

The Electronic and Transactions Law (EIT Law) as the First Cyber crime Law in Indonesia: An Introduction and Its Implementation

Mahrina¹, Joko Sasmito², Candra Zonyfar³

Jokosasmito112233@gmail.com

² Universitas Buana Perjuangan Karawang

Article Info

Received: 15 -12 - 2022

Revised: 29 - 12- 2022

Accepted: final ready to publish

Keywords:

Cybercrime, Cyberspace, EIT Law, National interest, Technology and internet development,

Abstract

The cybercrime cases across the country are remaining high. It caused the government decided to create the cybercrime law, including the Indonesian government. The first cybercrime law that created by Indonesian government is the Electronic and Transactions Law (EIT Law) of 2008, and revised in 2016. This paper then provides more comprehensive explanation regarding EIT Law, starting from its creation, substances, enforcement, and even its strengths and weaknesses. By using literature review method, the authors have been conducted research from the previous studies on related topic. Before entering the main discussions, this paper also explains the cybercrime law and policy in Indonesia's neighboring countries. After that, EIT Law is explained comprehensively. The result shows that background of the creation of EIT Law is the technology and the Internet development that can threaten the Indonesia's national interests. This law then categorize the types of cybercrime that prohibited in Indonesia. The jurisdiction, the investigation process, and the punishment to cyber criminals also regulated in that law. Furthermore, this paper also explains the strengths and weaknesses of EIT Law. The strengths of EIT Law can be seen in the complexity of the articles that contain within it. Nevertheless, the implementation of this law is still not effective.

I. Introduction

Nowadays, each person can communicate across the world easily through the technology and the Internet. This phenomenon then created the virtual world,

or commonly defined as cyberspace. However, major conflicts are emerged regarding how to regulate the Internet in order to prevent public wrongs which encompassed by cybercrime [1]. Cybercrime is a crime that execute using technology, computers, and the Internet. This crime can be categorized into three types, including (1) conventional crimes using the computers, such as piracy, forgery, theft of information or intellectual property, and digital child pornography; (2) attacks on the victim's computer networks; and (3) conventional criminal cases in which evidence exists in the form of digital [2].

The targets of cybercrime can range from government, multinational corporations, and even individual. In this context, the institutional level of cybercrime usually targeting governments, institutions, and multinational corporations which initiated by hackers or cyberterrorist. Meanwhile, the individual level of cybercrime has a purpose to attacking a specific target or person [3]. The globalization then triggered the development of several online groupings and the rise of numerous professional cybercriminal, in which these cybercrime actions join together in plots [4]. Through analyzing the data from 124 countries, it can be said that the main factors which influence the cybercrime are the technological and economic capital [5].

Cybercrime gives big consequences for each country which became the victims of these crimes. A report from the Center for Strategic and International Studies (CSIS) showed that the estimation of cost from cybercrime and espionage is \$445 billion annually worldwide [6]. Furthermore, a group of computer scientists and criminologists estimated that during the 2010s, the global cost of cybercrime could reach \$75 billion and even \$225 billion if including traditional crimes that are transforming to cyber technologies [7].

As a consequence, cybercrime began to joining the top list of security concerns for many countries [8, 9]. The government in these countries then give their attention to design cybersecurity policies. They also allocate billions of dollars to building new programs to strengthen the national ability in addressing the risks from cyberspace. Nowadays, there are many countries that decided to create cybercrime law to handle cybercrime, including Indonesia. In this country, the regulation regarding cyberspace—and also cybercrime—was arranged in the Electronic Information and Transactions Law (EIT Law).

Therefore, the literature review of this paper covered several studies regarding the cybercrime law or cybercrime policy in Indonesia. However, these studies focused only on reviewing the cybercrime law and policy in general [10][11][12][13][14]. Furthermore, there are numerous studies that have a limited scope, such as discuss strengthening the cybercrime law [15][16] and the problems of cybercrime law in Indonesia [17][18]. This paper then provides

a more comprehensive review concerning the cybercrime law in Indonesia, especially the EIT Law. The rest of this paper is organized as follows. In section 2, the authors explain first about the cybercrime law and policy in Indonesia's neighboring countries, such as Australia, Malaysia, Singapore, Thailand, Philippine, Vietnam, and Timor-Leste. Section 3 then explains the cybercrime law in Indonesia, that is EIT Law, which involving its creation, substances, and enforcement. After that, section 4 contains the authors' analysis of the implementation of EIT Law that more focus on the strengths and weaknesses of EIT Law. Section 5 then presents the conclusion of this paper, and also the future work of the EIT Law in Indonesia.

2. Research Method

The research approach that will be used is the doctrinal legal research. more comprehensive explanation regarding EIT Law, starting from its creation, substances, enforcement, and even its strengths and weaknesses. By using literature review method, the authors have been conducted research from the previous studies on related topic. Before entering the main discussions, this paper also explains the cybercrime law and policy in Indonesia's neighboring countries.

