Law Enforcement Jurisdiction In Cybercrime

Irpan
Master of Notarial Sultan Agung Islamic University
irfanmakkarumpa37@gmail.com

Abstract

Crimes using technology, namely information technology, especially computers and the internet have reached an alarming stage. Combating internet crime has become a major portion of national and international law enforcement agencies and intelligence, including business practitioners, merchants, customers, and to the end-user. In most cases, internet crime starts with exploiting hosts and computer networks. The approach method used uses the normative juridical method, the results of the research obtained are that Law Enforcement regarding Cybercrime in Indonesia is manifested in the enactment of Law Number 11 of 2008 concerning Electronic Information and Transactions and has been updated by Law Number 19 of 2016 Amendments to Law Law Number 11 of 2008 concerning Information and Transactions. Electronic where the provisions in criminal law are applied by means of extensive interpretation of laws and regulations that explicitly regulate crimes that attack computers and Jurisdiction related to law enforcement is regulated in 3 (three) areas of law enforcement, First, the authority to make substantive law is called legislative jurisdiction, Second, the authority to judge or apply law is called judicial or applicative jurisdiction. Third, the authority to implement/ enforce legal compliance that he makes is called executive jurisdiction.

Keywords: *Cybercrime; Jurisdiction; Law Enforcement;*

1. Introduction

The development of technology has been so rapid that there have been developments in various aspects of people's lives. Including the business community, while in the trading community these technological advances have been used. Not only what happens in trade traffic, but also in the relationships that occur in these trade relations. Among the activities in trade, banking services are also used, where in this sector too there are developments that also use technological developments.[1]

Currently, a new legal regime has been born, known as cyber law. The term "cyber law" is defined as the equivalent word for Cyber Law, which is currently internationally used for a legal term related to the use of information technology. Another term that is also used is the

1. Loebby Loqman, *Kapita Selekta Tindak Pidana Di Bidang Perekonomian*, Cetakan Pertama, Datacom, Jakarta, 2002, page. 46.

Law of Information Technology, Virtual World Law and Mayantara Law. These terms were born considering internet activities and the use of virtual-based information technology.[2]

From the very beginning, people have always looked for convenience in carrying out activities in achieving life. This has been fulfilled by advances in technology. Even so, people are still not satisfied, so there is always a search for the possibility of convenience in fulfilling their needs. On the other hand, in achieving their needs, someone often does something despicable. Either in the field of trade or in any field where the person carries out his activities. Included in this negative activity are activities in the banking sector. This is because in the banking sector, it is directly engaged in the money sector, so that it has attracted attention, whether in positive business ventures or activities that are negative in nature.

Crime using technology, namely information technology, especially computers and the internet (cyber crime) has reached an alarming stage. The progress of information technology, apart from bringing to the practical world of revolutionary business (digital revolution era), turns out to have a terrible dark side, such as pornography, computer crime, even digital terrorism, trash information wars, and hackers.[3]

The rapid development of telecommunication and computer technology has brought legal development towards the fourth revolution in law enforcement construction in Indonesia. The success of national development requires a requirement for national resilience which is supported by community empowerment, which constitutes a condition for avoiding disturbances and threats, including in the form of crimes. Along with the advancement and development of science and technology in society, this also applies to the development of crime. The crimes committed have taken advantage of and exploited the opportunities provided by the convenience of modern instruments with sophisticated equipment, not traditional anymore. Such a crime is a crime with a new dimension. This term is to indicate a crime related to the development of society in the economic sector in an industrial society, the perpetrators consist of the wealthy, intellectual, and organized (including white collar crime).[4]

Cyber crime or crime in cyberspace is a criminal activity that uses a computer network or computer as a tool, and is used as a target for the place where the crime occurs, also known as virtual world crime. Cyber crime is sometimes technically complex and legally complex. Thus, the rapid advances in information communication technology (ICT) functionality and the inherent disparities between legal systems globally are formidable challenges for first responders,

