JILS (JOURNAL *of* INDONESIAN LEGAL STUDIES)

NATIONALLY ACCREDITED JOURNAL (SINTA 2)

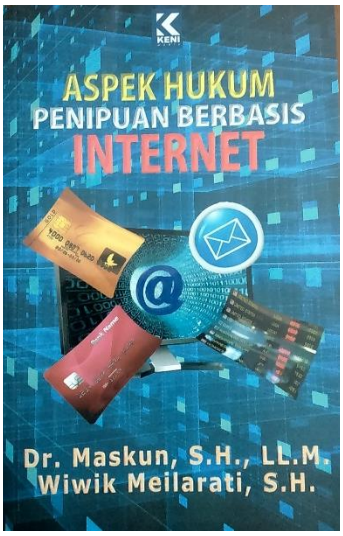
Published by Faculty of Law, Universitas Negeri Semarang, Indonesia
Volume 4 Issue 2, November 2019 ■ ISSN (Print) 2548-1584 ISSN (Online) 2548-1592

BOOK REVIEW

The Aspect of Law in Internet Based Fraud: A Book Review *Aspek Hukum Penipuan Berbasis Internet*, Dr. Maskun, S.H., LL.M., Wiwik Meilarati, S.H., CV Keni Media Makassar, 2016, 238 pages, ISBN 978-602-74375-5-5

Yehezkiel Lemuel
Student at Faculty of Law Universitas Negeri Semarang
✉ yehezkiel_lemuel@students.unnes.ac.id
ORCID: https://orcid.org/0000-0002-7477-3095

HOW TO CITE:
Lemuel, Y. (2019). Internet and Crimes: How the Law Responds to Internet Based Crimes? A Book Review of 'Aspek Hukum Penipuan Berbasis Internet', Maskun & Wiwik Meilarati, CV Keni Media, Makassar, 2016, 238 Pages, ISBN 978-602-74375-5-5. *JILS (Journal of Indonesian Legal Studies)*, 4(2), 343-350. https://doi.org/10.15294/jils.v4i2.34772



REVIEW

GLOBALIZATION HAS BECOME the main factor in the birth of modern technology and the information era. Because of this globalization, technology and information have been a key role in the advancement of a nation.

The writer view that globalization has made the world became borderless and made social conversion became significantly faster. Internet is the proof of this technological development that has created a new world called cyberspace that is the world of communication-based on computers. The person who is in the cyberspace is called netizen.

DATA *of* BOOK

Author(s)	: Dr. Maskun, S.H., LL.M. and Wiwik Meilarati, S.H.
Published Year	: 2016
Title	: Aspek Hukum Penipuan Berbasis Internet
Language	: Indonesia, Bahasa
City Published	: Makassar, South Sulawesi, Indonesia
Publisher	: CV Keni Media
ISBN	: 978-602-74375-5-5
Pages	: 238

In the context of the economy, two points made technology and information considered to be so important in spurring the growth of the world economy, first it increases the demand for technology and information products like computer and modem and the second is to simplify the financial and business transactions. Therefore, technology and information have succeeded in changing people's needs in social and economic sectors to become more efficient and effective.

It can be referred from the description before that there are positive and negative effects of the internet. The positive effects such as the ease of communication, as the search engine facility, to simplify the trades and transactions, etc. While the negative effects like generates the action of cybercrime, one of the examples is hacking activity and changing the behavior of the people into more individuals.

One of the international regulations that will be discussed in the book The *European Union Convention on Cybercrime* or the Budapest Convention of 2001 which contains the forms of cybercrime and the responsibility of the ratifying countries in handling the cybercrime nationally and internationally and Act Number 11 of 2008 concerning Information and Electronic Transaction. But the problem is that do the national regulation even international regulation could follow the advancement of cybercrime. That is the problem that the writers want to solve in this book. So to prevent these cybercrime activities, it is needed legislation that could prevent cybercrime once and for all and the negative effects that are caused by the cybercrime itself.

The definition of technology and informatics or telematics comes from a French word *telematique* which describes the integration of communication network systems and information technology. While information technology refers to the development of information processing devices.

The existence of the telematics system today can't be separated from the long journey of the history itself. It began from prehistoric times until today. It is recorded that the traditional peoples a long time ago had used signs and symbols as a communication tool. The first written form is a pictograph that is used by the Sumerians. Over time, pictograph turned into ideograph then turn into modern alphabets. The evolution of communication using writing is also developed very quickly. It is marked by the invention of Papyrus until the invention of the printing machine by Gutenberg. But the birth of communication technology started with the discovery of electrical connection with magnetism by Oersted which generates the invention of the telegraph, the telephone, radio wave, the radio, and television.