3. Results and Discussion

cybercrime law and policies in the neighboring countries

Besides Indonesia, the neighboring countries also tend to create and implement the cybercrime law and policies in order to combat cybercrime. These law and policies are explaining more detail below. Before entering the next discussion, we should know first about number of internet users in Indonesia and its neighboring countries that explain on the table 1.

table 1.
number of internet users (2021)

No.	Country	Total Population	Internet Users
1.	Indonesia	277.58 millions	201.37 millions
2.	Australia	25.92 millions	22.13 milions
3.	Malaysia	32.7 millions	29.03 millions
4.	Singapore	5.92 millions	5.29 millions

5.	Thailand	70.05 millions	48.59 millions
6.	Philippine	111.05 millions	82.41 millions
7.	Vietnam	98.32 millions	68.72 millions
8.	Timor-Leste	1.35 millions	599.7 thousands

A. Australia

Indeed, the Commonwealth Government has enacted the computer-related offenses in 1989, which then modernized by the Cybercrime Act 2001. This act explains about the key offenses that cover unauthorized impairment of electronic communications, and unauthorized access to and impairment or modification of data which held in a computer or other device [19]. The Cybercrime Act then updated search powers in the Custom Act 1901 and the Crimes Act 1914 in order to response to technological developments. Those search powers further amended by the Telecommunications and Other Legislation Amendment Act 2018 (TOLA Act) to enable the officers in accessing the data remotely for the certain duration. Before that, the Commonwealth Government also amended the Privacy Act 1988, which enable affected people to lessen the adverse effects of their personal information. It also can provide more accurate empirical data and strengthen data security practices in several companies and government agencies [20].

B. Malaysia

The Government of Malaysia has already enacted various legislations to handle the cybercrime issues. These legislations are including, (1) the Computer Act 1997 which prevent the unauthorized access to computer, and ensure that someone's password is not given to another one; the Digital Signatures Act 1997 which provide licensing of Certification Authorities (CA), and makes the validation of digital signatures; (3) the Telemedicine Act 1997 which permit the registered doctor and licensed healthcare to practice telemedicine; (4) the Copyright Act (Amendment) 1997 which protects the copyright works; (5) the Communication and Multimedia Act 1998 which provides defines roles and responsibility of people who are providing multimedia and communication services, create a new system of licenses, and eliminate the filter in Internet access; and (6) the Electronic Government Activities Act 2007 which facilitate electronic delivery on government services to the public [21]. Besides that, Malaysia also establish the National CyberSecurity Policy (NCSP) to strengthen the resiliency of the Critical National Information Infrastructure (CNII) in the country [22].

C. Singapore

The Government of Singapore has took several steps to improve the enforcement of cybersecurity laws. In 2013, the Government amended the Computer Misuse Act into the Computer Misuse and Cybersecurity Act (CMCA). It was aimed to strengthen country's capability in responding cyber threats in the national-level. When the cyber threat is detected or happened, the CMCA will empower the Minister of Home Affairs to point out affected people or community to share vital information. The CMCA will also execute numerous necessary measures in order to mitigate the impact of the threat [23]. Besides that, the Government also passed the Cybersecurity Act in 2018 to complement the CMCA. The purpose of this act is to establish a legal framework for the maintenance or oversight of national cybersecurity [24]. It also will equip the Cybersecurity Agency (CSA) with the necessary powers to address cyber threats more effectively.

D. Thailand

The enforcement of cyber law and the investigation of cybercrime is regulated by the Computer Crime Act 2007, which have been amended in December 2016. This law has purpose to protect the computer system from violations, such as illegal accesses. However, the enforcement of the law is quite complicated and even impractical [25]. This is because the police officers or another related official are not informed in many cases, and finally resulting in an improper investigation of cyber criminals. Besides that, the Thailand authorities tend to implement the Computer Crime Act more aggressively, with much greater protections for free speech. It shows that Thailand has failed to comply entirely with the standards of international human rights [25]. Indeed, this law will expand powers of the Thailand authorities because they can engage in surveillance, undermine freedoms to use anonymity and encryption, restrict free speech, and conduct warrantless searches of individual data.

E. Philippine

The Government of Philippine had enacted various special laws relating the technology or cyber aspects. These special laws are including (1) the Special Protection of Children against Abuse, Exploitation and Discrimination Act 1991; (2) the Access Devices Regulation Act 1998;

the Electronic Commerce Act 2000; (4) the Anti-Trafficking in Persons Act 2003; (5) the Anti-Violence against Women and Children Act 2004; (6) the Anti-Photo and Video Voyeurism Act 2009; (7) the Anti-Child Pornography Act 2009; (8) the Data Privacy Act 2012; and (9) the Cybercrime Prevention Act 2012 [26].

However, these laws are not sufficient to deter cybercrime completely, and to protect the national cyberspace. This is because there are no existence of an umbrella agency which focus to address the problems of cyberspace, ill-trained law enforcers, lack of coordination and cooperation between private sector and government, and measly budget earmarked for implementing the cybercrime prevention strategy [27]. Besides that, the public is not fully concern about cybercrime issues that further escalate in this country.

