



Implementation of E-Commerce Crime Law Enforcement at the West Nusa Tenggara Regional Police

Siti Zahratul Azizah¹; Zainal Asikin²; Lalu Parman²

¹ Postgraduate Program Legal Study and Notaries, Mataram University, Indonesia

² Lecture of Law Faculty Mataram University, Indonesia

<http://dx.doi.org/10.18415/ijmmu.v8i2.2273>

Abstract

This study aims to analyze the implementation of e-commerce criminal law enforcement in the NTB police institution related to how the law enforcement of e-commerce crime in the NTB Regional Police agency and how the legal protection of e-commerce consumers in the NTB Regional Police agency. Through empirical legal research related to law enforcement of e-commerce crimes in the NTB Regional Police. Based on the statutory approach, conceptual approach, and sociological approach to law. The legal basis for law enforcement of the NTB police e-commerce crime is the Criminal Code and Law Number 19 of 2016 concerning Electronic Information and Transactions. Enforcement of criminal law against e-commerce in article 378 of the Criminal Code, the penalty is too light, so the police apparatus uses article 28 paragraph (1) and article 45A paragraph (1) of Law number 19 of 2016 concerning Electronic Information and Transactions. In e-commerce crime, the police have difficulties such as difficulty finding evidence, finding anonymous accounts and electronic identities. In addition, the NTB Police agency does not have the authority to intercept and block accounts used by e-commerce criminals. The NTB Regional Police's legal protection measures for consumers include conducting checks at internet cafes, collecting evidence related to crimes, tracking related crimes, confiscating electronic evidence, disclosing (blocking bank accounts) or detaining based on preliminary evidence or so-called evidence enough.

Keywords: *NTB Regional Police; E-Commerce; Crime Law*

Introduction

E-commerce is a modern business model in addition to promising a number of benefits, but at the same time also has the potential for a number of losses and can open up opportunities for criminals to commit criminal acts. The US Department of Commerce's census body states that:

“Total revenue in e-commerce is \$ 25.8 billion. Legal issues that can arise are when a contract is deemed closed (tijdstip van sluiting van het contract), what is the legality and legality of documents and electronic records without conventional signatures, to what extent is the responsibility of the

internet service provider (ISP) as an intermediary (aansprakelijkheid van tussen personen), and how to protect the rights of consumers in connection with this electronic transaction, such as consumers cannot directly identify or touch the goods to be ordered; unclear information about the products offered and / or there is no certainty whether consumers have obtained various information which deserves to be known or should be needed to make a decision in a transaction.”¹

The cheats that are often found in e-commerce include:

1. Regarding the seller, for example the virtual store seller is a fictitious shop.
2. Regarding goods sent by the seller, for example the goods were not delivered to the buyer, prolonged delays in delivery, damage to the goods delivered or defective items sent, etc.²

Legal issues that can be found in e-commerce transactions include:³

1. The buyer cannot immediately identify, see, or touch the goods to be ordered;
2. Unclear information about the products offered and / or there is no certainty whether the buyer has obtained various information which deserves to be known, or which is duly required to make a decision in a transaction;
3. Unclear legal subject status, of business actors;
4. There is no guarantee of transaction security and privacy as well as an explanation of the risks associated with the system used, especially in the case of electronic payments by credit card or electronic cash;
5. Unbalanced risk imposition, because generally for buying and selling on the internet, the payment has been made in full in advance by the buyer, while the goods are not necessarily accepted or will follow later, because the guarantee there is a guarantee of delivery of goods not receipt of goods;
6. Transactions that cross borderless countries raise questions about how to resolve disputes in the event of a dispute between the parties.

Crime cases or fraud in the e-commerce business have entered areas, namely the jurisdiction of the West Nusa Tenggara police, based on data from preliminary observations or interviews with the Special Criminal Investigator, Subdit V Regional Police of West Nusa Tenggara (NTB), saying that the fraud case or e-commerce business crimes in 2020 there have been six cases per February 2020.⁴

Theoretical Basis

1. Teori Keadilan

a. Teori Keadilan Aristoteles

Aristotle's views on justice can be found in his work *nichomachean ethics*, politics, and rhetoric. Specifically seen in the book *nichomachean ethics*, the book is entirely devoted to justice, which, based on Aristotle's philosophy of law, must be considered the core of his legal philosophy, "because law can only be established in relation to justice".

In essence, this view of justice is a provision of equal but not equal rights. Aristotle distinguished his equal rights from proportional rights. Human rights view equality as a unit or the same container. This is what can be understood that all people or every citizen before the law is the same. Proportional equality

¹ See further <http://www.census.gov/mrts/www/current.html>, accessed 12 March 2020.

² The survey shows that 88.4% of private user respondents are aware of purchases via the internet, but only 16.3% of them use the internet as a means of commerce. The conclusion of research conducted by PT. Pasifik Prima Partners with Mc Kinsey & company Satelindo and APJII. See: *Bisnis Indonesia* 27 November 2000.

³ Abdul Halim Barkatullah & Syahrida, Op cit, p. 35.

⁴ Data from interviews with the NTB Police Criminal Investigation Unit

gives each person what is due according to the abilities and achievements he has done. Furthermore, according to Aristotle's view, justice is divided into two types of justice, "distributief" justice and "commutative" justice.

b. John Rawls's Theory of Justice

According to Rawls, the most basic principle of justice is that everyone has equal rights from their fair positions. According to him, goodness for the whole society cannot override or interfere with the sense of justice of everyone who has obtained a sense of justice, especially those who are weak.⁵ With this concept Rawls leads the public to obtain the principle of fair equality with his theory known as "justice as fairness".⁶

c. Justice in the Pancasila Legal System

Franz Magnis Suseno as quoted by Surajiyo⁷ stated that Frans Magnis Suseno has discussed principle by precept where the demands of justice for the notion of Pancasila are:

1) Belief in the one and only God

The essence of this first principle is that as humans we recognize that we must comply with the awareness of our hearts, believe and respect God Almighty. According to the beliefs of all religions, God's basic requirement of us in our relationships with others is for us to be fair.

2) Just and civilized humanity

Justice here is explicitly mentioned in relation to humanity. To build a humane attitude must be based on justice. Justice is a prerequisite for the normal relationship between humans, because justice demands that we respect the dignity of all other people as human beings. Justice applies to all of us equally, does not discriminate against gender, ethnicity, religion, social class, race and other differences.

3) The unity of Indonesia

Indonesian unity only occurs on the basis of justice. Groups or sections of society who are treated unfairly will not want to unite. Justice requires us to reject all forms of discrimination that threaten the unity of the nation.

4) Community Guided By Wisdom Wisdom In Representative Consultations

The fourth precept expresses the understanding of people's sovereignty. The sovereignty of the people itself is a demand for justice. Democracy as a populist operation is a demand for justice. Every citizen of the community has the right to participate in the deliberations of the whole nation about what he wants together.

