The Seybold Report

ISSN 1533-9211

DOI: 10.5281/zenodo.10183881

THE DEVELOPMENT OF CYBER CRIMINAL LAW IN INDONESIA ELECTRONIC INFORMATION AND TRANSACTIONS PERSPECTIVE

ROFIQ RIPTO HIMAWAN [1]*, YUSRIADI [2] and NUR ROCHAETI [3]

[1] Student Doctoral Program in Law, Faculty of Law, Diponegoro University, Jl. Prof. Soedarto, SH., Tembalang, Semarang. *Corresponding Author Email: rofiqriptohermawan@students.undip.ac.id
[2, 3] Lecturers Doctoral Program in Law, Faculty of Law, Diponegoro University, Jl. Prof. Soedarto, SH., Tembalang, Semarang.

Abstract

This study aims to analyze the development of cyber criminals in the development of law in Indonesia. The research method used is jurisid normative with a qualitative design. The results showed that the development of cybercrime types has occurred in Indonesia, such as online pornography, viruses, Trojans, contaminating websites, hacking, piracy software, cyber fraud, DDos attacks, cyber gambling, cyber terrorism and others. Cybercrime law and proper regulations in the ICT sector are considered important in attracting investment and developing an IT-based economy. While Indonesia does not yet have a special cybercrime legal instrument, however, there are several other positive laws that are generally accepted and can be imposed on cybercrime actors, especially for cases that use computers as a means, including: a) Criminal Code, b) Law No. 19 of 2002 regarding Copyright, c) Law No. 11 of 2008 Jo. Law No. 19 of 2016 concerning Electronic Information and Transactions, d) Law Number 15 of 2002 concerning Money Laundering, and e) Law Number 15 of 2003 concerning Eradication of Criminal Acts of Terrorism.

Keywords: Cybercrime, Law, Information and Technology, Legal Development.

A. INTRODUCTION

The development of science and technology that is quite rapid and increasingly sophisticated today, especially in the fields of transportation, communication, and information and with the increasing flow of globalization has caused the territory of one country to another as if without borders so that the movement of people or goods from one country to another is carried out easily and quickly (Sitompul, 2012)

Advances in science and technology, in addition to having a positive impact on human life, also have negative impacts that can harm individuals, society, and/or the country (Arifah, 2011). One of the negative impacts of the advancement of science and technology is the misuse of this scientific and technological advance by certain people as a medium to commit crimes, especially crimes committed through *cyberspace (cyber-crime*) (Brenner, 2007)

The development of information technology in turn changes the order of society and social practice. In fact, it not only ends there, but also changes the reality of economy, culture, politics and also law (Arief, 2000). Therefore, behind its positive benefits, internet technology also on the other hand has a slight negative impact. One of them is used as a means of committing crimes, which is hereinafter known as internet crime or cybercrime (MR, 2012).

Besides being known as *cybercrime*, this term is also called *computer-related* crime, which is a type of human crime committed in the world or the internet through computer means to reap

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10183881

as much profit from others, either by deceiving, lying to the public, breaking into other people's accounts, or by scrambling a country's information system (Fitriani & Pakpahan, 2020). According to Enggarani that this act is carried out by a handful of people who take advantage of it for their own benefit but harm others (Jannah & M. Naufal, 2012). In fact, in some cases, this type of crime has the potential to cause great harm to its victims compared to conventional or traditional types of crime. For example, theft is in *hacking* mode (McQuade, 2009)

The phenomenon of cybercrime (internet) is increasing over time. In fact, the modes of crime are increasingly diverse, ranging from fraud cases to bank account breaches. The forms of fraud also vary, ranging from the use of fake accounts on social media, products that seem to promise gifts to consumers, to fake websites that lure prizes of hundreds of millions of rupiah (Suharyo, 2010). The bank account breach can be in the form of hacking mode by scrambling the Bank's network, and then absorbing customer balances, or also directly breaking into the passwords of certain people who are famous for having "fat" accounts (Widodo, 2013).