F. Vietnam

During the 1990s, Vietnam faced the online activities that started to emerging in national level. In order to response to this phenomenon, the government then added 'Cybercrime' as one of the crimes in the Criminal codes. On 21 December 1999, the Criminal Code No. 15/1999/QH10 or Criminal Code of Vietnam 1999 was passed by Vietnam National Assembly [28]. It showed that for the first time, the government was succeeded to criminalize various types of cybercrime. However, between 1999 and 2009, there was no case that prosecuted under these articles. This made the articles of the Criminal Code of Vietnam 1999 became very vague and ambiguous. The government then decided to pass the law 37/3009/QH12 on 19 June 2009, which aimed to amend and supplement the national cybercrime law [28]. This law gives more objectivity of crime types, such as telecommunication networks, computer networks, internet, and digital services. Besides that, the new cybercrime law also regulate the base for investigation, prosecution, and trial against cybercrime cases that happened from 2009 to 2017. Nevertheless, many Vietnamese law enforcement officers argue that the realization of this law had many serious loopholes [28].

G. TIMOR-LESTE

The strategy to handling cybercrime was regulated in the draft Criminal Defamation Law, which put forward by the Minister of Justice. This draft aimed to prevent online criticism of public officials by amending Article 187 of the Penal Code about criminal defamation. However, the reintroduction of criminal defamation can give severely impact to freedom of expression, either online or offline. This is because the government tend to criminalizing the critical free speech against political incumbents and public officials [29]. Not only that, the draft Cybercrime Law also raising a concern within the public. This draft was submitted by the national public prosecutor to the Council of Ministers. Different from the previous law, the Cybercrime Law particularly focuses on cybercrime, especially regarding the collection of evidence about these crimes. However, the provisions are lack of specificity, so that it can lead to the misuse to constrain access to information online and freedom of expression [29]. Data Privacy and Protection

Law also still in question. This is because the law can threaten citizens' privacy right and constrain freedom of expression on the Internet, such as social media.

cybercrime law and policy in indonesia: an introduction to the electronic information and transactions law (eit law)

The internet users in Indonesia had reached a peak to the number of 201.37 million users in 2021. Indeed, the COVID-19 pandemic have accelerated digital transformation in Indonesia because of change in consumption behaviors during large-scale social restrictions (PSBB) that imposed by the government. Between March to April 2020, the Ministry of Communication and Information Technology reported that the implementation of PSBB has caused increasing of internet users at the rate of 70 percent [30]. As a consequence, the increase number in internet users led to more cybercrime or cyberattacks cases. In 2019, report from the Indonesian National Cyber and Crypto Agency (BSSN) showed that there are 290 million cases of cyberattacks in this country.

But in 2020, especially from January to April, there is 88 million cybercrime cases involving information gathering, malware attacks, and phishing attempts [30]. Before that, cybercrime cases in Indonesia are remaining high, especially in the form of defamation, hatred comments, online deception, pornography, and related crimes [31]. Historically, there are various cases regarding cybercrime, such as (1) unauthorized use of Mustika Ratu's website domain; (2) attack on the BCA banking internet facilities by making an imitation site; (3) using carding through applying other people's credit cards to make transactions; and (4) commit deface through modify the name of political parties with fruits' name on website of the Indonesian General Election Commission [15].

Furthermore, various institutions also became targets for the cybercrime, such as institutions of banking and financial, health, business, education, and military [18]. The detail information can be seen through figure 1 below.

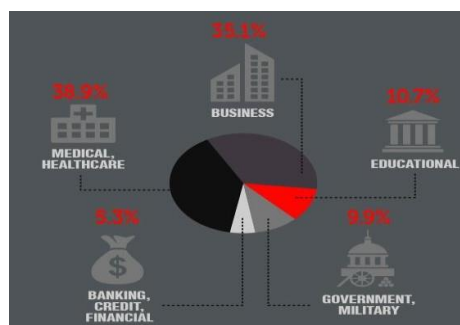


Figure 1. The percentage of cybercrime cases on the various institutions

Indeed, Indonesia was created a legal basis to strengthen cybersecurity, that is the Electronic Information and Transactions Law No. 11 of 2008 (EIT Law), and Law No. 19 of 2016 as a revised version. The explanation about this law can be seen in the following subsections.

THE CREATION

EIT Law states that information technology has to be use securely to keep the information more availability, integrity, and confidentiality [32]. Before EIT Law introduced, there are numerous law or regulation concerning criminal acts that using information technology or internet, such as (1) Law No. 38 of 1999 on Telecommunication; (2) Law No. 19 of 2002 on Copyright; (3) Law No. 25 of 2003 concerning the Amendment of Law No. 15 of 2002 on Money Laundering Crime; (4) Law No. 15 of 2003 on Eradication of the Criminal Act of Terrorism; and (5) Presidential Regulation No. 20 of 2006 on the National Agency for Information and Communication Technology [10, 33].

