scene), tempus delicti (the time of the crime), the problem of evidence is also a separate problem for law enforcement officers. Jurisdiction of a country recognized by international law in the conventional sense, limited ability of law enforcement in this case Polri investigators in dealing with this cyber crime.

Efforts that can be made by the government as a solution to overcome obstacles in law enforcement against perpetrators of cybercrimes such as preventive efforts or prevention efforts before a crime occurs, among others:

1. Security of Computer Network Software is a preventive measure that can be taken in the context of securing computer network software, such as regulating access (access control), through an authentication mechanism using a password. Firewall, a program which is a device that is placed between the internet and the internal network that functions to prevent access into and out of unauthorized persons. Intruder Detection System (IDS), including Autobase, detects probing by monitoring log files. Regular backup, for backup when our system is successfully entered by other parties. (intruders) etc.

2. The government together with law enforcement officials need to immediately take countermeasures and law enforcement, namely by socializing, realizing and implementing various existing laws and regulations such as the Criminal Code and the ITE Law to ensnare the perpetrators of cyber crime.
3. The existence of special laws and regulations governing the cyber world and the institutions that will carry out the regulations, namely the police, prosecutors and special judges who specifically deal with cyber crime as well as facilities or means to support the implementation of these regulations. Legal awareness of the people affected by the regulations.
4. Implement international cooperation and apply international principles that can be recognized as international customs for law enforcement, considering that modern crimes have crossed national borders so it is necessary to make bilateral agreements to overcome them and overcome any problems involving between countries, especially cyber crime.

That Efforts can be made by the government as a solution to overcome obstacles in law enforcement against perpetrators of cybercrimes such as preventive efforts or prevention efforts before a crime occurs. The solution to overcome obstacles in law enforcement against cybercriminals in addition to preventive efforts is also repressive measures, namely the efforts made by the government when the crime occurred. This activity is a law enforcement activity that is aimed at reducing, suppressing or stopping criminal acts committed by a person or group of people. Repressive activities after a crime has occurred, among other things:

1. Law enforcement operations, collecting materials, securing evidence, arresting suspects in handling, handling conflicts that occur in the crime.
2. Escorting suspects, witnesses or evidence, as well as other tasks as regulated is one of the efforts made after this cyber crime has occurred.
3. A new international organization which specifically deal with problems in the internet world.
4. Synchronize law enforcement mechanisms, legal assistance, extradition, and international cooperation in conducting cyber crime investigations
5. Optimizing in the form of increasing supporting facilities and infrastructure for law enforcers as well as facilities and infrastructure for the community such as the existence of electronic reporting applications, where the public can submit reports online to law enforcement regarding cybercrimes that have occurred.
6. Provide training and skills regarding technology and information on a regular basis to law enforcers in tandem with the development of information technology so as to assist in the law enforcement process and create competent law enforcers in their fields .

## IV. CONCLUSION

Law enforcement on the jurisdiction of cybercrimes in Indonesia is regulated in UU ITE, in UU ITE regulates the regulation of electronic transactions and cybercrimes. But, this law has limitations, these limitations include the absence of ratification of international treaties in the cyber field. So that this result, Cyber law enforcement is limited to extradition agreements and reciprocal agreements between countries that are set forth in a law, where these limitations can become obstacles in law enforcement against cybercrimes.

## REFERENCES

[1] M.R. Ahmad, Cyberlaw dan HAKI dalam Sistem Hukum Indonesia, Refika Aditama, Bandung, 2006, hlm. 1
[2] Putusan Pengadilan Negeri Singaraja Nomor 11/Pid.sus/2018/PN Sgr 24 Mei 2018.
[3] Putusan Pengadilan Negeri Surabaya Nomor 1567/Pid.Sus/2020/PN Sby 5 Oktober 2020
[4] S. Soerjono and M. Sri, Pengantar Penelitian Hukum, Rajawali Press, Jakarta, 2006, hlm.2.
[5] H.S. Roni, Metodologi Penulisan Hukum dan Jurimetri, Jakarta: Ghalia Indonesia, 2009, hlm. 97
[6] A. Zainudin, Metode Penelitian Hukum, Sinar Grafika, Jakarta, Tahun 2009, hlm. 57.