Criminality that uses the internet as a medium or often referred to as cyber-crime has soared dramatically (Wibawa, 2017). This is in accordance with the adagium that says that "crime is a product of society itself", where crime with this mode of information technology will increasingly develop in a society that is increasingly accustomed to cyberspace (Sari et al., 2020). In simple terms, the *International Telecommunciation Union* (ITU) suggests that the definition of *cybercrime* is a crime involving a computer either as a tool, target or intermediary to conventional crimes (Raharjo, 2005). Broadly speaking, *cyber-crime* consists of several types, including the following: (Sadino & Dewi, 2021)

a. *Offences against Confidentiality, integrity and Availability of Computer Systems and Data,* is a crime that aims to access, intercept data or systems illegally.
b. *Content Related Offences, is a computer* crime that uses content in a computer for crimes such as pornography, spreading slander, gambling.etc.
c. *Copyright and Trademark Related Offences,* is a crime that infringes copyright or trademark, such as piracy.
d. *Computer Related Offences,* is a crime that uses a computer system to retrieve certain data, such as identity, identification numbers to bank accounts.
e. *Combination Offences,* is a crime that combines *cybercrime* and conventional crimes such as *cyberterrorism, cyberwarfare,* and *cyber laundering*.

The internet, which actually destroys and effectualizes human labor, is actually used for the wrong purpose and harms others (Alfian, 2017). Therefore, to deal with the problem of internet crime (*Cybercrime*), the government issued the ITE Law, namely law No. 11 of 2008 and revised it to Law No. 19 of 2016 concerning Information and Electronic Transactions. The hope is that this rule can reduce and solve the problem of internet crime (Widiyanto, 2017). However, this ITE Law is not a specific criminal act, but also contains government regulations for the management of information and electronic transactions, with the aim of developing optimal and equitable information technology nationally (Maqableh et al., 2021).

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10183881

B. DISCUSSION

1. Regulation of *Cyber-crime* in Indonesian Laws and Regulations

Cyber-crime is any kind of use of computer networks for *high-tech* criminal and/or criminal purposes by abusing the ease of digital technology. In two UN Congress documents cited by Barda Nawawi Arief, on *The Prevention* of Crime and the Treatment of Offenders in Havana Cuba in 1990 and in Vienna Austria in 2000, it explains the existence of two terms related to the definition of *Cyber Crime*, namely *cyber*-crime and *computer related crime*. In *a background* paper for the X/2000 UN Congress workshop in Vienna Austria, the term *cyber-crime* is divided into two categories. First, *cyber*-crime in *a narrow sense* is called computer crime. Second, cyber-crime in a broad sense (*in a broader sense*) is called computer related crime (Zakaria, 2012). The details are as follows:

a. *Cyber-crime in a narrow sense (computer crime): any legal behaviour directed by means of electronic operations that targets the security of computer system and the data processed by them.*

b. *Cyber-crime in a broader sense (computer related crime): any illegal behaviour committed by means on in relation to, a computer system or network, including such crime as illegal possession, offering or distributing information by means of a computer system or network.*

Indonesia does not yet have a special law / cyber law that regulates cybercrime However, there are several other positive laws that are generally accepted and can be imposed on cybercrime perpetrators (Anggraeni & Rizal, 2019), especially for cases that use computers as a means, including:

a. Criminal Code

Articles in the Criminal Code are usually used by more than one Article because they involve several acts as well as articles that can be imposed in the Criminal Code on cybercrime, namely:

1) Article 362 of the Criminal Code is imposed on carding cases where the perpetrator steals someone else's credit card number even though it is not physically because only the card number is taken using card generator software on the Internet to make transactions in ecommerce. After the transaction was made and the goods were delivered, then the seller who wanted to withdraw the money at the bank turned out to be rejected because the cardholder was not the person who made the transaction (Crimes, 2007).

2) Article 378 of the Criminal Code can be charged for fraud by ostensibly offering and selling a product or item by placing an advertisement on one of the websites so that people are interested in buying it and then sending money to the advertiser. But, in fact, the item does not exist. This is known after the money is sent and the ordered goods do not come so that the buyer becomes deceived.

3) Article 335 of the Criminal Code can be imposed on cases of stoning and extortion carried out through e-mails sent by the perpetrator to force the victim to do something according

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10183881

to what the perpetrator wants and if not implemented will have a harmful impact. This is usually done because the perpetrator knows the victim's secret.