2. Bonanda Japatani Siregar, Problem dan Pengaturan Cybercrime Melalui Aktifitas Internet Dalam Kasus Sara Di Pilkada Serentak 2018, *Jurnal Penelitian Pendidikan Sosial Humaniora*, Vol. 3. No. 1 2018, page.330-336
3. Ade Maman Suherman, *Aspek Hukum Dalam Ekonomi Global*, Edisi Revisi, Ghalia Indonesia, Bogor, 2005, page. 189.
4. Supanto, Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) dan Antisipasinya Dengan Penal Policy, *Yustisia*, Vol.5 No.1 Januari-April 2016, page.52-70

investigative authorities, forensic interrogators, prosecution agencies and criminal justice administration.[5] Cybercrime is also related to crime which is a process of dehumanization that will undermine trust among people. Corruption can arise through cyberspace that institutionalizes suspicion and creates a deep loss of trust in the organization. Cyber crime (cybercrime) is a new form of threat that has never existed before in the world community. Hacking, cracking, defacing, sniffing, carding, phishing, spaming, or scam are a series of internet crimes that are quite dangerous and have caused real losses to many parties.[6]

With this imbalance, that is, when information technology, in this case computer technology, especially the internet, has developed greatly even in remote villages and has been used as a means and media to commit crimes, our law cannot reach it so that technology criminals have not or even not. cannot be convicted and sentenced for his actions as well as unclear resolution of cases of other technological crimes that occur without our knowledge and without our knowing it.

Combating internet crime has become a major portion of national and international law enforcement agencies and intelligence, including business practitioners, merchants, customers, and end-users. In most cases, internet crime starts with exploiting hosts and computer networks. therefore scammers and entrants are coming across the network, especially networks based on the TCP / IP protocol.[7]

With regard to cybercrime perpetrators who have unique characteristics, the author argues that imprisonment for cybercrime actors as practiced in Indonesia so far is an unwise step. This is due to the mismatch between the characteristics of the perpetrator of a criminal act and the system of guiding prisoners in prisons, so that the objectives of criminalization are regulated in the social law. The author argues that the type of imprisonment can be replaced with social work or supervisory penalties, because there is a match between the characteristics of cybercrime offenders and the criminal paradigm in social work and supervisory penalties, so that the purpose of punishment can be achieved. Social work and surveillance crimes are more humane and prospective than imprisonment. The results of research in several countries, social work punishment and supervision punishment are quite effective in applying to criminals, including cybercrime. In eight countries in the world threatening cybercrime offenders with social work penalties, and this is not against the provisions of the convention on cybercrime.

The purpose of this study is to determine and analyze the jurisdiction of law enforcement regarding cybercrime where computer-related crimes are all forms of crime directed against

5. Brown and Cameron S.D. Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice, *International Journal of Cyber Criminology*, Vol. 9, No. 1, 2015, page. 62
6. Andri Winjaya Laksana, Pemidanaan Cybercrime Dalam Perspektif Hukum Pidana Positif, *Jurnal Hukum Unissula*, Vol 35, No I (2019), page.52-76
7. Rachmat Rafiudin,*Internet Foeronsik,* CV Andi Offset, Yogyakarta, 2009, page.1

computers, computer networks and their users, and traditional forms of crime using or with the help of computer equipment. These crimes can be divided into two categories, namely cybercrime in a narrow sense and in a broad sense. Cybercrime in the narrow sense is a crime against computer systems, while cybercrime in a broad sense includes crimes against computer systems or networks and crimes that use computer facilities.

2. Research Method

The approach method used is juridical normative, namely research by examining library materials (secondary data) or library law research.[8] The legal approach method is as a norm system building. The norm system in question is about the principles, norms, rules of legislation and doctrine. Normative juridical research examines the rule of law as a system building related to certain legal events. The type of data used in this research is secondary data which consists of primary legal materials, secondary legal materials, and tertiary law materials obtained from books, literature, papers, journals, laws and regulations, and other data sources. Secondary data collection was carried out using a literature approach method. The collection of legal materials is done by conventional search, collection and study of documents such as reading, viewing, listening, and information technology.

3. Result and Discussion.

1. Cybercrime Criminal Law Enforcement in Indonesia

The development of the use of information technology (IT) in Indonesia has formed a regime in which all life activities can be carried out on a digital basis. Various facilities can be obtained but various problems will also arise if there is no strong regulation on Information technology. The number of problems is indicated by the increasing number of cybercrime in Indonesia which is very worrying.