5) Social justice for all the people of Indonesia

By social justice, it means that the condition of the whole society is enjoying justice, or not receiving injustice. Social justice means that the structures of the community life processes contained in the political, economic, social, cultural and ideological fields are arranged in such a way that justice is achieved.

⁵ Amran Suadi, *Filsafat Hukum Refleksi Filsafat Pancasila, Hak Asasi Manusia, dan Etika*, Edisi Pertama, PRENADAMEDIA GROUP, Jakarta, p. 119.

⁶ Pan Mohamad Faiz, *Teori Keadilan John Rawls*, dalam jurnal *Konstitusi*, Vol. 6, No. 1, April 2009, p. 135.

⁷ Surajiyo, *Keadilan Dalam Sistem Hukum Pancasila*, Universitas Indraprasta PGRI, IKRAITH-humaira, Vol. 2, No. 3, November 2018, p. 25.

2. Legal Protection Theory

According to Fitzgerald, explaining Salmond's legal protection theory that law aims at integrating and coordinating various interests in society because in a traffic of interests, protection of interests can of course only be done by limiting various interests on other parties.⁸

According to Satjipto Raharjo, legal protection is to provide protection for human rights (HAM) that are harmed by others and this protection is given to the community so that they can enjoy all the rights provided by law.⁹ According to Lili Rasjidi and L. B. Wyasa Putra, they argue that law can be used to realize protection which is not only adaptive and flexible, but also predictive and anticipatory.¹⁰ According to Sunaryati Hartono said that the law is needed for those who are weak and not yet strong socially, economically and politically to obtain social justice.¹¹

Theory of Legal Effectiveness

According to Soerjono Soekanto, the degree of legal effectiveness is determined by the level of public compliance with the law, so that there is an assumption that a high level of compliance is an indicator of the functioning of a legal system. And the functioning of the law is a sign that the law achieves the desired goal, namely trying to defend and protect people in social life.¹² Soerjono Soekanto explained that in the sociology of law, the problem of compliance or legal obedience to the rule of law in general has become a major factor in regulating the effectiveness or failure of these legal rules.¹³

The enforcement of law means that everyone acts as they should, this is a form of compliance and norms implementation. If validity is the quality of law, then the actual quality of human behavior applies.¹⁴ It can be said that legal effectiveness is a reality that occurs in society regarding compliance with the implementation of a legal rule.

Research Methods

1. Type of research

In this study, the type of research used is a type of empirical legal research, namely research that uses empirical facts taken from human behavior, both verbal behavior obtained through interviews and real behavior through direct observation.¹⁵

2. Research approach

a. Statute Approach

The statutory approach is an approach that is carried out by examining all laws and regulations related to legal issues that researchers discussed in the preparation of this legal research. This means that this scientific researcher uses statutory regulations as the initial basis for conducting analysis.¹⁶

⁸ Satjipto Raharjo, *Ilmu Hukum*, PT. Citra Aditya Bakti, Bandung, 2000, p. 53.

⁹ *Ibid*, hlm, 58.

¹⁰ Lili Rasjidi & L.B. Wyasa Putra, *Hukum Sebagai Suatu Sistem*, Remaja Rusdakarya, Bandung, 1993, p. 118.

¹¹ Sunaryati Hartono, *Politik Hukum Menuju Satu Sistem Hukum Nasional*, Alumni, Bandung, 1991, p. 55.

¹² *Ibid*, p. 7.

¹³ Soerjono Soekanto, *Sosiologi: Suatu Pengantar*, Rajawali Press, Bandung, 1985, p. 20.

¹⁴ Jimly Asshidiqie & M. Ali Syafa'at, *Teori Hans Kelsen Tentang Hukum*, 2nd printing, Konstitusi Press, Jakarta, 2012, p. 39.

¹⁵ Mukti Fajar ND & Yulianto Achmad, *Dualisme Penelitian Hukum Normatif & Empiris*, Pustaka Pelajar, Yogyakarta, 2015, p. 185.

¹⁶ *Ibid*, p. 186.

b. Conceptual Approach

The statutory approach is an approach that is carried out by examining all laws and regulations related to legal issues that researchers discussed in the preparation of this legal research. This means that this scientific researcher uses statutory regulations as the initial basis for conducting analysis.

c. Approach to Legal Sociology

It is an approach that analyzes how the reactions and interactions that occur when the norm system works in society. This approach is constructed as a social behavior that is permanent, institutionalized and socially legitimate.¹⁷

3. Types and sources of data

Empirical legal research also uses secondary legal materials as the starting material, then continues with primary legal materials or field data. Thus, empirical legal research still rests on normative premises.¹⁸ In relation to this research, the data sources used are:

a. Primary data

Primary data is data from social facts related to the operation of real laws faced by researchers.¹⁹ Usually, there are at least three types of data collection tools, namely document study or library material, observation or observation and interview or interview.²⁰ Primary data in this study were obtained from interviews or interviews with the Sub-Directorate V Cyber Crime Reskrimus Polda West Nusa Tenggara.

b. Secondary Data

Secondary data is data that is usually used as initial or comparative data. This research departs from social facts referenced from books, research results and scientific journals. Used as result data that supports primary data in the discussion and analysis process.²¹ Data sekunder dikelompokkan menjadi 3 bahan hukum yaitu:

- 1) Primary legal material is binding legal material, and consists of statutory regulations relating to the issue under investigation, among others:
 - a) The 1945 Constitution of the Republic of Indonesia;
 - b) Law No. 39 of 1999 concerning Human Rights, State Gazette of the Republic of Indonesia of 1999 no 165.
 - c) Law No. 19 of 2016 Amendments to Law No. 11 of 2008 concerning Information and Electronic Transactions (ITE).
 - d) Law Number 7 of 2014 concerning Trade.
 - e) Law Number 8 of 1999 concerning Consumer Protection.
 - f) RI Government Regulation Number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions.
- 2) Secondary legal materials are legal materials that provide an explanation of primary legal materials, such as draft laws, research results, works from legal circles, and so on.²²
- 3) Tertiary legal materials are materials that provide directions and explanations for primary and secondary law, for example the Big Indonesian Dictionary, Wikipedia, and so on.

¹⁷*Ibid*, p. 47-48.

¹⁸Amiruddin & Zainal Asikin, *Pengantar Metode Penelitian Hukum*, Cet. 6, Raja Grafindo Persada, Jakarta, 2012, p. 133

¹⁹ Mukti Fajar ND & Yulianto Achmad, *Op. Cit*, p. 59

²⁰ Soerjono Soekanto, *Pengantar Hukum*, UI Press, Jakarta, 2006, p. 66.

²¹ Mukti Fajar ND & Yulianto Achmad, *Op. Cit*, p. 60.