In general, communication technology is a way to process and manipulate data which later data that has been manipulated and processed will be delivered using tools both hardware and software. The purpose is to make communication can run well.

The Internet is a network that has developed throughout the world and has become a necessity for most people in the world. It is a computer-based network that is connected through a communication device. This network can include the Local Area Network (LAN) which is often used internally.

Social Media in the other hand is an online media with its users can easily participate, share and create content in the form of blogs, social networks, forums, etc. Because of the easiness of using social media, the role of conventional mass media became increasingly marginalized. We can see the history of social media started from the first invention of electronic mail, the invention of the website until the establishment of the well-known social media that are still used even today. And the characteristic of social media such as the message delivered is not just for one person but can be to various people, for example, SMS and the message that has been delivered tend to be faster than other media. The growth of social media itself is really fast. It can be seen from the increase in the use of social media which is increasing every year.

Cyber-crime is a crime committed virtually through the internet online. There are some differences between cybercrime and computer crime. If cybercrime is used internet connection so can penetrate until another country but computer crime doesn’t use internet connection or it can use an internet connection but only limited to using the LAN. But these two things can be considered the same because both cause the same legal consequences.

The scope of this crime is also global. This crime is often done transnationally that is covering national boundaries so it is difficult to ascertain the legal jurisdiction of which countries must apply to the perpetrators. The scope of cybercrime itself for example pornography, hijacking, thievery, defamation, etc. These kinds of scope can penetrate the other realm of activities like broadcasting, privacy, decency, and terrorism.

There are seven forms of cybercrime: unauthorized access to computer system and service that is the using of computer system without any permission, illegal contents that is a data entry where the data is not accordance with the law, data forgery that is falsification of important data, cyber espionage, cyber sabotage and extortion that is damaging the program or data by infiltrating a computer virus, offence against intellectual property and infringements of privacy that is dismantling someone's privacy.

According to Barda Nawawi, three main offenses are categorized as cybercrime which refers to the Draft Convention on Cyber Crime by the Council of Europe in 2000. The first offenses are about confidentiality, integrity, and availability of data and computer systems governing about illegal access, illegal interception, data and system interference and misuse of the device. The second offenses are about computer-related, forgery and fraud. The third offenses are about child pornography and the fourth offenses are about infringements of copyright. Some characteristics of the cybercrime itself are illegally done, have to use a device that is connected to the internet, resulting in material or in material losses and the perpetrators are an expert in using the internet.

Cyberlaw is a set of rules made by a particular country regarding crime in technology and information and that only applies to certain communities. Cyberlaw in Indonesia is sourced from Information and Electronic Transactions Act that just exists in Indonesia and has been passed by the People's Representative Council in 2008. The act itself is consists of 13 chapters and 54 articles. It is mainly detailed in the rules of using cyberspace and its transactions and the prohibited acts.

In some countries especially the ASEAN countries like Malaysia, Singapore, Vietnam, and Thailand they have special legislation that regulates cybercrime activity for example in Malaysia there is the *Digital Signature Act 1997* which is to enable businesses and consumers to use electronic signatures. Especially if in the United States that has the UETA or *Uniform Electronic Transaction Act* which regulates the electronic transaction.

The *Council of Europe Convention on Cyber Crime (COECC)* had agreed in Budapest in 2001 that this convention is open to be accessed by any country in the world. The purpose of this convention is to combating cybercrime and by establishing international cooperation.

In the practice of cyber law, Australia has the Act of 1999 concerning online service that gives the rules described in detail with the determination of the Australian Classification Board. It is different in China, that the internet is controlled by the government. But there is still the *Circular of the Public Security Bureau* which contains circulars regarding deviations that are prohibited on the internet which can threaten the unity of China and the government. Although there is no special legislation that regulates the content material on the internet, South Korea had used other laws that is related to cybercrime like the *National Security Law* for blocking political content and also some content that is prohibited on the internet and in the article 7 paragraph 1 set a sentence of up to seven years in prison.

Internet fraud is a crime where the perpetrators develop a form of fraud by using the internet to take other people's property or any interests by providing misleading or not factual information. Internet fraud is also known as an electronic fraud offense that is an action of stealing someone's data access to gain profit. It could be also in the form of buying items on the internet using the credit card without the knowledge of the card owner. Some notable cases of internet fraud in Indonesia like the fraud cases of online shopping through the site www.raseloka.com and BBM social media in 2012 in Pinrang, South Sulawesi which offered fictitious products to customers and loss IDR 4.3 million.