The EIT Law gives a mandate to various government agencies, such as the Ministry of Defense, to take carefully steps to protect the safety of cyberspace. This is because cyberspace is one of aspects from sovereignty and territorial integrity of Indonesia, as well as the safety of the nation. Besides that, there is also Ministry of Communication and Information Technology, which has a role as the leading government agency to handle cybercrime issues [32]. EIT Law also gives an important mandate to society to build ethics and be more careful during use of social media [34]. The creation of this law was based on Article 28F of the Indonesian Constitution 1945, which stated that each people has right to communicate and acquire information using all kind of availability channels.

Indeed, Indonesia people are really need the creation of EIT Law to regulate their activities in cyberspace. Through this law, they can use and exploring the Internet more safely. This is because the creation of EIT Law was based on the principle of legal certainty and freedom to own technology [35]. Therefore, the implementation of EIT Law is expected to increase the efficiency and effectiveness of public services. The Law also expected to give more opportunity for the society to improve their thinking and ability in utilization of information technology responsibly and optimally [36].

EIT Law is the first cyber law in Indonesia that regulate specifically on the information and transaction technology. The substance of this law is similar to the international regulation on the related contents. Particularly, EIT Law referred to the regulations or principles that were applied by several countries in Europe,

America, and Asia. The regulations are including UNCITRAL Model Law on Electronic Signature, UNCITRAL Model Law on Electronic Commerce, EU Directives on Electronic Signature, EU Directives on Electronic Commerce, and Convention on Cybercrime [37]. The structure of EIT Law can be seen on the table 2 below.

table 2.
the structure of eit law

Chapter	Main Content
Chapter I	General Provisions
Chapter II	Principles and Objectives
Chapter III	Electronic Information, Documents, and Signatures
Chapter IV	Operation of Electronic Certification and Electronic System
Chapter V	Electronic Transactions
Chapter VI	Domain Names, Intellectual Property Rights and Protection of Privacy Right
Chapter VII	Prohibited Acts
Chapter VIII	Dispute Resolution
Chapter IX	Role of the Government and Role of the Society
Chapter X	Investigation
Chapter XI	Penal Provisions
Chapter XII	Transitional Provisions
Chapter XIII	Closing Provisions

The regulation and implementation of EIT Law is based on the principle of *lex specialis derogat legi generali*. It means that law regulation which are specific can be valid, although it contradicts with the general of law regulations [38]. EIT Law had stipulated various types of cybercrime, such as breach of decency, gambling, insulting or defamation, extortion or threat, cyberstalking, spreading of fake news or hoax, hate speech, facilitating criminal acts, and illegal access or interception of the information and computer system [13, 17, 39]. Furthermore, table 3 then categorizes the criminalization based on EIT Law.

table 3. the forms of criminalization in EIT law

No.	Information Technology as Facilities	Information Technology as Object
1.	Article 45 jo Article 27: Breach of decency, gambling, insult or defamation.	Article 46 jo Article 30: Unauthorized access to computer system.
2.	Article 45 (2) jo Article 28: Deception and spreading fake news.	Article 47 jo Article 31: Illegal interception.
3.	Article 45 (3) jo Article 29: Threats of violence.	Article 48 jo Article 32: Data interference.
4.	Article 51 (1) jo Article 35: Falsification of information or electronic documents.	Article 49 jo Article 33: Computer system disruption. Article 50 jo Article 34: Computer abuse.

EIT Law is applied to each people who are conducting cybercrime, either they are in Indonesia or other countries, that give an impact for Indonesia. The law also regulated about the punishment weigh on the cyber criminals. For example, people who committing illegal interception and breaking the electronic information can be imprisoned for 10 years and/or fine IDR 800 millions [15]. The entrepreneurs who provide false information about their products also can be imprisoned for almost 12 years or fine IDR 12 billions. Furthermore, people who distribute information that contain gambling, humiliation, extortion, or threat can be imprisoned for six months or fine IDR 1 billion [15]. The matters of jurisdiction also regulate in EIT Law. This law has applying a universal principle, so that the law is valid for each people who conduct cybercrime, either they are in Indonesia or other countries, in which their actions have a law impact or endanger the national interests of Indonesia [10].

The Enforcement

We can illustrate that the data is a property of person, the site is a house, and the internet is a method. Thus, EIT Law can be seen as a guarantee to make your property and house more safely. The enforcement process of this law is particular, because electronic information or documents are legal evidence within investigation, prosecution, and examination process in court [36]. In Indonesia,

there are three law enforcement officers that have authority to handle cybercrime cases, such as the court, the prosecutor, and the police [40].