²² Soerjono Soekanto, *Op. Cit*. P. 68

4. Data collection techniques

a. Literature study

Researchers will use literature study by examining legal materials consisting of primary legal materials. Researchers also use secondary legal materials such as draft laws, research results, works from legal circles and tertiary legal materials, namely legal dictionaries, encyclopedias, cumulative indexes and so on.

b. Field Study

Researchers will carry out field studies using data collection techniques by conducting interviews by asking questions to informants and respondents in order to obtain relevant answers related to the problem under study which is determined based on random sampling techniques (by making symbolic appointments). The informants in this study were part of Sub-Directorate V Cyber Crime Reskrimsus Polda West Nusa Tenggara.

5. Data analysis

Primary data and secondary data obtained in this study will be systematically arranged and analyzed. Researchers will analyze the data in a descriptive qualitative way, namely by providing descriptions and explaining in detail and in depth (*verstehen*) to reveal what lies behind real events with the intention of looking for the values contained therein.²³

Result and Discussion

1. Law Enforcement of E-Commerce Crime at Polda NTB

1.1 The Role of the NTB Regional Police in Enforcing E-Commerce Crime

In Law Number 2 of 2002 concerning the State Police of the Republic of Indonesia, it is explained that the main duties of the State Police of the Republic of Indonesia are:

- a) Maintaining public safety and order;
- b) Upholding the law; and
- c) Providing protection, protection and services to the community.²⁴

In order for the implementation of Police duties as described above to run well, the public can obey, respect, and respect the implementation of their duties in the context of law enforcement, by law the Police are given considerable general authority, including:

- a) Receiving reports and / or complaints
- b) Helping to resolve disputes among members of the public that could disrupt public order
- c) Preventing and overcoming the growth of community diseases
- d) Oversee the flow that can cause division or threaten the unity of the nation
- e) Issue a Police regulation within the scope of the Police administrative authority
- f) Carry out special examinations as part of the police action in the context of prevention
- g) Take the first action at the scene

²³ Mukti Fajar ND & Yulianto Achmad, *Op. Cit.*, p. 283.

²⁴ Article 13, Law Number 2 of 2002 concerning the Indonesian National Police

- h) Take fingerprints and other identities and take a picture of someone
- i) Looking for information and evidence
- j) Organizing a National Criminal Information Center
- k) Issuing permits and / or certificates required for public service purposes
- l) Providing security assistance in trials and implementation of court decisions, activities of other agencies, and community activities
- m) Receive and store the findings temporarily.²⁵

Based on the results of the interviews that the author has conducted, the answers to the problems regarding the role of the police in investigating e-commerce crimes are as follows:

a. The legal basis of the NTB Regional Police in law enforcement of e-commerce crimes

1) Criminal Code

In the KUHP, the legal basis used is Article 378 of the Criminal Code²⁶ where there are several main elements, namely:

- a) Benefiting yourself or others against the law;
- b) By using a false name or false dignity; by trickery or a series of lies;
- c) Moving other people to hand over something to him, or to provide debt or write off receivables.

In the case of criminal acts of fraud through e-commerce means, it has the objectives set out in article 378 of the Criminal Code. This goal is to benefit oneself or others against rights, the purpose of which is by using a false name or false situation, or clever intelligence, or false words displayed in electronic information systems.

Whereas the meaning of the word persuade here is to influence people with cunning so that the person obeyed him to do something if he knew what the real case was, he would not do that.²⁷

2) Law Number 19 Year 2016 Concerning Electronic Information and Transactions

Law Number 19 of 2016 concerning Electronic Information and Transactions seems less specific in regulating crimes against E-commerce transactions but through contextual interpretations, several provisions in Law Number 19 of 2016 concerning electronic information and transactions can be applied, one of which is cases of misuse of credit cards in E-commerce transactions. One example is as follows:

The act of "peeking" at another person's credit card "pin" number, either for immediate use or duplication, can be interpreted as theft which can be described as follows:

- a) If the method of "peeking" at the credit card number is done by tapping the transaction activity between the card owner and the online shop via the internet (E-commerce), the perpetrator may be subject to Article 31 paragraph (1) or (2) which regulates the "illegal" problem interception "jo. Article 47 of the ITE Law regulates the sanctions

²⁵ *Ibid*, Article 15

²⁶ Article 378 of the Criminal Code:

Anyone who with the intention of illegally benefiting himself or another person by using a false name or dignity (hoedanigheld); by deception, or a series of lies, moving another person to hand over goods to him, or to give a debt or write off a debt, shall be punished for fraud, by a maximum imprisonment of four years.

²⁷ *Ibid*,

- b) The act of using someone else's credit card number to "trick" the online shop so that the perpetrator can shop for a number of items without paying, may be subject to Article 35 of the ITE Law which regulates the problem of "computer-realistic forgery" jo. Article 51 paragraph (1) regulates the sanctions.

Article 30 Paragraph 3:

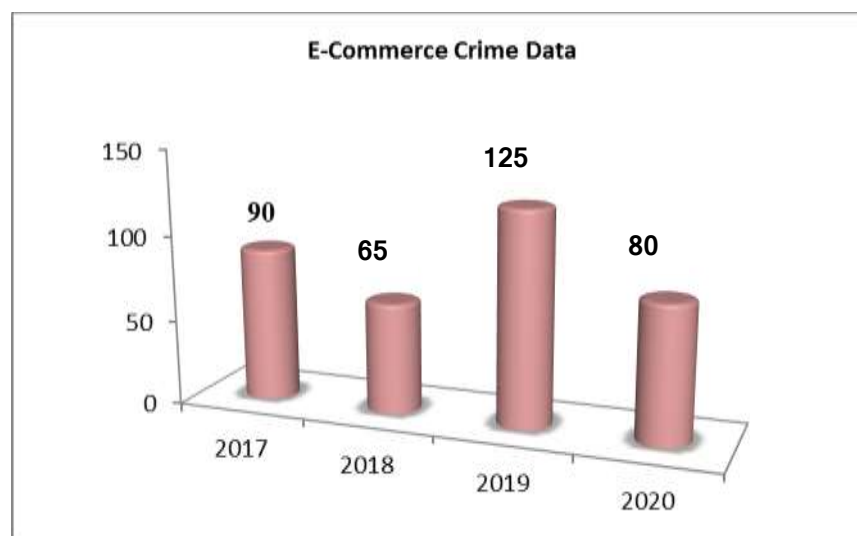
"Anyone who knowingly and without right or unlawfully accesses computers and / or electronic systems in any way by violating, bypassing, bypassing or breaking into security systems (cracking, hacking, illegal access)".

The element that is highlighted in this Paragraph (3) is the element "by violating, breaking through, exceeding, or breaching the security system". In this element, it means that the hackers commit their crimes by breaking into a security system or in computer science it is called a firewall. Hackers use various hacking tool applications to commit their crimes. Where the application is useful for breaking through or breaking into the security system of an electronic system. This can be analogous to entering someone else's house without permission by breaking through the door or window hinges, the penal provisions of which are regulated in Article 167 Paragraph (2) of the Criminal Code.²⁸

b. Investigation Process

In investigating e-commerce cases, the police experience many obstacles and difficulties, because the handling of cases related to cybercrime is different from ordinary or conventional criminal cases. Moreover, the perpetrators of these crimes can carry out the action at any time without the knowledge of other people and use fake accounts. Data on e-commerce crime crimes in NTB continues to grow.