To ensure benefit, justice, and balance and harmony, the state (government) has created policies related to criminal acts, both through the Penal policy (the eradication of crime with criminal law) and the non-Penal policy (the eradication of crime without criminal law).[9] One of the government's Penal policies in an effort to eradicate cybercrime (cyber crime) is by issuing Law Number 11 of 2008 concerning Electronic Information and Transactions which was passed on April 21, 2008. This law covers a broad range of matters and is adapted to current needs.[10]

As is known, currently has Law Number 11 of 2008 concerning Electronic Information and Transactions. However, the ITE Law is in fact still unable to solve current problems,

8. Ediwarman, *Monograf Metodologi Penelitian Hukum*, genta Publishing, Yogyakarta, 2016, page.22
9. Widodo, *Aspek Hukum Pidana Kejahatan Mayantara*, Aswaja Pressindo, Yogyakarta, 2013, page.179
10. Ahmad Muyasir, Kejahatan Defecting: Studi Perbandingan antara Undang-Undang ITE dan Hukum Pidana Islam, *Al-Mazahib*, Volume 3, Nomer 1, Juni 2015, page.143-159

especially in the context of building ethics for media users to use social media in accordance with their freedom guaranteed by the constitution. As for the hustle and bustle of this political year, Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions was born (Law Number 19 of 2016). This law is a change from the ITE Law and was born as a constitutional solution from the state to regulate ethics for media users in exercising their freedom on social media and preventing cybercrime in Indonesia.[11]

Relating to cybercrime in Indonesia, until this time the majority of cybercrime has not been regulated in a clear legal norms in the legislation, because it was in prosecuting cybercrime applied the provisions of the Criminal Code and the provisions of the Act beyond the Criminal Code. The provisions in the Criminal Code that can be used to prosecute cybercrime by means of extensive interpretation are provisions on the crime of forgery (as regulated in Article 263 to Article 276), theft (as regulated in Articles 362 to 367), fraud (as referred to regulated in Articles 378 to 395), and the crime of damage to property (as regulated in Articles 407 to 412).[12]

Imprisonment for perpetrators of cybercrime in the Draft Bill is also very dominant, in fact none of the types of crimes that are not punishable by imprisonment. Based on the comparison between the results of a study of the 56 foreign nationals with criminal law provisions in the Indonesian criminal law and the Criminal Code draft above can be seen kind of criminal imprisonment be the most dependable staple in most countries criminal policies.

Completion of cybercrime is an indicator of a decrease in work ability of Indonesian National Police in the investigation, as well as a decrease in the ability of the criminal law in solving the crime. Factors decline in legal ability to solve crimes occur because of the legal structure of the legal function is not developed in parallel so that law enforcement tends to weaken.[13]

The threat of imprisonment for cybercrime perpetrators in the Draft Criminal Code is also very dominant, in fact there is no single type of crime that is not punishable by imprisonment. Based on a comparison between the results of a study of 56 criminal laws of foreign countries with the provisions in Indonesian criminal law and the Draft Criminal Code above, it can be seen that the type of imprisonment is the most reliable principal criminal in the criminal policy of most countries.[14]

11. Achmadudin Rajab, Urgensi Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Sebagai Solusi Guna Membangun Etika Bagi Pengguna Media, *Jurnal Legislasi Indonesia*, Vol. 14 No. 04 Desember 2017, page.463-472
12. Andri Winjaya Laksana, Cybercrime Comparison Under Criminal Law In Some Countries, *Jurnal Pembaharuan Hukum*, Vol V No.2 April-Agustus 2018, page.217-226
13. Mahfud MD, *Politik Hukum Nasional*, Alumni, Bandung, 2000, page. 35
14. Barda Nawawi Arief, *kebijakan legislatif dalam penanggulangan kejahatan dengan pidana*

Based on the description of the criminal law that regulates cybercrime in Indonesia, it can be concluded as follows;

a. In regulating Cybercrime, there are 4 alternative arrangements, namely (1) enforcing the conventional Criminal Code by expanding the meaning of certain terms through legal interpretation, (2) amending the Criminal Code, (3) issuing laws and regulations that specifically regulate crimes that related to computers; and (4) amending the Criminal Code as well as issuing a special law that regulates Cybercrime.
b. The country that regulates cybercrime for the first time in special laws, and has the most laws and regulations governing the world of ”mayantara” (cyberlaw) is the United States. While the country that last issued a Special Law that regulates Cybercrime was Mauritius in 2003 (*The Computer Misuse And Cybercrime Act* 2003)

The material of Law Number 19 Year 2016 ITE in general includes information and electronic documents, sending and receiving of electronic mails, electronic signatures, electronic certificates, and electronic system operations. Based on the description of crime cases and the application of criminal law enforcement above, it can be concluded as follows:

a. Provisions in criminal law are applied by means of extensive interpretation.
b. Laws and regulations that explicitly regulate crimes that attack computers are only the Telecommunications Law. Meanwhile, the only law that specifically regulates computer program piracy is the Copyright Law.
c. The types of punishment imposed are imprisonment and fines.