Some forms of internet fraud such as online lottery that is regulated Act Number 22 of 1954 concerning lottery which according to the act, a lottery is a profitability agreement as referred to in article 1774 of the code of civil law. In practice, the lottery is conducted online through email, SMS, etc. Fake online business is usually done by the perpetrators because of its easiness to be practice and three forms of it are cheap credit business, jumble sale, etc. The next practice is phishing which is getting information like username, password, and credit card by posing as a trusted entity. The other practices are program to pay which usually done in social media through e-advertisement and, online dating and fake email services.

They are many kinds of legal basis concerning internet fraud like Convention on Cyber Crime as been said before, the *International Telecommunication Union* that gives the characteristics of cybercrime and gives the guidelines to make the legislation for any countries.

In the international law perspective, there are some efforts by international organizations in preventing the internet fraud like the effort of the United Nations by the Havana 1990 and Vienna 2000 Congress about

The Prevention of Crime and the Treatment of Offenders which has the conclusion that computer-related crime must be criminalized, it is needed the perfect procedural law to investigation and prosecution and there must be international cooperation in handling this case. For the effort of ASEAN is shown by the ASEAN *Regional Forum on Cyber Incident Response Workshop* in Singapore. The forum concludes that cybercrime has to be solved by national and international cooperation. It can be seen that this forum just emphasized to the only hold and build cooperation between countries so there is no legal basis that is strong enough to prevent cybercrime.

In the practice of regulating internet fraud, Indonesia has already have Act Number 11 of 2008 concerning Information and Electronic Transaction. The internet-based fraud is regulated in article 28 paragraph 1 which says that the people who are categorized as the offender is who intentionally and without the right to spread false and misleading news which results in consumer losses in electronic transactions. The offender was sentenced to a maximum of six years imprisonment and or a maximum fine of 1 billion rupiah. And it is officially formed the Indonesia *Security Incident Response Team on Internet and Infrastructure/Coordination Center* (Id-SIRTII) that in charge of supervising internet protocol-based telecommunications network security. Its stakeholders such as the Directorate General of Post and Telecommunication, The Republic of Indonesia Police, Attorney General of the Republic of Indonesia, Indonesian Central Bank and some other organizations.

STRENGTH & WEAKNESS

IN THE FIRST CHAPTER the writers attached the preface in order. The writers also explain the outline of the topics that will be discuss in the book so the readers could know the topics that the book will discuss. But unfortunately, in this chapter 1, the writers made the preface too long and almost the entire contents of the preface only include the topic that will be discuss on the book not included like the purpose of the writers to write the book and what the category of people that suite to read the book. Chapter 2 explains about the definition and the history of the topic that is technology, information and communication and the writers explain the history of the topic coherently according to the period of time and also gives the definition clearly and can be understood easily by the readers but the weakness is that the writers also puts some scientific term that is not explained in the book so it can make it difficult for the reader to understand these terms. Chapter 3 explains about the cybercrime. The writers gave many definitions of cybercrime from the experts so the readers could compare the definitions from those experts and can enrich the readers insight and the writers included the forms of cybercrime clearly. Chapter 4 explains about the cyber law which the writers gave some examples of the cyber law from many countries specifically from the ASEAN region, Asia and well-known countries like United States and the international convention that discuss about cybercrime itself and this examples could make the readers know more about the cyber laws all around the world not just in Indonesia and also the convention that discuss about cybercrime. And the last chapter is about the internet fraud which is the main topic of this book. The writers gave the explanation clearly like the previous chapters along with the legislation so that the readers could the legislation that is applicable from each of the topic but the weakness of chapter 5 is that the author does not explain the topic in briefly so the discussion of the topic is too excessive and make it difficult for the readers to understand the contents of the topic clearly.

CONCLUSION

VARIOUS INTERNET CRIMES such as cyberstalking, internet fraud, website scam, cyber aggression, cyber espionage, and child pornography are new types of crime that have evolved from various types of conventional crimes such as fraud and theft which previously could only be done physically have been switched by using only the internet. This book is expected to be academically useful for undergraduate students and the general public who want to find out about cybercrime and internet fraud specifically. With this kind of situation, it is needed a strong legal basis of law to not just ensure the people's comfort and safety in using the internet but also to crack down the perpetrators assertively so that this action will not be repeated in the future.