4) Article 311 of the Criminal Code may be imposed for defamation cases using Internet media. The mode is that the perpetrator spreads an email to the victim's friends about a story that is not true or sends an email to a mailing list so that many people know the story.
5) Article 303 of the Criminal Code can be imposed to ensnare gambling games carried out online on the Internet with organizers from Indonesia.
6) Article 282 of the Criminal Code can be imposed for the dissemination of pornography as well as pornographic websites that are widely circulated and easily accessible on the Internet. Even though they speak Indonesian, it is very difficult to crack down on the perpetrators because they register the domain outside the country where pornography featuring adults is not prohibited or illegal.
7) Articles 282 and 311 of the Criminal Code may be imposed for cases of dissemination of vulgar personal photos or films of a person on the Internet, for example cases of pornographic videos of students, workers or public officials.
8) Articles 378 and 262 of the Criminal Code can be imposed on carding cases, because the perpetrator commits fraud as if he wants to buy an item and pay with his credit card whose credit card number is stolen.
9) Article 406 of the Criminal Code can be imposed on cases of deface or hacking that make other people's systems, such as websites or programs, malfunction or can be used as appropriate.

b. Law No. 19 of 2002 on Copyright

According to Article 1 number (8) of Law No. 19 of 2002 concerning Copyright, a computer program is a set of instructions that are realized in the form of language, code, scheme or other forms that when combined with computer-readable media will be able to make the computer work to perform special functions or to achieve special results, including preparation in designing these instructions (Gani & Gani, 2019)

Copyright for computer programs is valid for 50 years (Article 30). The price of computer programs / software that is very expensive for Indonesian citizens is a promising opportunity for business people to double and sell pirated software at very low prices. For example, an anti-virus program for $ 50 can be purchased for IDR 20,000.00. Sales at very low prices compared to the original software generate very large profits for actors because the capital spent is no more than RP 5,000.00 per piece. The rampant software piracy in Indonesia, which seems understandable, is certainly very detrimental to copyright owners (Ismoyo, 2014)

The act of hijacking a computer program is also a criminal offense as stipulated in Article 72 paragraph (3), namely "Whoever intentionally and without the right to reproduce the use for commercial purposes of a computer program shall be punished with a maximum imprisonment of 5 (five) years and/or a maximum fine of Rp500,000,000.00 (five hundred million rupiah)."

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10183881

c. Law No. 11 of 2008 Jo. Law No. 19 of 2016 concerning Electronic Information and Transactions

According to Article 1 number (1) of Law No. 19 of 2016 concerning Electronic Information and Transactions, Telecommunications is any transmitting, sending, and/or receiving and any information in the form of signs, gestures, writings, images, sounds, and sounds through wire, optical, radio, or other electromagnetic systems. From this definition, the Internet and all its facilities are a form of communication because it can send and receive any information in the form of images, sounds and films with an electromagnetic system (Vilic, 2017) Misuse of the Internet that disrupts public or private order may be sanctioned by using this Law, especially for hackers who enter other people's network systems as stipulated in Article 22, namely everyone is prohibited from committing acts without rights, unauthorized acts, or manipulating:

1) Access to telecommunications networks
2) Access to telecommunications services
3) Access to special telecommunications networks

d. Law Number 15 of 2002 Concerning Money Laundering

Law Number 15 of 2002 is the most powerful law for an investigator to obtain information about suspects who commit fraud through the Internet, because it does not require long bureaucratic procedures and takes a long time, because fraud is one type of criminal act included in money laundering (Article 2 Paragraph (1) Letter q). This law also regulates electronic evidence or digital evidence in accordance with Article 38 letter b, namely other evidence in the form of information that is spoken, sent, received, or stored electronically with optical devices or similar thereto (Theohary & Rollins, 2015)

e. Law Number 15 of 2003 Concerning the Eradication of Criminal Acts of Terrorism