When compared with the provisions in the Convention on Cybercrime, the forms of cybercrime in Indonesia that have already been tried are data interference (namely cases of breaching the KPU site, Computer Realeted Fraud (namely cases of corruption in several banks), Computer Realeted Forgery, offenses Realeted to infrigement of copyright and related rights (namely the case of piracy of the Word Star computer program version 5.0).[15]

2. Criminal Law Jurisdiction in Cybercrime

Jurisdiction is very crucial and complex, especially with regard to the disclosure of international cybercrime (international cybercrime). With the existence of jurisdiction certainty, a country gets full recognition and sovereignty for its various rules and policies in full. This power must also be respected by every other country as the power possessed by other countries.[16]

The jurisdiction of a country that is recognized by international law in a conventional

penjara. Badan Penerbit Universitas Diponegoro, Semarang, 1996, page.201-202

15. Sri Sumarwani, Tinjauan Yuridis Pemidanaan Cybercrime Dalam Perpektif Hukum Pidana Positif, *Jurnal Pembaharuan Hukum*, Volume I No. 3 September-Desember 2014, page.287-269
16. Yudha Bhakti Ardhiwisastra, 1999, *Imunitas Kedaulatan Negara di Forum Pengadilan Asing*, Alumni, Bandung, page.14

sense, is based on geographic boundaries, while multimedia communication is international, multi-jurisdictional, without borders, so that until now it is not certain how the jurisdiction of a country can be applied to multimedia communication as one of the uses. information Technology.

In relation to the determination of the applicable law, there are several commonly used principles, namely:[17]

1. *Subjective territoriality,* which emphasizes that the validity of the law is determined based on the place where the act is committed and the settlement of the crime is committed in another country.
2. *Objective territoriality,* which states that the applicable law is the law where the main result of the act occurs and gives a very detrimental impact to the country concerned.
3. *Nationality* which determines that the state has jurisdiction to determine laws based on the nationality of the perpetrator.
4. *Passive nationality* emphasizing jurisdiction based on the nationality of the victim.
5. *Protective principle* which states that the law is enforceable based on the desire of the state to protect the interests of the state from crimes committed outside its territory, which is generally used if the victim is the state or the government.
6. *Universality.* The principle of Universality should receive special attention related to legal handling of cyber cases. This principle is also known as "*universal interest jurisdiction*".

At first the principle of Universality stipulated that every country has the right to arrest and punish the perpetrators of piracy. This principle was later expanded to cover crimes against humanity, for example torture, genocide, air hijacking and others. Although in the future the principle of universal jurisdiction may be developed for internet piracy, such as computers, cracking, carding, hacking and viruses, it should be considered that the use of this principle is only applicable to very serious crimes based on developments in international law.

It must be admitted that applying proper jurisdiction to crimes in cyberspace (cybercrime) is not an easy job, because the type of crime is international in nature so that it has a lot to do with the sovereignty of many countries (legal systems of other countries). With regard to this jurisdiction, an important question that must be raised is the extent to which a state has given its authority to the courts to try and punish the perpetrators of criminal acts.

Regarding cyberspace crimes, Darrel Menthe stated that jurisdiction in cyberspace requires clear principles rooted in international law. Furthermore, Menthe stated that by

17. Ahmad M.Ramli, *Perkembangan CyberLaw Global dan Implikasinya Bagi Indonesia*, Makalah Seminar *The Importance of Information System Security in E-Government*,Tim koordinasi Telematika Indonesia, Jakarta, 28 Juli 2004, page.5-6.

recognizing the principles of jurisdiction that apply in international law in cyberspace activities by each country, it will be easy for countries to collaborate in order to harmonize criminal provisions to tackle cybercrime.