Based on Article 42 of EIT Law, the investigation process of criminal offenses are conducted under the provisions of EIT Law and Law No. 8 of 1981 concerning the Criminal Code. The investigation is more specify by EIT Law as follows, (1) the Ministry of Communication and Information Technology and the National Police has role as investigators who handle cyber criminal actions; (2) the investigation process must conduct in the principle of confidentiality, data integrity, protection of privacy, or smooth running of public services; (3) search and seizure of the electronic system regarding an alleged crime should be executed after the chairman of the local district court gives a permission; and (4) the investigator have to protecting the interest of public services during carry out the search and seizure those electronic system [39].

As explained before, EIT Law gives a mandate to the government to protect cyberspace and implement cyber strategy. The Ministry of Communication and Information Technology then created a cybersecurity policy and strategy. This is involving the Directorate of Information Security, the Information Security Coordination Team, and the Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII) [32]. In this context, the Directorate of Information Security has the tasks to formulate and implement cyber policy, give a training, conduct monitoring and evaluation, and reporting about the information security fields. Furthermore, the Information Security Coordination Team was created in April 2010, which has a purpose to coordinate cybersecurity. This team is more focuses on the expertise and practice in the information and technology. ID-SIRTII then established in 2012 to handle the security on internet infrastructure [32].

Not only that, there are also two community organizations that involved to strengthen cybersecurity in Indonesia. The first organization is the Indonesia Communication Emergency Response Team (ID-CERT) which has a role as a supporting institution. It purposes to support the development of Indonesian cybersecurity. Therefore, ID-CERT often working together with the government to handle special cases. The second organization is the Indonesia Academic Computer Security Incident Response Team (ID-ACAD-CSIRT). This is the organization for the universities which focuses on the security development in Indonesia [32].

Implementation of the electronic information and transactions law (eit law): strengths and weaknesses

We know that EIT Law was running since more than two decades. It became the first Indonesian law to handle the cybercrime issues. However, since this law passed by the government, the implementation is often facing various obstacles. In this section, the strengths and weaknesses of EIT Law will be more explained.

The Strengths

EIT Law has a complexity because it regulated numerous aspects involving penal, non-penal, and administration issues. In the Chapter VII, especially from Article 27 to Article 37, the Law lists many of prohibited acts related to cyberspace or electronic system. These prohibited acts are, extortion or threat, gambling, spreading of fake news or hoax, insulting or defamation, cyberstalking, hate speech, breach of decency, facilitating criminal acts, and illegal access or interception of the information and computer system [13, 17, 39].

Furthermore, the provisions within EIT Law are appropriate with several cybercrime regulations in other countries, regions, and even international, such as the Convention on Cybercrime. Based on Article 2, this law applying a universal principle, in which its jurisdiction is extraterritorial. It means that EIT Law is valid for each people who are conducting cybercrime, either they are in Indonesia or another countries, that their actions give negative impact for Indonesia [10]. This is similar with ubiquity principle that aimed to protect the communication or information networks, because these networks had become the national and even international interests. More information concerning the extraterritorial principle of EIT Law can be seen on the figure 2.

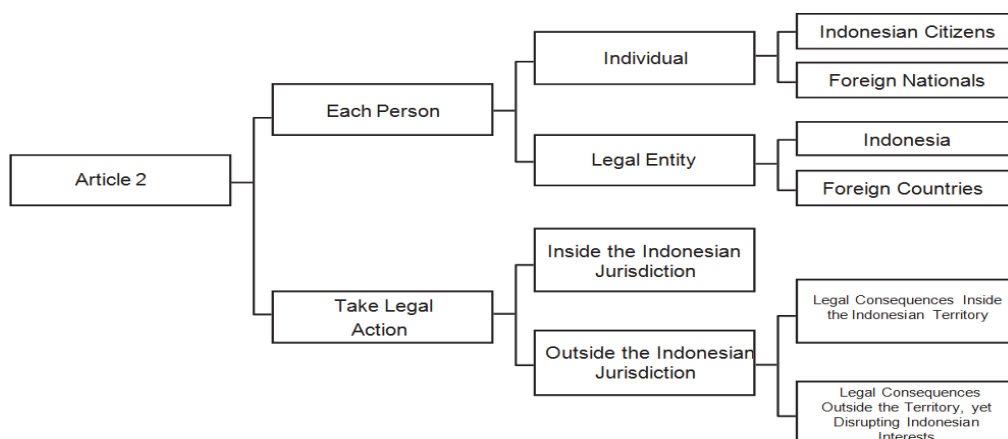


Figure 2. The extraterritorial principle of EIT Law

From figure 2 above, it can be said that EIT Law has expanded the scope of extraterritorial principle regulation within the Indonesian Criminal Law Code. This is because the law added more national interests that have to be protected from cybercrime [37]. Furthermore, the scope of EIT Law is very extensive by including electronic transactions, electronic evidence, privacy, jurisdiction of state, intellectual property, and related issues. This 'all-in-one' regulation is economizing in time because if each of the cases regulate within different laws, it will certainly need more time to be discussed in the Indonesian House of Representatives. Besides that, the government also can observe the whole issues in a more holistic view, and arrange these issues more comprehensively [37].