Law Number 15 of 2003 regulates electronic evidence in accordance with Article 27 letter (b), namely other evidence in the form of information that is spoken, sent, received, or stored electronically with optical devices or similar to it. Digital evidence or electronic evidence plays a very important role in the investigation of terrorism cases, because currently communication between perpetrators in the field and their leaders or intellectual actors is carried out by utilizing facilities on the internet to receive orders or convey conditions in the field because the perpetrators know tracking the internet is more difficult than tracking via cellphones (Ardiyanti, 2016)

2. The Development of *Cyber-criminal* on Legal Developments in Indonesia

One of the most crucial issues that *cybercrime* raises is the issue of jurisdiction relating to the extent to which a state can exercise its legal sovereignty or in other words the extent of a country's ability to hear an internationally nuanced case. Jurisdictional issues in a country can apply its legal sovereignty or in other words the extent of a country's ability to hear an internationally nuanced case (Fitriani & Pakpahan, 2020).

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10183881

Legal regulation on the Internet is still relatively new and growing, there is a global regulatory impulse, but legal sovereignty makes it not easy to implement (Ismail, 2009). This is one of the weaknesses of cybercrime law enforcement, especially when it comes to crimes committed by individuals or business entities located in other countries. The constitution of one country cannot be imposed on another country because it can conflict with the sovereignty and constitution of another country (Subagyo, 2018).

Various types of cybercrime have occurred in Indonesia, such as online pornography, viruses, Trojans, site littering, hacking, software piracy, cyber fraud, DDoS attacks, cyber gambling, cyber terrorism and others. The data available is only from reported crimes, the tip of an iceberg that cannot be used as an actual measure of the actual situation (Gultom & Elisatris, 2005).

In 2003, the Indonesian National Police established an IT and cybercrime unit. Within certain economic and crime sections the Directorate of Criminal Investigations, as well as the cybercrime Unit in Jakarta Regional Police, to deal with the threat of cybercrime. Similar units have been established in several other regional police departments, such as in Bali and East Java. Training to improve the *cybercrime* investigation skills of police investigators continues to be provided, as well as the provision of necessary facilities and infrastructure (Hafidz, 2014).

Cybercrime crimes have the characteristics of not only a national scope but also a global nature that can penetrate time and space, no national borders, do not know jurisdiction, and can be carried out from anywhere and anytime. In 2013 the Ministry of Communication and Informatics provided data that Indonesia was the second contributor to cybercrime attacks after China. Meanwhile, in the midst of the development of the financial system in cyberspace, the latest research from Kaspersky Lab. From data from the Consumer Security Risks Survey 2016 conducted by B2B International and Kaspersky Lab, it was revealed that 5 percent of global users have lost money online due to online fraud. The average loss they suffered was Rp 6 million. This shows that new cybercrime in banking has also begun to emerge, not with conventional techniques anymore but by using increasingly advanced applications as well (Putri & Budiono, 2019).

Cybercrime law and proper regulation in the field of ICT are considered important in attracting investment and IT-based economic development (Panjaitan et al, 2005). Cybercrime has the potential to inflict harm on several fronts: political, economic, Socio-cultural, with greater impact than other high-intensity crimes. In the future, it can disrupt the national economy through infrastructure networks based on electronic technology (banking, satellite telecommunications, electricity networks, and aviation traffic networks (Astuti, 2015).

With the rapid development of information technology, it is necessary to pay attention to efforts to improve and improve the National Criminal Code, namely:

1. The increasing prevalence of new crimes that arise as a result of advances in information technology (*cybercrime*), the necessary evidence must be in accordance with the development of science and technology, both with the addition of other technology-based evidence, such as evidence in the form of electronic mail and electronic recordings (Josianto, 2014).

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10183881

2. One of the characteristics of *cybercrime* is to utilize a global telematics (telecommunications, media and informatics) network. The global aspect creates conditions as if the world has no *borders (borderless*) this situation results in perpetrators, victims and places where criminal acts (*locus delicti*) occur in different countries. Therefore, to anticipate this, the implementation of the Criminal Code must be expanded, so that it does not only refer to the principles that have been adopted in article 2-article 9 of the Criminal Code, namely personal principles, territorial principles, and universal principles (Ersya, 2017).
3. To formulate and determine actions that can be subject to criminal sanctions in a relatively new and fast-moving world, it is certainly not an easy job. Therefore, to ensnare perpetrators who commit *cybercrimes*, legal interpretation institutions (interpretation) can be used. This is intended to avoid the emergence of a legal vacuum (Danuri & Suharnawi, 2017).