Figure 1. Number of e-commerce crimes in 2017-2020 of the NTB Regional Police's Cyber Crime Crime Unit



Description: Section DIT RESKRIMSUS CYBER CRIME POLDA NTB

²⁸ *Op. Cit.*, Article 167 Paragraph (2) of the Criminal Code:

Anyone who enters by destroying or climbing, using a false key, fake orders or fake evil clothes, or whoever does not know the first right and who does not by mistake enter and is caught there at night, is deemed to have forced entry.

From the data on e-commerce crime, every year there is always a change (increasing and decreasing), in 2017 the number of cases was 90 cases, 2018 65 cases, 2019 there were 125 cases and in 2020 from January to July there were 80 cases of e-crime. commerce. The highest number of cases occurred in 2019 using internet facilities both in the form of fraud and online buying and selling.

In addition to fraud using social networking facilities, there are also scams using website facilities. Website is a place that allows a person or business entity to state himself, his knowledge, the products he sells, and anything that can be accommodated by text, images, writing, video, animation and other multimedia or as a means of buying and selling online for sale.²⁹

The steps taken by the police are:

- a) Conducting checks such as in internet cafes that are usually used by criminals
- b) Collect evidence related to crime
- c) Track related crimes
- d) Confiscate electronic evidence such as hard disks,
- e) Conduct disclosure or detention based on preliminary evidence or sufficient evidence.³⁰

The NTB Police (investigators) in handling e-commerce crimes, the article used to ensnare the perpetrators of e-commerce crime, the suspects charged under Article 28 paragraph (1)³¹ Law number 19 of 2016 concerning Electronic Information and Transactions (ITE) in conjunction with Article 378 of the criminal code on fraud.³²

Article 378 of the Criminal Code regulates:

"Anyone who with the intention of unlawfully silencing himself or another person using a false name or dignity, by deception or a series of lies, moves others to surrender something to him, or to pay a debt or write off a debt, is threatened with fraud. , with a maximum imprisonment of four years. "

Article 28 paragraph (1) of Law No. 19 of 2016 concerning Electronic Information and Transactions regulates:

"Every person knowingly and without right spreads false and misleading news that results in consumer losses in Electronic Transactions".

The prosecution efforts carried out by the police in investigating e-commerce crimes will experience many obstacles where it will be difficult to find the perpetrators where they are because usually the perpetrators use fake accounts and fake identities in making account numbers. So the police action should also urge the public to be more careful in conducting online buying and selling transactions.

²⁹ Budi Suharianto, *Tindakpidana Teknologi Informasi*, (Rajawali Pers, Jakarta, 2013), p. 41.

³⁰ Interview with Kopol Yusuf Taziri, S.I.K on July 7, 2020, at 09.16 Wita, at the Cyber Crime Investigation Satellite Office (CCISO) Laboratory of the NTB Police

³¹ Article 28 paragraph (1) Law Number 19 Year 2016 concerning Electronic Information and Transactions (ITE) reads:

Everyone knowingly, and without right, spreads false and misleading news that results in consumer losses in electronic transactions.

³² Interview with Kopol Yusuf Taziri, S.I.K on July 7, 2020, at 09. 16 Wita, at the Cyber Crime Investigation Satellite Office (CCISO) Laboratory of the NTB Police.

c. Investigation Process

The investigation conducted by the police will trace the source of these electronic documents. In practice, usually investigators will first trace the whereabouts of the perpetrator by tracing the perpetrator's Internet Protocol address ("IP Address") based on the IP address log stored on the website manager server or the home page that the perpetrator uses in committing fraud.

The problem is, investigators will encounter difficulties if the website / homepage is owned outside the jurisdiction of Indonesia (such as Facebook, Google, Twitter, Yahoo, etc.). Although currently APH (Police and Civil Servant Investigator / PPNS of the Ministry of Communication and Information Technology) has collaborated with several website / homepage managers outside the territory of Indonesia. Inter-state governments through their law enforcement officers have made Mutual Legal Assistance ("MLA") agreements or mutual legal assistance agreements, in fact MLA does not automatically apply in every case involving between countries. This jurisdiction issue is often the cause of not being processed and being processed or in particular cybercrime.³³

d. Collection of evidence of criminal acts (e-commerce) at the NTB Police Agency

The E-Commerce Crime Evidence System used in the NTB Regional Police are:

1) Computer crime

Criminal acts in the computer world can be interpreted as a type of crime committed by using the internet as a tool. In the world of the internet, several types of criminal acts can be grouped into the computer category including:

- a) Cyber terrorism
- b) Cyber pornography
- c) Cyber harassment (sexual harassment via e-mail, website, or chat programs)
- d) Cyber stalking (crimes of stalking through the use of computers and the internet)
- e) Hacking (criminal program through the internet)
- f) Carding (credit card crime).³⁴

The form and type of fraud is the theft of money or property by means of a computer against the law, namely in the form of data fraud and program fraud, the details of which are as follows:

- a) Entering unauthorized instructions, namely those carried out by authorized persons or not, who can access a system and enter instructions for their own benefit by unlawfully (eg transfers);
- b) Changing the input data, which is done by someone by entering data to benefit themselves or others by breaking the law;
- c) Damaging data, is done by someone to destroy the print out or output with the intention of obscuring, hiding data or information in bad faith;
- d) The use of computers as a means of committing a criminal act, is in solving information via a computer, the results of which are used to commit crimes or modify programs.

³³ Results of an interview with Kompol Yusuf Tauziri, S.I.K on July 7, 2020, at 09. 16 Wita, at the Cyber Crime Investigation Satellite Office (CCISO) Laboratory of the NTB Police.

³⁴ Didik M. Arief Mansur, *Cyber Law Aspek Hukum Teknologi Informasi*, Aditama, Bandung, 2009, p. 26

- e) The criminal act of fraud, which in fact can include elements of other acts, which are primarily intended to avoid one's obligation, or to obtain something that is not his or her right or possession through deceptive computer means.³⁵
- 2) E-commerce evidence uses an electronic system at the NTB Regional Police

In the Criminal Procedure Code, the regulated evidence is not sufficient to reach the realm of ITE crime. What can be seen from this. If we want to get witness testimony of ITE crimes, the possibility of obtaining evidence is very minimal. This is because seen from the mode of fraud that uses e-commerce facilities, witnesses in transactions tend not to exist, because they make transactions in cyberspace, so that other people cannot know what and how the transaction process is. If you use expert testimony evidence in proving elements of criminal acts in ITE, digital expert statements can be used. But in the case of expert testimony, of course it cannot stand alone without being supported by other evidence, then the expert's statement means nothing if it is not supported by electronic information or data.