The Weakness

Although EIT Law has various strengths, but the implementation is still not perfect. This is because there are many obstacles in conducting this law, which finally became the weaknesses of EIT Law. The handling of cybercrime tends to be partial and scattered because there is no standard coordination. Within EIT Law, responses to ever-changing cyber threats are inadequate, especially threats toward critical infrastructure of the national government [30]. It is definitely dangerous because critical infrastructure can become the target of cybercrime. For example is the disruption of Soekarno-Hatta International Airport that happened for a couple of times [32]. It shows that the implementation of cyber defense is not a coordinated national initiative. The steps of implementation are still sectoral, and rely on capability and interests of each sector.

Several articles in EIT Law also problematic and causing different interpretations. This can be seen in Article 27 (1) concerning breach of decency, and Article 27 (3) concerning defamation. In this article, there is no clear explanation about what kind of this defamation and breach of decency actions [41]. Each person who is offended by other persons' words might be feeling mad and report them to police, even though that person is not intended to humiliate him/her. The next ambiguity is the content of Article 29 concerning threats of violence and scare other. However, this article is not explained clearly about what kind of scare people. As a consequence, the effort to warn and admonish other person can be viewed as scare action if that person feels afraid of it [41]. The ambiguity of these articles can trigger negative impacts, such as constrain the freedom of opinion and of expression. Many people even get arrested after express their criticisms on the government.

Given that cybercrime is a new form of crime, EIT Law also facing numerous obstacles in its enforcement against the crime. First, difficulties to present the

victims of cybercrime, especially those who come from another countries. Whereas, the victims also has role as a witness, so that

their testimony became crucial evidence to the cybercrime cases [36]. Second, electrical evidencesometimes difficult to provide. This is because programs and data in the computer can easily move,deleted, duplicated, and manipulated [17, 36].

Third, lack of cyber facilities and infrastructure. In the law enforcement offices, computer facilities are still limited to the needs of cyber operation. The laboratory of cybercrime must be owned by each of police officers, including local police, to accelerate detection and prediction of cybercrime. However, this facility is only owned by police officers that located in the city [13]. Fourth, weakness of mastery in the information technology between the law enforcement officers. This is because there are only few law enforcement officers who mastered of informationtechnology. As a consequence, there may be different interpretation about cybercrime cases that leading to legal uncertainty [36]. Fifth, the law enforcement officers had a lack of awareness regarding cybercrime cases. It leads to the slow respond to the cybercrime reports which provide by the society. They often said that there is no related crime, without doing a further investigation[18].

Although EIT Law has been revised in 2016, but the there are remaining have numerous problems. The Institute for Criminal Justice Reform (ICJR) stated that issues of the revised of EITLaw are including (1) the discussion meeting of EIT Law was held behind closed doors; (2) the revised of EIT Law gives too extensive authority for the law enforcement officers; and (3) the Article 27 (3) that contains about prohibition of spreading defamation and insult information is tending to decrease the punishment period, and it can threaten the freedom of expressions [35]. Therefore, EIT Law still have several issues that must be corrected. This law is not completely resolve the cybercrime cases nowadays, because these cases are higher from year to year.



Figure 3. The percentage of cybercrime cases in Indonesia (2018-2020)

Figure 3 shows that the cybercrime cases in Indonesia are increasing from 2018 to 2020. Thereport from police officers explains that the total cybercrime are 4.360 cases in 2018, 4.586 casesin 2019, and 4.790 cases in 2020 [14]. Indeed, there are many cases which are not involved in thereport. This is because the society often not reported their cases to the law enforcement officers. Sometimes they feel not safe to report cases, or even their trust to the officer is low. The society also feel more suffer because the process of cybercrime investigation is sometimes not free [42]. These problems were made the implementation of EIT Law is still not effective, and this is becomethe main weaknesses of the law.

4. Conclusion

This paper provides a comprehensive review on the cybercrime law and policy in several countries, especially Indonesia. Different from the previous study, this paper provide more complete information regarding the cybercrime law in Indonesia, that is the Electronic Informationand Transactions Law (EIT Law). This information was conducted in the literature review method by collecting and processing various data from the previous studies related to the main topic. From this paper, there are at least three important things to ponder.

First, along with the technology and the Internet development, most countries began to viewed cybercrime as the one of their crucial national threats. This is because cyber criminals can attack vital infrastructures of these countries. Therefore, most countries seek to create various lawand policy to handling threats from cybercrime. This cybercrime law was created and implemented by Indonesia's neighboring countries, such as Australia, Malaysia, Singapore, Thailand, Philippine, Vietnam, and Timor-Leste.

Second, Indonesia was created its first cybercrime law, that is EIT Law, which created in 2008 and then revised in 2016. This law has divided the type of cybercrime which are prohibited in Indonesia, such as breach of decency, gambling, insulting or defamation, extortion or threat, cyberstalking, spreading of fake news or hoax, hate speech, facilitating criminal acts, and illegal access or interception of the information and computer system. Besides that, the Law also regulate the investigation process in the cybercrime cases, and the form of punishment for the cyber criminals, either imprison or fine.