Although there are already several articles that can ensnare *cybercime* perpetrators, there are still obstacles in implementation in the field, which include the following:

1) Inadequate Legal Tools

Investigators (especially the National Police) make analogies or parables and similarities to the articles in the Criminal Code agree that it is necessary to make a law specifically regulating *cybercrime* (Maskun et al., 2013)

2) Investigator Capabilities

In general, Police investigators are still very minimal in their mastery of computer operations and understanding of computer hacking and the ability to investigate these cases (Wahyudi, 2013)

3) Evidence

The issue of evidence faced in the investigation of Cybercrime is among others related to the characteristics of cybercrime itself, namely; the target or medium of cybercrime is data and or computer systems or internet systems that are easily changed, deleted, or hidden by the perpetrator, *Cybercrime* Often done almost without witnesses, on the other hand, victim witnesses are often far abroad, making it difficult for investigators to examine witnesses and file the results of investigations (Kartiko, 2014).

4) Forensic Computer Facilities

To prove the traces of hackers, and crackers in carrying out their actions, especially those related to programs and computer data, the police facilities are not adequate because there is no forensic computer needed to uncover digital data (Bahri et al., 2019). The development of *cybercrime* types has occurred in Indonesia, such as online pornography, viruses, Trojans, littering sites, hacking, software piracy, cyber fraud, DDoS attacks, cyber gambling, cyber terrorism and others. Cybercrime law and proper regulation in the field of ICT are considered important in attracting investment and IT-based economic development (Napitupulu, 2017).

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10183881

With the rapid development of information technology, it is necessary to pay attention to efforts to improve and improve the National Criminal Code, namely:

1) The increasing prevalence of new crimes that arise as a result of advances in information technology (*cybercrime*), the necessary evidence must be in accordance with the development of science and technology,
2) One of the characteristics of cybercrime is to utilize a global telematics (telecommunications, media and informatics) network.
3) To formulate and determine actions that can be subject to criminal sanctions in a relatively new and fast-moving world, it is certainly not an easy job. Therefore, to ensnare perpetrators who commit *cyber-crimes*, legal interpretation institutions (interpretation) can be used. This is intended to avoid the emergence of a legal vacuum

C. CONCLUSION

Cyber-crime is any kind of use of computer networks for high-tech criminal and/or criminal purposes by abusing the convenience of digital technology. *Cybercrime* is a type of human crime committed in the world or the internet through computer means to reap as much profit as possible from others, either by deceiving, lying to the public, breaking into other people's accounts, or by scrambling the information system of a country. Indonesia does not yet have a special law / cyber law that regulates cybercrime However, there are several other positive laws that are generally accepted and can be imposed on cybercrime perpetrators, especially for cases that use computers as a means, including:

a) The Criminal Code,
b) Law No. 19 of 2002 concerning Copyright,
c) Law No. 11 of 2008 Jo. Law No. 19 of 2016 concerning Electronic Information and Transactions,
d) Law Number 15 of 2002 concerning Money Laundering, and
e) Law Number 15 of 2003 concerning the Eradication of Criminal Acts of Terrorism.

The development of *cybercrime* types has occurred in Indonesia, such as online pornography, viruses, Trojans, littering sites, hacking, software piracy, cyber fraud, DDoS attacks, cyber gambling, cyber terrorism and others. Cybercrime law and proper regulation in the field of ICT are considered important in attracting investment and IT-based economic development.

With the rapid development of information technology, it is necessary to pay attention to efforts to improve and improve the National Criminal Code, namely:

1) The increasing prevalence of new crimes arising as a result of advances in information technology (cybercrime), the necessary evidence must be in accordance with the development of science and technology,
2) One of the characteristics of cybercrime is to utilize telematics networks (telecommunications, media and informatics) global.

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10183881

3) To formulate and determine acts that can be subject to criminal sanctions in a relatively new and fast-moving world, is certainly not an easy job.