This opinion of the Minister can be interpreted that by recognizing the principles of jurisdiction that apply in international law in cyberspace activities by each country, it will be easy for countries to carry out cooperation in order to harmonize criminal provisions to tackle cybercrime.

According to Masaki Hamano, there are three scopes of jurisdiction in cyberspace, as quoted by Barda Nawawi Arief which is owned by a country regarding the determination and implementation of supervision of every event, every person and every object. The three categories of jurisdiction, namely:

1. legislatif jurisdiction or jurisdiction to prescribe;
2. judicial jurisdiction or jurisdiction to adjudicate; And
3. executive jurisdiction or jurisdiction to enforce.

The jurisdiction above relates to the limits of state authority in three areas of law enforcement. First, the authority of making substantive laws (hence, called legislative jurisdiction, or can also be called "formulative jurisdiction"). Second, the authority to judge or apply the law (hence the name judicial or applicative jurisdiction). Third, the authority to carry out / enforce legal compliance that is made by it (therefore, it is called executive jurisdiction) [18]

According to Barda Nawawi Arief, the problem of jurisdiction that stands out is the problem of judicial jurisdiction (the authority to judge or apply the law) and executive jurisdiction (the authority to implement a decision) rather than the issue of legislative jurisdiction (law-making authority). with the territorial sovereignty and the legal sovereignty of each country.[19]

The countries that are members of the European Union (Council of Europe) on 23 November 2001 in the city of Budapest, Hungary have made and agreed on the Convention on Cybercrime which was then included in the European Treaty Series with Number 185. The purpose of the Convention is to protect the public from cybercrime , either through law or international cooperation. This is intended to overcome cyber crime, without reducing the opportunity for each individual to continue to be able to develop creativity in the development of information technology. In Section 3, Article 22 of the Convention is governed by matters of jurisdiction, it is stated:

1. Each Party shall adopt such legislative and other measures as may be necessary to estabilish jurisdiction over any offence estabilished in accordance with Article 2 through 11 of this convention,when the offence is

18. Barda Nawawi Arief, *Kapita Selekta Hukum Pidana*, Citra Aditya Bakti, Bandung, 2003, page.247.
19. Barda Nawawi Arief*, Sari Kuliah: Perbandingan Hukum Pidana*, Raja Grafindo Persada, Jakarta, 2006, page.280.

commited:

a. *In its teritorry; or*
b. *On board a ship flying the flag of that party;or*
c. *On board an aircraft registered under the laws of that party;or*
d. *By one its national,if the offence is punishable under criminal law where it was commited outside the territorial jurisdiction of any state.*

2. *Each party may reserve the right not to apply only in specific cases or conditions the jurisdiction rules laid down in paragrphs 1.b through 1.d of this article or any part there of;*
3. *Each party shall adopt such measures as may be necesarry to estabilish jurisdiction over the offences reffered to in Article 24,paragraph 1, of this convention, in cases where an alleged offender is present in its territory and it does not estradite him or her to another party,solely on the basis of his or her natonality,after a request for extradition;*
4. *This convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law;*
5. *when more than one Party claims jurisdiction over an alleged offence estabilished in accordance with this Convention, the Parties involved shall, where apporiate,consult with a view to determining the most apporiate jurisdiction for prosecution.*

The issue of jurisdiction relates to the ability of a particular forum to hear cases (adjudicate jurisdiction). Jurisdiction in cybercrime can use theory:[20]

1. *The therory of uploader and downloader*.*Uploader* adalah pemberi informasi dan *downloader* adalah penerima transaksi elektronik.
2. *The law of the server*.Jurisdiksi ditentukan dengan menggunakan atau memperlakukan server dimana *webpages* secara fisik berlokasi,yaitu dimana mereka dicatat sebagai data elektronik.
3. *The theory of internasional spaces*, ada usulan bahwa internet dijadikan ruang tersendiri, menjadi ruang ke empat setelah air, darat, dan udara.

Regulations regarding the issue of jurisdiction are important, and in the formation of a special law on cybercrime, it is necessary to think about a form of jurisdiction capable of reaching crimes in the cyber world, considering that this crime has a unique character and is transborder in nature. Thus the application of the universal principle (ubiquity principle) can be used as well as the need for cooperation with other countries.