For documentary evidence in a criminal act of fraud through e-commerce means, getting it is not as easy as conventional criminal acts. This is because getting authentic evidence is not easy. So maybe it could be corroborated with expert information, but even then it takes a lot of time.

According to the data obtained from Mr. Yusuf Taziri, S.I.K, to be able to be said to be documentary evidence and electronic information including the printed output which will be used as evidence in a criminal case must have the following criteria:

- a) Information and / or electronic documents can be used as evidence if the electronic information and documents use an electronic system in accordance with the provisions stipulated in the ITE Law.
- b) In this regard, before the information and / or electronic documents are used as evidence, expert information from the Ministry of Communication and Information must first be requested whether the electronic information and / or documents use an electronic system in accordance with the provisions stipulated in the ITE Law.
- c) If the Depkominfo expert's statement states that the electronic information and / or documents use an electronic system in accordance with the provisions of the ITE Law, then the information and / or electronic documents can be used as evidence equivalent to the testimony of witnesses, experts, or letters.
- d) If the Depkominfo expert's statement states that the electronic information and / or documents do not use an electronic system in accordance with the provisions of the ITE Law, the electronic information and documents cannot be used as evidence, but only as evidence.³⁶

1.2 Kebijakan Penanggulangan Kejahatan *E-Commerce* (Cyber) Instansi Polda NTB

a. Penal policy

Penal policy is one of the policies in overcoming crime by using criminal law, the policy is operated by implementing criminal law, namely material crime, formal law and penitentiary in society. In essence, criminal law policy is an attempt to realize criminal legislation to suit the conditions at a certain time (*ius constitutum*) and in the future (*ius constituendum*).³⁷

In an effort to tackle cyber crime, the resolution of the VIII / 1990 UN Congress on computer related crimes proposed several policies, including:

³⁵ Niniek Supami, *Cyberspace Problematika Dan Antisipasi Pengaturannya*, Sinar Grafika, Jakarta, 2009, p. 5

³⁶ Interview with Kompol Yusuf Taziri, S.I.K (Kasubbid Digital Computer Forensics Polda NTB), on July 8, 2020 at 09.44 Wita in the Criminal Investigation Section of the NTB Police

³⁷ Lilik Mulyadi, *Bunga Rampai Hukum Pidana Prespektif, Teoritis dan Praktik*, PT Alumni, Bandung, 2008, p. 390

- 1) Call on member countries to intensify efforts to combat computer abuse more effectively by considering the following steps;
 - a) Modernizing material criminal law and criminal procedural law
 - b) Develop computer precautions and safeguards
 - c) Take steps to sensitize citizens, law enforcement officials, and courts to the importance of preventing computer-related crimes
 - d) Conduct training efforts for judges, law enforcers, officials regarding crimes in the economic sector and cyber crimes
 - e) Extend the rules of ethics in computer use and teach them through the informatics curriculum
 - f) Adopt a victim protection policy in accordance with the UN declaration on victims, and take steps to encourage victims to report cyber crimes.
- 2) Call on member countries to increase international activities in efforts to combat cyber crime.
- 3) Recommend to the UN Crime Control and Prevention Committee;
 - a) Disseminate guidelines and standards to assist member countries in dealing with cyber crimes at the national, regional and international levels,
 - b) Developing further research and analysis in order to find new ways to deal with cyber crime problems in the future,
 - c) Consider cyber crimes when reviewing the implementation of extradition agreements and cooperation assistance in the field of crime prevention.³⁸

b. Non penal policy

Non-penal policies can be pursued by improving the national economy, conducting moral education to everyone both formally and non-formally, especially for parties who are prone to committing crimes, improving the public mental health system, making international cooperation effective in eradicating cyber crime, improving the security system computers, and streamline administrative law and civil law relating to the administration of computer systems and networks.

c. Policy in the Criminal Code

The regulation regarding the Crime of E-commerce transactions in the Concept of the Criminal Code of 2008 is in Chapter VIII of the Second Book of the fifth part of the first paragraph is regulated in Article 373, Article 375, the second paragraph is regulated in Article 376 to Article 378.

- 1) Article 373 with the elements of a crime: accessing computers and / or electronic systems in any way without rights, with the intention of obtaining, changing, destroying, or removing information in computers and / or electronic systems; (related to e-commerce transaction crime in the form of Unauthorized access computer system and service, Hacking, and Cyber Sabbath and extortion).
- 2) Article 375 with the elements of a criminal act: everyone who owns and uses a domain name based on bad faith violates unfair business competition and violates the rights of others (related to confiscation of the domain name).
- 3) Article 376 with the elements of a crime: accessing computers, and / or electronic systems without rights, which causes interference or harm to the country and / or relations with international legal subjects; (Related to the crime of Unauthorized access computer system and service).

³⁸ Barda Nawawi Arief, *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia*, PT RajaGrafindo Persada, Jakarta, 2006, p. 3

- 4) Article 377 with the elements of a criminal act: accessing computers and / or electronic systems without the right to obtain, change, destroy, or eliminate government-owned information which because of its status must be kept confidential or protected; (related to e-commerce transaction crime in the form of Unauthorized access computer system and service, Hacking, and Cyber Sabbath and extortion).
- 5) Article 378 with the elements of a criminal act: accessing computers and / or electronic systems without rights with the intention of obtaining profits or obtaining financial information from the Central Bank, banking or financial institutions, credit card issuers or payment cards or containing customer report data; (related to e-commerce transaction crime in the form of Unauthorized access computer system and service, and Carding).

Basically, the concept of the Criminal Code can be used to ensnare criminal acts of e-commerce transactions and there has been progress towards criminal law policies compared to the current KUHP, but the policies are still lacking, namely criminal law policies related to criminal acts of e-commerce transactions made must also be oriented. One international reference that is widely used is the Uncitral Model Law on Electronic Commerce 1996. The reference which contains the legal model in e-commerce transactions is published by UNCITRAL as one of the international commissions under the United Nations. The model was approved by General Assembly Resolution No. 51/162 dated December 16, 1996.³⁹

2. NTB Regional Police Legal Protection in E-Commerce Crime

Based on the results of the interviews that the author has conducted, the answers to the problems regarding the role of the police in investigating e-commerce crimes are as follows:

2.1 Legal Protection With Layered Articles

The use of multi-layered articles is intended to create a deterrent effect, because in addition to the material loss of the victim, the immaterial loss in the form of the company's good name is tarnished so that customer trust is reduced. For their actions, the suspects were charged with Article 28 paragraph (1) of Law number 19 of 2016 concerning Electronic Information and Transactions in conjunction with article 378 of the criminal code on fraud, and charged with the Money Laundering Criminal Act (TPPU).