Therefore, to ensnare perpetrators who commit *cybercrimes*, legal interpretation institutions (interpretation) can be used. This is intended to avoid the emergence of a legal vacuum.

Bibliography

1) Alfian, Muh. (2017). Penguatan Hukum Cyber Crime Di Indonesia Dalam Perspektif Peraturan Perundang-Undangan. *Jurnal Kosmik Hukum*, *17*(2).
2) Anggraeni, R. D., & Rizal, A. H. (2019). Pelaksanaan Perjanjian Jual Beli Melalui Internet (E-Commerce) Ditinjau Dari Aspek Hukum Perdataan. *SALAM: Jurnal Sosial Dan Budaya Syar-i*, *6*(3), 223–238.
3) Ardiyanti, H. (2016). Cyber-security dan tantangan pengembangannya di indonesia. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *5*(1).
4) Arief, B. N. (2000). *Tindak Pidana Mayantara, Perkembangan Kajian CyberCrime di Indonesia*. PT. Raja Grafindo Persada.
5) Arifah, D. A. (2011). Kasus Cybercrime Di Indonesia Indonesia's Cybercrime Case. *Jurnal Bisnis Dan Ekonomi (JBE)*, *15*(3).
6) Astuti, S. A. (2015). Law Enforcement of Cyber terrorism ini Indonesia. *Jurnal Rechtsidee*, *2*(2).
7) Bahri, S., Yahanan, A., & Trisaka, A. (2019). Kewenangan Notaris Dalam Mensertifikasi Transaksi Elektronik Dalam Rangka Cyber Notary. *Repertorium: Jurnal Ilmiah Hukum Kenotariatan*, 142–157.
8) Brenner, W. (2007). *Cybercrime: Re-Thinking Crime Control Strategies, dalam Yvonne Jewkes*. Willan Publishing.
9) Crimes, L. on C. (2007). *Alongwith IT Act and Relevant Rules,*. Book Enclave.
10) Danuri, M., & Suharnawi. (2017). Trend Cyber Crime Dan Teknologi Informasi Di Indonesia. *Jurnal INFOKAM*, *XIII*(2).
11) Ersya, M. P. (2017). Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia. *Journal of Moral and Civic Education*, *1*(1).
12) Fitriani, Y., & Pakpahan, R. (2020). Analisa Penyalahgunaan Media Sosial untuk Penyebaran Cybercrime di Dunia Maya atau Cyberspace. *Analisa Penyalahgunaan Media Sosial Untuk Penyebaran Cybercrime Di Dunia Maya Atau Cyberspace*, *20*(1).
13) Gani, H. A., & Gani, A. W. (2019). *Penyelesaian Kasus Kejahatan Internet (Cybercrime) dalam Perspektif UU ITE No.11 Tahun 2008 dan UU No.19 Tahun 2016* (p. 121). Prosiding Seminar Nasional LP2M UNM.
14) Gultom, D. M. A. M., & Elisatris. (2005). *Cyber Law (Aspek Hukum Teknologi Informasi)*. Rafika Aditama.
15) Hafidz, J. (2014). Kajian Yuridis Dalam Antisipasi Kejahatan Cyber. *Jurnal Pembaharuan Hukum*, *1*(1).
16) Ismail, D. E. (2009). Cyber Crime di Indonesia. *Jurnal Inovasi*, *6*(03).
17) Ismoyo, D. W. (2014). Kendala Penyidik Dalam Mengungkap Tindak Pidana Penipuan Online Melalui Media Elektronik Internet (Studi di Polres Malang Kota). *Jurnal Hukum Universitas Brawijaya Malang*, *2*(1).
18) Jannah, H. S., & M. Naufal. (2012). Penegakan Hukum Cyber Crime Ditinjau Dari Hukum Positif Dan Hukum Islam. *Jurnal Al-Mawarid*, *XII*(1).
19) Josianto, A. (2014). Tindak Pidana Cyber terrorism Dalam Transaksi Elektronik. *Jurnal Lex Administratum*, *3*(3).
20) Kartiko, G. (2014). *Pengaturan Terhadap Yurisdiksi Cyber Crime Ditinjau dari Hukum Internasional*.