20. Edmon Makarim, *Kompilasi Hukum Telematika*, Raja Grafindo Persada, Jakarta, 2003, page.305

4. Conclusion.

Law Enforcement regarding Cybercrime in Indonesia is manifested in the enactment of Law Number 11 of 2008 concerning Electronic Information and Transactions and has been updated by Law Number 19 of 2016 Amendments to Law Law Number 11 of 2008 concerning Information and Transactions. Electronic where the provisions in criminal law are applied by means of extensive interpretation of laws and regulations that explicitly regulate crimes that attack computers and Jurisdiction related to law enforcement is regulated in 3 (three) areas of law enforcement, First, the authority to make substantive law is called legislative jurisdiction, Second, the authority to judge or apply law is called judicial or applicative jurisdiction. Third, the authority to implement/ enforce legal compliance that he makes is called executive jurisdiction

BIBLIOGRAPHY

Achmadudin Rajab, Urgensi Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Sebagai Solusi Guna Membangun Etika Bagi Pengguna Media, *Jurnal Legislasi Indonesia*, Vol. 14 No. 04 Desember 2017;

Ade Maman Suherman, 2005, *Aspek Hukum Dalam Ekonomi Global*, Edisi Revisi, Ghalia Indonesia, Bogor;

Ahmad Muyasir, Kejahatan Defecting: Studi Perbandingan antara Undang-Undang ITE dan Hukum Pidana Islam, *Al-Mazahib*, Volume 3, Nomer 1, Juni 2015;

Ahmad M.Ramli, *Perkembangan CyberLaw Global dan Implikasinya Bagi Indonesia*, Makalah Seminar *The Importance of Information System Security in E-Government*,Tim koordinasi Telematika Indonesia, Jakarta, 28 Juli 2004;

Andri Winjaya Laksana, Cybercrime Comparison Under Criminal Law In Some Countries, *Jurnal Pembaharuan Hukum*, Vol V No.2 April-Agustus 2018;

Andri Winjaya Laksana, Pemidanaan Cybercrime Dalam Perspektif Hukum Pidana Positif, *Jurnal Hukum Unissula*, Vol 35, No I (2019);

Barda Nawawi Arief, 1996, *kebijakan legislatif dalam penanggulangan kejahatan dengan pidana penjara*. Badan Penerbit Universitas Diponegoro, Semarang;

Barda Nawawi Arief, 2003, *Kapita Selekta Hukum Pidana*, Citra Aditya Bakti, Bandung;

Barda Nawawi Arief, 2003, *Sari Kuliah: Perbandingan Hukum Pidana*, Raja Grafindo Persada, Jakarta;

Bonanda Japatani Siregar, Problem dan Pengaturan Cybercrime Melalui Aktifitas Internet Dalam Kasus Sara Di Pilkada Serentak 2018, *Jurnal Penelitian Pendidikan Sosial Humaniora*, Vol. 3. No. 1 2018;

Brown and Cameron S.D. Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice, *International Journal of Cyber Criminology*, Vol. 9, No. 1, 2015;

Ediwarman, 2016, *Monograf Metodologi Penelitian Hukum*, genta Publishing, Yogyakarta;

Edmon Makarim, 2003, *Kompilasi Hukum Telematika*, Raja Grafindo Persada, Jakarta;

Loebby Loqman, 2002, *Kapita Selekta Tindak Pidana Di Bidang Perekonomian*, Cetakan Pertama, Datacom, Jakarta;

Mahfud MD, 2000, *Politik Hukum Nasional*, Alumni, Bandung;

Rachmat Rafiudin, 2009, *Internet Foeronsik,* CV Andi Offset, Yogyakarta;

Sri Sumarwani, Tinjauan Yuridis Pemidanaan Cybercrime Dalam Perpektif Hukum Pidana Positif, *Jurnal Pembaharuan Hukum*, Volume I No. 3 September-Desember 2014;

Supanto, Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) dan Antisipasinya Dengan Penal Policy, *Yustisia*, Vol.5 No.1 Januari-April 2016;

Widodo, 2013, *Aspek Hukum Pidana Kejahatan Mayantara*, Aswaja Pressindo, Yogyakarta;

Yudha Bhakti Ardhiwisastra, 1999, *Imunitas Kedaulatan Negara di Forum Pengadilan Asing*, Alumni, Bandung;