The investigation conducted by the NTB Regional Police on e-commerce crimes was carried out by the NTB Regional Police for Certain Crimes Unit. The investigation stage is the first stage carried out by an investigator in carrying out an investigation of a criminal act as well as the most difficult stage in the investigation process, this is because at this stage the investigator must be able to prove the crime that occurred and how and the causes of the crime in the effort to overcome.

The main task of the Police is to maintain security in the country. In the Law on the Police of the Republic of Indonesia Number 2 of 2002 in Article 13 it is explained that the main duties of the Police are:

- a. Maintain security and public order
- b. Enforce the law
- c. Providing protection, protection and services to the community.⁴⁰

The authority in the general understanding is contained in Article 15 and Article 16 of the Law of the Republic of Indonesia regarding the Police, which is an opportunity for freedom to act and / or not to act responsibly. In order for the implementation of Police duties as described above to run well, the public

³⁹ Teguh Wahyono, *Etika Komputer Tanggung Jawab Profesional dibidang Teknologi Informasi*, Andi, Yogyakarta, 2005, p. 174

⁴⁰ Viswandro, Maria Matilda. Bayu Saputra. *Mengenal Profesi Penegak Hukum*, Pustaka Yustisia, Yogyakarta, 2015, p. 20-21.

can obey, respect, and respect the implementation of their duties in the context of law enforcement, by law the Police are given considerable general authority, including:

- a. Receiving reports and / or complaints
- b. Helping to resolve disputes among members of the public that could disrupt public order
- c. Preventing and overcoming the growth of community diseases
- d. Oversee the flow that can cause division or threaten the unity of the nation
- e. Issue a Police regulation within the scope of the Police administrative authority
- f. Carry out special examinations as part of the police action in the context of prevention
- g. Take the first action at the scene
- h. Take fingerprints and other identities and take a picture of someone
- i. Looking for information and evidence
- j. Organizing a National Criminal Information Center
- k. Issuing permits and / or certificates required for public service purposes
- l. Providing security assistance in trials and implementation of court decisions, activities of other agencies, and community activities
- m. Receive and store the findings temporarily.⁴¹

As a form of consumer protection against criminal acts of e-commerce, the NTB Regional Police also urged the public to be proactive in reporting to the authorities, in this case the police. Reporting to the police if there has been a cyber fraud crime, the public can report it to law enforcement (police) accompanied by initial evidence in the form of electronic data or information and/or printed results. If the case is followed up by law enforcers in an investigation / investigation process, the law enforcer will trace the source of the electronic document.

In practice, usually law enforcers will first track the whereabouts of the perpetrator by tracing the perpetrator's Internet Protocol (IP Address) address based on the IP address log stored on the website / homepage management server which is used as a vehicle for the perpetrator to commit fraud. The problem is, law enforcers will encounter difficulties if the website / homepage is owned outside the jurisdiction of Indonesia (such as Facebook, Google, Twitter, Yahoo, and others).

Although currently law enforcers (police and Civil Servant Investigators/PPNS of the Ministry of Communication and Information Technology) have collaborated with several website / homepage managers outside the territory of Indonesia, in practice it is not easy to get the IP address of an perpetrator who is suspected of committing a criminal offense by using certain website/homepage services. This is due to differences in legal procedures between countries.

Although governments between countries through their law enforcement officers have made Mutual Legal Assistance (MLA) agreements or mutual legal assistance agreements, in reality MLA does not automatically apply in every case involving between countries. This jurisdiction problem is often the cause of the inability to process or the delay in investigations / investigations into cybercrime cases.

2.2 Legal Protection of Parties by Polda NTB in E-Commerce

The emergence of the phenomenon of Electronic Commerce or abbreviated as E-Commerce is a business activity that involves consumers (consumers), manufactures (manufactures), service providers, and intermediaries by using computer networks, namely the Internet. E-Commerce already covers the entire spectrum of commercial activities. With the ease of communicating electronically, trade has now begun to spread to the electronic world. Transactions can be carried out with the convenience of information technology, without any distance barriers. Julian Ding pointed out that:

⁴¹ Article 15 Paragraph (1) of Law Number 2 of 2002 concerning the Indonesian National Police

"E-Commerce as a concept is not defined. E-Commerce means different things to different people. It is like we define an elephant, that is, depending on which part of the elephant we see or hold, it will be different definitions that can be given".⁴²

The e-commerce case that occurred in the NTB Regional Police:

Post Date : July 17, 2019
 Full Name : Ahmad Fahmi
 Contact : Fahri Rohman@yahoo.com
 Subject : online shopping scams
 Contact : Monday 27 June 201 1, after ordering goods at WWW.Cheesestore. com (address: Jln. Sisingamangaraja No. 254 Cirebon West Java Indonesia 45 153), that same day I immediately transferred to the BRI account 022. 121. 6033 an Wardi, confirmation after the money was received directly the goods were sent, the next day I texted to no 08219-0000-399 & 021-384-9977 but for 24 hours they have no answer, every day I follow up but there is no answer, on 20 July there is a confirmation claiming to be from JNE (087740147666), and ask for money worth IDR . 150.000, - to redeem my ordered items on the grounds that there is a problem at customs, I am not sure about that I force the person to provide a shipping receipt number but for various reasons they do not want to give it because from the start I have not received a shipping receipt number so it is strange if the goods have indeed been sent but have not received a delivery receipt number. Then I concluded that my order has not been sent and will never be sent.

The steps taken by the police are:

- a. conduct an examination such as in an internet cafe that is usually used by criminals
- b. collect evidence relating to crime
- c. Track related crimes
- d. to confiscate electronic evidence such as hard disks,
- e. make disclosure or detention based on preliminary evidence or sufficient evidence.⁴³

In addition, there are several things that the NTB Police have done in providing legal protection in terms of agreements, electronic evidence, and the responsibilities of the parties.

a. Agreement

1) Legal protection inside

E-Commerce Agreement In the agreement there is an electronic document, usually the document is made by the merchant which contains the rules and conditions that must be obeyed by the customer but the contents do not burden the customer. These rules and conditions are also used as legal protection for both parties.

Legal protection for both parties is:

- a) Legal protection for merchants is mainly emphasized in terms of payment, merchants require the customer to make payment and then confirm payment, only after that will the goods ordered be delivered.

⁴² Julian Ding, *E-Commerce: Law & Practice*.: Sweet & Maxwell Asia, Malaysia, 1999, p. 25.

⁴³ Interview with Kompol Yusuf Taziri, S.I.K on July 7, 2020, at 09.16 Wita, at the Cyber Crime Investigation Satellite Office (CCISO) Laboratory of the NTB Police

- b) Legal protection for customers lies in the guarantee of returning or exchanging goods if the goods received do not match what was ordered.
- c) Privacy
Personal data of electronic media users must be legally protected. The information provided must be accompanied by the consent of the owner of the personal data. This is a form of legal protection for parties carrying out E-Commerce transactions, which is contained in Article 25 of the ITE Law "Electronic information and / or electronic documents that are compiled into intellectual works, internet sites, and intellectual works contained therein are protected as rights. intellectual property based on statutory provisions".