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10183881

Politeteknik Negeri Malang.

21) Maqableh, M., Obeidat, A., & Obeidat, Z. (2021). Exploring the determinants of internet continuance intention and the negative impact of internet addiction on students' academic performance. *International Journal of Data and Network Science*, *5*(3), 183–196. https://doi.org/10.5267/j.ijdns.2021.6.014

22) Maskun, M., Manuputty, A., Noor, S. M., & Sumardi, J. (2013). Kedudukan Hukum Cyber Crime Dalam Perkembangan Hukum Internasional Kontemporer. *Masalah-Masalah Hukum*, *42*(4), 511–519.

23) McQuade, S. C. (2009). *Encyclopedia of Cybercrime. USA: Greenwood Pers The Concise Oxford Dictionary of Current English. (8th edition). 1990*. Clarendon Press.

24) MR, A. (2012). Yuridiksi dan Transfer of Procedding Dalam Kasus Cybercrime. *Tesis, Program Studi Magister Hukum Universitas Indonesia*.

25) Napitupulu, D. (2017). Kajian Peran Cyber Law Dalam Memperkuat Keamanan Sistem Informasi Nasional. *Deviance Jurnal Kriminologi*, *1*(1), 100–113.

26) Panjaitan, H. I., & Dkk. (2005). *Membangun Cyber Law Indonesia Yang Demokratis*. IMLPC.

27) Putri, C. C., & Budiono, A. R. (2019). Konseptualisasi Dan Peluang Cyber Notary Dalam Hukum. *Jurnal Ilmiah Pendidikan Pancasila Dan Kewarganegaraan*, *4*(1), 29–36.

28) Raharjo, B. (2005). *Keamanan Informasi Berbasis Internet*. PT. Insan Indonesia.

29) Sadino, S., & Dewi, L. K. (2021). Internet Crime Dalam Perdagangan Elektronik. *Jurnal Magister Ilmu Hukum*, *1*(2), 9–17.

30) Sari, D. C., Effendy, F., Sudarso, A., Abdillah, L. A., Fadhillah, Y., Fajrillah, F., Setiawan, Y. B., Simarmata, J., Watrianthos, R., & Jamaludin, J. (2020). *Perdagangan Elektronik: Berjualan di Internet*. Yayasan Kita Menulis.

31) Sitompul, J. (2012). *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana.* PT. Tatanusa.

32) Subagyo, A. (2018). Sinergi Dalam Menghadapi Ancaman Cyber Warfare. *Jurnal Pertahanan & Bela Negara*, *5*(1), 89–108.

33) Suharyo. (2010). *Laporan Penelitian Penerapan Bantuan Timbal Balik Dalam Masalah Pidana Terhadap Kasus-kasus Cybercrime*. BPHN Departemen Hukum dan HAM RI.

34) Theohary, C. A., & Rollins, J. W. (2015). *Cyberwarfare and Cyber terrorism: In Brief.* Congressional Reseach Service.

35) Vilic, V. (2017). *Cyber terrorism on The Internet and Social Networking: A Threat to Global Security. International Scientific Confrence on Information Technology and Cata Related Research Serbia*. Singidunum University.

36) Wahyudi, D. (2013). *Perlindungan Hukum Terhadap Korban Kejahatan Cyber Crime Di Indonesia*. Jurnal Ilmu Hukum Universitas Jambi.

37) Wibawa, I. (2017). Cyber Money Laundering (Salah satu bentuk White Collar Crime abad 21). *YUDISIA*, *8*(2), 241.

38) Widiyanto, B. (2017). Dampak Serangan Virtual ISIS Cyber Calipathe Terhadap Amerika Serikat. Jurnal International & Diplomacy. *Universitas Paramadina Jakarta*, *2*(2).

39) Widodo. (2013). *Hukum Pidana di Bidang Teknologi Informasi, Cybercrime Law: Telaah Teoritik dan Bedah Kasus.* Aswaja Pressindo.

40) Zakaria. (2012). Analisis Hubungan Hukum Dan Akses Dalam Transaksi Melalui Media Internet. *Jurnal Hukum*, *2*(2).