Third, EIT Law have strengths and weakness during its implementation. The contents of thislaw are very complex because it regulated various types of cybercrime, the investigation process,and the punishment to cyber criminals.

Furthermore, the jurisdiction regulated by this law also extensive, because it applied to each person who are conducting cybercrime and has negative impacts for Indonesia. However, EIT Law also has various issues that contribute to its weaknesses. In fact, the implementation of this law is not completely effective. Several articles are not clearly explained, which resulting in the different interpretations. The awareness and capability of the law enforcement officers concerning cybercrime also remaining low.

References

- [1] Alexander, G. (2007). The Emergence of Cybercrime and the Legal Response. *Journal of Security Education*, 2(2), 47-79. http://dx.doi.org/10.1300/J460v02n02_04
- [2] Grabosky, P. (2004). The Global Dimension of Cybercrime. *Global Crime*, 6(1), 146-157. <http://dx.doi.org/10.1080/1744057042000297034>
- [3] Nasi, M., Oksanen, A., Keipi, T., & Rasanen, P. (2015). Cybercrime victimization among young people: a multi-nation study. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, 1-8. <http://dx.doi.org/10.1080/14043858.2015.1046640>
- [4] Lusthaus, J. (2013). How organised is organised cybercrime? *Global Crime*, 14(1), 52-60. <http://dx.doi.org/10.1080/17440572.2012.759508>
- [5] Srivastava, S. T., Das, S., Udo, G. J., & Bagchi, K. (2020). Determinants of Cybercrime Originating within a Nation: A Cross-country Study. *Journal of Global Information Technology Management*, 1-26. <https://doi.org/10.1080/1097198X.2020.1752084>
- [6] Center for Strategic and International Studies. (2014). *Net Losses: Estimating the Global Cost of Cybercrime*. Center for Strategic and International Studies.
- [7] Anderson, R. C., Barton, C., Bohme R., Clayton, R., van Eeten, M., Levi, M., Moore, T., & Savage, S. (2013). Measuring the Cost of Cybercrime. In R. Bohme (Ed.), *The Economics of Information Security and Privacy* (pp. 265-300). Springer.
- [8] Dupont, D. (2019). Enhancing the effectiveness of cybercrime prevention through policy monitoring. *Journal of Crime and Justice*, 1-16. <https://doi.org/10.1080/0735648X.2019.1691855>
- [9] Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*, 1-16. <https://doi.org/10.1080/0960085X.2020.1771222>
- [10] Daud, A. S. (2013). Kebijakan Penegakan Hukum dalam Upaya Penanggulangan Tindak Pidana Teknologi Informasi. *Lex Crimen*, 2(1), 98-112.
- [11] Prastini, E. (2018). Kebijakan Kriminal Pemerintah terhadap Kejahatan Dunia Maya (CyberCrime) di Indonesia. *Jurnal Surya Kencana Dua*, 5(2), 594-610.
- [12] Bunga, D. (2019). Politik Hukum Pidana terhadap Penanggulangan Cybercrime. *Jurnal Legislasi Indonesia*, 16(1), 1-15.