2) Legal protection outside the agreement

Legal protection for merchants also concerns Intellectual Property Rights over the domain names they own as contained in Article 23 of the ITE Law. Electronic information that is compiled into an intellectual work in any form must be protected by law relating to Intellectual Property Rights. This is because electronic information has an economic value for the creator or designer. Therefore, their rights must be protected by the IPR law.

In the explanation of Law Number 8 of 1999 concerning Consumer Protection, it is stated that legal instruments protecting consumers are not intended to kill business actors, but on the contrary, because consumer protection will be able to promote a healthy business climate and the birth of companies that are tough in facing competition through the provision quality goods and / services.

In order to direct activities and developments in Cyberspace, especially to encourage and direct the development of E-Commerce, special and firm arrangements regarding the validity and legal power of electronic documents as valid evidence are non-negotiable.

2.3 Legal Protection Using Criminal Policy

Upaya menanggulangi kejahatan terhadap berbagai sarana sebagai reaksi yang dapat diberikan kepada pelaku kejahatan *e-commerce*, berupa sarana pidana maupun non hukum pidana, yang dapat diintegrasikan satu dengan yang lainnya. Dilaksanakan politik hukum pidana, yakni mengadakan pemilihan untuk mencapai hasil perundang-undangan pidana yang sesuai dengan keadaan dan situasi pada suatu waktu dan masa yang akan datang.⁴⁴

Policies to carry out crime prevention and control, including policies in the field of criminal policies, this criminal policy cannot be separated from a broader policy, namely social policy which consists of policies or efforts for social welfare (social-self-policy) and policies. or efforts for community protection (social-defense policy).⁴⁵ Policies for dealing with crime have three ways in terms of using the means, namely through the means of the criminal justice system (penal), repressive actions, namely efforts after the occurrence of a crime, and means (non-penal) for pre-emptive actions, namely actions to prevent the occurrence of criminal acts by instilling values or norms against a person and preventive action, namely preventing before the occurrence of a crime. The difference between the three can be described as follows:

a. Pre-Emptive Action

Pre-emptive is the initial action taken by the Police to prevent a crime from occurring. The efforts made in prevention of crime pre-emptively instill good values or norms so that these norms are internalized in a person. Even if there is an opportunity but do not have the intention to do so, there will be no crime.

⁴⁴ Sudarto. *Kapita Selekta. Hukum Pidana*. Alumni.Bandung.1986. p. 77

⁴⁵ Barda Nawawi Arief, *Masalah Penegakan Hukum Dan Kebijakan Penanggulangan Kejahatan*, Citra Aditya Bakti, Bandung, 2001, p. 73

b. Preventive Measures

Preventive action is an action taken to prevent or guard against the possibility of a crime. According to A. Qirom Samsudin M, in relation to taking preventive action:

"Preventing crime is better than educating criminals to be good again, because it is not only calculated in terms of cost, but this effort is easier and will get satisfying results or achieve goals".

c. Repressive Actions

Repressive actions are all actions taken by law enforcement officials after a criminal act has occurred. Respective action is more focused on the person who has committed a criminal act, namely, among others, by providing a law (criminal) which is appropriate for the act.⁴⁶

There are several ways that can be used in tackling crime:

- a. Crime prevention in a broad sense, including reform and prevention in the narrow sense.
- b. Crime prevention in the narrow sense includes moralism, namely disseminating the means that can reinforce one's morals in order to avoid lust to do evil.
- c. Trying to supervise and control crime by trying to create:
 - 1) Good Police organizational system and equipment;
 - 2) An objective justice system; and
 - 3) Good law (legislation).
- d. Prevent crime with regular supervision and patrol.⁴⁷

2.4 Barriers to Legal Protection of E-Commerce Crime at the NTB Police Agency

The National Police of the Republic of Indonesia in the West Nusa Tenggara (NTB) region found that there are many e-commerce criminal cases that continue to grow every year, the increasing number of e-commerce criminal cases cannot be separated from the increasing number of people in NTB who use the internet as a means of seeking their daily needs. The NTB Regional Police's obstacles in protecting e-commerce criminal acts are as follows:

a. The difficulty of finding evidence

Evidence that is recognized in court proceedings must go through a long process and requires other agencies to provide information to be used as appropriate evidence in court. To apply the existing articles in the ITE Law, especially article 5 paragraph 1. When compared with the provisions in KUHAP, namely article 184, Article 5 paragraph 1 is more difficult and takes time to process the evidence desired by the ITE Law. Meanwhile, when viewed from the Criminal Procedure Code, evidence tends to be easier to process as evidence and in terms of time is also shorter.

According to AKP Prayit Hariyanto, SH:

"Evidence as regulated in the ITE Law and the provisions required in the Attorney General's circular letter in reality only applies to cases that are large in nature and are in the public spotlight. For cases that do not really grab people's attention, he said that investigators rarely use evidence with the provisions of the ITE Law and a circular from the Attorney General's Office".

⁴⁶ Soejono, D, *Penanggulangan Kejahatan (Crime Prevention)*, Alumni Bandung, 1976, p. 42

⁴⁷ Bonger, *Pengantar Tentang Kriminolog*, Pembangunan Ghalia Indonesia, Jakarta, 1981, p.15.

E-commerce evidence that can be used for criminal acts of fraud through e-commerce is evidence both in article 184 of the Criminal Procedure Code and as well as evidence in article 5 of the ITE Law. But in fact the investigators tend to only use the evidence in Article 184 of the Criminal Procedure Code. In fact, the evidence in Article 5 of the ITE Law is evidence that is specifically for criminal acts that use ITE facilities.

b. Difficulty finding anonymous accounts (fake accounts that are difficult to detect)

For example, the perpetrator uses a fake account such as an email that is used as a website to sell fake or fictitious items that can attract the attention of people who want to shop on online media.

c. Electronic identity

Personal data or electronic media belonging to the perpetrator such as discarded electronics, inactive cellphone numbers. After the perpetrator finds the victim, using a cellphone and card that is not permanent or temporarily used. so that it can make it difficult for the police to trace the whereabouts of the perpetrator.

Conclusion

1. Enforcement of criminal law against e-commerce uses the Criminal Code and the ITE Law, because in article 378 of the Criminal Code for the threat of punishment is too light, the police apparatus uses article 28 paragraph (1) and article 45A paragraph (1) of Law number 19 of 2016 regarding Electronic Information and Transactions. In the case of e-commerce crime, police officers who act as investigators have difficulties because e-commerce crime has differences when compared to other criminal cases. The difficulties encountered by the NTB Regional Police were the difficulty in finding evidence, finding anonymous accounts (fake accounts that were difficult to detect) and electronic identities. In addition, the NTB Police agency does not have the authority to intercept and block accounts used by e-commerce criminals.
2. Legal protection measures taken by the NTB Regional Police against consumers, namely conducting checks at internet cafes that are usually used by criminals, collecting evidence related to crimes, tracking related crimes, confiscating electronic evidence such as hard disks, make disclosure (block bank accounts) or detain based on preliminary evidence or sufficient evidence. In addition, the use of multi-layered articles is intended to create a deterrent effect, the suspects are charged under Article 28 paragraph (1) of Law number 19 of 2016 concerning Electronic Information and Transactions in conjunction with article 378 of the criminal code book on fraud, and charged with law. Money laundering (TPPU).