- [13] Liviani, M. R. H. (2020). Kejahatan Teknologi Informasi (*Cyber Crime*) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Al-Qanun: Jurnal Pemikiran dan Pembaharuan Hukum Islam*, 23(2), 400-426.
- [14] Nugraha, R. 2021. Perspektif Hukum Indonesia (*Cyberlaw*) dalam Penanganan Kasus *Cyber* di Indonesia. *Jurnal Ilmiah Hukum Dirgantara*, 11(2), 44-56.
- [15] Enggarani, N. S. (2012). Penanggulangan Kejahatan Internet di Indonesia. *Jurnal Ilmu Hukum*, 15(2), 149-168.
- [16] Alfian, M. (2017). Penguatan Hukum *Cyber Crime* di Indonesia dalam Perspektif Peraturan Perundang-Undangan. *Jurnal Kosmik Hukum*, 17(2), 148-166.
- [17] Ersya, M. P. (2017). Permasalahan Hukum dalam Menanggulangi *Cyber Crime* di Indonesia. *Journal of Moral and Civic Education*, 1(1), 50-62.
- [18] Putra, B. K. B. (2018). Kebijakan Aplikasi Tindak Pidana Siber (*Cyber Crime*) di Indonesia. *Journal of Law*, 1(1), 1-14.
- [19] Department of Parliamentary Services. (2019). *Cybersecurity, cybercrime and cybersafety: a quick guide to key internet links* (Research Paper Series, 2018-2019). Parliament of Australia.
https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1819/Quick_Guides/CybersecurityCybercrimeCybersafety
- [20] Attorney-General's Department. (2013). *National Plan to Combat Cybercrime*. Australian Government. <https://www.homeaffairs.gov.au/criminal-justice/files/national-plan-combat-cybercrime.pdf>
- [21] Jayabalan, P., Ibrahim, R., & Manaf, A. A. (2014). Understanding Cybercrime in Malaysia: An Overview. *Sains Humanika*, 2(2), 109-115
- [22] Ibrahim A., Mahmud, N., Isnin, N., Dillah, D. H., & Dillah D. N. F. (2019). Cyber Warfare Impact to National Security – Malaysia Experience. *Paper of the FGIC 2nd Conference on Governance and Integrity 2019, KnE Social Sciences*, 206-224. <https://doi.org/10.18502/kss.v3i22.5052>
- [23] Cyber Security Agency. (2016). *Singapore's Cybersecurity Strategy*. The Ministry of Communication and Information of Singapore.
<https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy>
- [24] Cyber Security Agency. (2020). *Singapore Cyber Landscape 2020*. The Ministry of Communication and Information of Singapore.
<https://www.csa.gov.sg/News/Publications/singapore-cyber-landscape-2020>
- [25] Article 19. (2017) Thailand: Computer Crime Act.
<https://www.article19.org/data/files/medialibrary/38615/Analysis-Thailand-Computer-Crime-Act-31-Jan-17.pdf>
- [26] Geronimo, L. (). *Cybersecurity and Cybercrime: Philippine Perspective*. Department of Justice of the Republic of the Philippines.
- [27] Li, J. (2021). Cybercrime In The Philippines: A Case Study Of National Security. *Turkish Journal of Computer and Mathematics Education*, 12(11), 4224-4231.
- [28] Luong, H. T., Phan, H. D., Chu, D. V., Nguyen, V. Q., Le, K. T., & Hoang, L. T. (2019). Understanding Cybercrimes in Vietnam: From Leading-Point Provisions to

- Legislative System and Law Enforcement. *International Journal of Cyber Criminology*, 13(2), 290-308. <https://doi.org/10.5281/zenodo.3700724>
- [29] Asia Centre. (2021). Internet Freedoms Under Threat in Timor-Leste. *Submission to the 40th Session of the Universal Periodic Review*. <https://asiacentre.org/wp-content/uploads/Internet-Freedoms-Under-Threat-in-Timor-Leste.pdf>
- [30] Anjani., N. H. (2021). Cybersecurity Protection in Indonesia. *Policy Brief No. 9*, Center for Indonesian Policy Studies.
- [31] Muthia, F. R. & Arifin, R. (2019). Kajian Hukum Pidana pada Kasus Kejahatan Mayantara (Cybercrime) dalam Perkara Pencemaran Nama Baik di Indonesia. *RESAM Jurnal Hukum*, 5(1), 21-39.
- [32] Rizal, M. & Yani Y. M. (2016). Cybersecurity Policy and Its Implementation in Indonesia. *Journal of ASEAN Studies*, 4(1), 61-78.
- [33] Yulianto, A. (2021). Cybersecurity Policy and Its Implementation in Indonesia. *Law Research Review Quarterly*, 7(1), 69-82. <https://doi.org/10.15294/lrrq.v7i1.43191>
- [34] Rajab, A. (2017). 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*, 14(4), 463-472.
- [35] Permatasari, I. A. & Wijaya, J. H. (2019). Implementation of Electronics Information and Transaction in Completion of the Problem of Hate Speech on Social Media. *Jurnal Penelitian Pers dan Komunikasi Pembangunan*, 23(1), 27-41.
- [36] Jhon, R. M. (2018). Existence of Criminal Law on Dealing Cyber Crime in Indonesia. *Indonesian Journal of Criminal Law Studies*, 3(1), 25-34.
- [37] Setiawan, R. (2013). Efektivitas Undang-Undang Informasi dan Transaksi Elektronik di Indonesia dalam Aspek Hukum Pidana. *Recidive*, 2(2), 139-146.
- [38] Gulo, A. S., Lasmadi, S., & Nawawi, K. (2020). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *PAMPAS: Journal of Criminal*, 1(2), 68-81.
- [39] Saragih, Y. M. & Siahaan, A. P. U. (2016). Cyber Crime Prevention Strategy in Indonesia. *SSRG International Journal of Humanities and Social Sciences*, 3(6), 22-26.
- [40] Arisandy, Y. O. (2020). Penegakan Hukum terhadap Cyber Crime Hacker. *Indonesian Journal of Criminal Law and Criminology*, 1(2), 162-169.
- [41] Mainake, Y. & Nola, Y. F. Dampak Pasal-Pasal Multitafsir dalam Undang-Undang tentang Informasi dan Transaksi Elektronik. *Info Singkat: Kajian Singkat terhadap Isu Aktual dan Strategis*, 12(16), 1-6.
- [42] Sumadi, H. (2015). Kendala dalam Menanggulangi Tindak Pidana Penipuan Transaksi Elektronik di Indonesia. *Jurnal Wawasan Hukum*, 33(2), 175-203.