Recommendation

1. In the process of law enforcement on e-commerce criminal acts, law enforcers must carry out special education and training to improve the quality and ability of law enforcement officials in uncovering e-commerce cases so that they can comprehensively understand the applicable regulations. to the perpetrator of fraud based on electronic transactions and there is no multiple interpretation in the application of the articles. In addition, the government should be able to accommodate law enforcement officers to be able to provide facilities and infrastructure in accordance with the specifications expected to be able to reveal and arrest the perpetrators of criminal acts.

2. It is necessary to collaborate with the bank concerned to find data on the perpetrators of e-commerce crime for the sake of the investigation process.

References

Books

- Abdul Halim Barkatullah & Syahrida, *Sengketa Transaksi E-Commerce Internasional Pengertian Sebab Kemunculan dan Metode Penyelesaian Yang Efektif*, Nusa Media, Bandung, 2010.
- Ahmad Miru & Sutarman Yodo, *Hukum Perlindungan Konsumen*, PT. Raja Grafindo Persada, Jakarta, 2007.
- Alvin Toffler. *The Third Wave*. Bantam Books, Toronto, 1982.
- Amran Suadi, *Filsafat Hukum Refleksi Filsafat Pancasila, Hak Asasi Manusia, dan Etika*, Edisi Pertama, PRENADAMEDIA GROUP, Jakarta.
- Edmon Makarim, *Kompilasi Hukum Telematika*, PT Raja Grafindo, Jakarta, 2003.
- Amiruddin & Zainal Asikin, *Pengantar Metode Penelitian Hukum*, Cet. 6, Raja Grafindo Persada, Jakarta, 2012,
- FN Jovan. *Pembobol Kartu Kredit Menyingkap Teknik dan Cara Kerja Carder Di Internet*. Mediaseorang, Yogyakarta, 2006.
- Jimly Asshidiqie dan M. Ali Syafa'at, *Teori Hans Kelsen Tentang Hukum*, Cetakan ke-2, Konstitusi Press, Jakarta, 2012.
- Lili Rasjidi & L.B. Wyasa Putra, *Hukum Sebagai Suatu Sistem*, Remaja Rusdakarya, Bandung, 1993.
- Marwan Mas, *Pengantar Ilmu Hukum*, Ghalia Indonesia, Bogor, 2004.
- Mukti Fajar ND & Yulianto Achmad, *Dualisme Penelitian Hukum Normatif & Empiris*, Pustaka Pelajar, Yogyakarta, 2015.
- Ninie Suparni, *Cyberspace Problematika dan Antisipasi pengaturannya*, Sinar Grafika, Jakarta, 2009.
- Onno W. Purbo & Aang Arif Wahyudi, *Mengenal E-Commerce*, Elex Media Komputindo, Jakarta, 2001.
- Peter Mahmud Maerzuki, *Penelitian Hukum*, Prenada Media Group, Jakarta, 2005.
- Phillipus M. Hadjon, *Perlindungan Hukum Bagi Rakyat Indonesia*, PT. Bina Ilmu, Surabaya, 1987.
- Raji Soemarno Partodiharjo, *Tanya Jawab Sekitar UU. No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik*, PT Gramedia pustaka Utama, jakarta, 2009.
- Riyeke Ustadiyanto, *Framework e- Commerce*, cetakan 1, andy, Yogyakarta, 2001.
- Salim, H.S & Erlis Septiana Nurbani, *Penerapan Teori Hukum pada Penelitian Tesis dan Disertasi*, Edisi Pertama, Cetakan ke-1, Rajawali Press, Jakarta, 2013.
- Satjipto Raharjo, *Ilmu Hukum*, Bandung: PT. Citra Aditya Bakti, 2000.
- Soemarno Partodiharjo, *Tanya Jawab Sekitar UU. No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*, PT. Gramedia Pustaka Utama, Jakarta, 2009.
- Soerjono Soekanto, *Efektifitas Hukum dan Penerapan Sanksi*, Bandung: Remaja Karya, 1985,
 , *Pengantar Penelitian Hukum*, UI Press, Jakarta, 1984.
 , *Pengantar Hukum*, UI Press, Jakarta, 2006.
 , *Sosiologi: Suatu Pengantar*, Bandung: Rajawali Press, 1985.
- Sudikno Mertokusumo, *Mengenal Hukum Suatu Pengantar*, Liberti, yogyakarta, 2003.
- Sunaryati Hartono, *Politik Hukum Menuju Satu Sistem Hukum Nasional*, Alumni, Bandung, 1991.
- Theo Huijber, *Filsafat Hukum dalam Lintas Sejarah*, cet. VIII, Yogyakarta: Kanisius, 1995.
- Yayasan Lembaga Konsumen Indonesia, *Liku-liku Perjalanan Undang-undang Perlindungan Konsumen*, Cet.1, YLKI dan USAID, Jakarta, 2001.

Journal

AZ Nasution, *Perlindungan Konsumen; Tinjauan Singkat UU No.8 Tahun 1999 – L.N. 1999 NO.42*”, *Hukum dan Pembangunan, No. 2* (April-June 2002).

Ferry Irawan Febriansyah, *Keadilan Pancasila Sebagai Dasar Filosofi Dan Ideologis Bangsa*, DiH Jurnal Hukum, Volume 13 Number 25, Muhammadiyah Islamic College, Tulungagung.

Mazmanian & Sobotier dalam Joko Widodo, *Analisis Kebijakan Publik, Konsep dan Aplikasi Analisis Kebijakan Publik*, Malang: Bayu Media Publishing, 2007.

Pan Mohamad Faiz, *Teori Keadilan John Rawls*, dalam jurnal Konstitusi, Vol. 6 No. 1 April 2009.

Surajiyo, *Keadilan Dalam Sistem Hukum Pancasila*, Universitas Indraprasta PGRI, IKRAITH-Humaira Vol. 2 No. 3 Bulan November 2018

Regulations

The 1945 Constitution of the Republic of Indonesia.

Law No. 39 of 1999 concerning Human Rights, State Gazette of the Republic of Indonesia of 1999 no 165.

Law No. 19 of 2016 Amendments to Law No. 11 of 2008 concerning Information and Electronic Transactions (ITE).

Law Number 7 of 2014 concerning Trade.

Law Number 8 of 1999 concerning Consumer Protection.

RI Government Regulation Number 82 of 2012 concerning Implementation of Electronic Systems and Transactions.

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/4.0/>).