




# Cyber Crime E-Commerce Business Transactions

Fauziah Lubis

Faculty of Law University Islam Negeri Sumatera Utara, Medan, Indonesia.

 : [fauziahlubis@gmail.com](mailto:fauziahlubis@gmail.com)

Corresponding Author\*



Submitted: 2022-08-16

Revised: 2022-11-07

Published: 2022-12-30

## Article Info

### Keywords:

Cybercrime; Legal Protection;  
E-Commerce.

## Abstract

**Introduction:** Law enforcement and protection for cyber cases is focused on consumers as victims of digital crimes where consumers are generally harmed when conducting business transactions digitally. Where the focus of this paper discusses the legal protection of victims of cybercrime victims when transacting business.

**Purposes of the Research:** The purpose of this study is to explain the concept of cybercrime in financial transactions.

**Methods of the Research:** The research method used is normative legal research with a statute legal approach and a conceptual approach.

**Results of the Research:** Cyber crime is currently very growing in Indonesia, especially in the current era of digitalization. Where the law can protect from new crimes that live in the current kekininia period so that victims of cyber crime legally in Indonesia can be implemented in accordance with its purpose, which is to protect all Indonesian people from crime cases.

## 1. INTRODUCTION

The activity of using the internet with business transactions is known as Electronic Commerce (E-Commerce). E-Commerce can occur between business organizations and consumers, including the use of the Internet and the World Wide Web to sell products and services to consumers. E-Commerce technology is a business mechanism that works electronically by focusing on online business transactions and has the opportunity to build more human and personalized relationships with customers without depending on space and time.<sup>1</sup>

In order to examine legal/juridical norms or standards, this research uses a statutory approach, which is used to determine the laws pertaining to cybercrime. It is also supported by library research, with the aim of enhancing theoretical studies by creating an inventory of legal materials in the form of journals, articles, bulletins, books/libraries, along with research findings that, of course, are of course.

The scope of e-commerce according to the World Trade Organization (WTO) includes the fields of production, distribution, marketing, sales, and delivery of goods or services through electronics, while the OECD (Organization for Economic Cooperation and Development) explains that e-commerce is a transaction based on the process and

<sup>1</sup> E. A. Pratama, "Optimalisasi Cyberlaw Untuk Penanganan Cybercrime Pada Ecommerce," (Purwokerto, 2013), .25.

transmission electronic data.<sup>2</sup> Apart from these two international institutions. Alliance for Global Business, a leading trade association defines e-commerce as all value transactions involving the transfer of information, products, services or payments via electronic networks as a medium.<sup>3</sup> Meanwhile, e-commerce from ECEG Australia (Electronic Commerce Expert Group) is "Electronic commerce is a broad concept that covers any commercial transaction that is effected via electronic means and would include such mean as facsimile, telex, EDI, Internet and the telephone".<sup>4</sup>

Electronic commerce (E-Commerce) is the result of information and technology advancements that transform traditional business practices from face-to-face interactions between sellers, business actors, and buyers, to virtual interactions between business actors and consumers in cyberspace. These developments can be observed in the explosive rise of online stores that use the internet as a medium for trading goods or services with businesses or individual customers, as well as in the use of digital technology in bartering methods for goods, services, information, and knowledge.

The Internet is a worldwide computer network. Economically, it is acknowledged that the use of the internet is extremely urgent/essential to speed up business transactions, but the use of the internet also needs to be extra cautious. This is transnationally synonymous with the word "internet business." E-commerce is the practice of conducting business through the use of a computer network, such as the internet, that involves consumers, manufacturers, service providers, and intermediaries.<sup>5</sup>

In fact, there are a lot of issues that affect consumers when they transact in e-commerce because it frequently occurs that the goods/products ordered are different from the goods that actually arrive in terms of size, color, type, and quality of the goods, from the circumstances experienced by consumers based on consumer law.<sup>6</sup> Law No. 8 of 1999 concerning consumer protection states that anybody can file a civil lawsuit in the District Court, and Law No. 11 of 2008, as amended by Law No. 19 of 2016 about ITE, states that anyone can also file a criminal complaint there: According to the provisions of Article 45 of the Law, anyone who intentionally and without authorization spreads false and misleading information that causes consumer losses in electronic transactions is subject to a maximum penalty of six years imprisonment and/or a maximum fine of Rp 1,000,000,000 (one billion rupiah).<sup>7</sup>

Cyber crime is a type of crime that involves the use of the internet, computer networks, or other digital technologies. Computer misuse, computer abuse, computer fraud, computer-related crime, compute-assisted crime, and computer crime are additional phrases that are interchangeable with cybercrime. Along with the growth of e-commerce, cybercrime crimes also emerged. Technology is utilized by business players to advertise goods and services more effectively, efficiently, and productively, yet it frequently

---

<sup>2</sup> <https://www.ui.ac.id/dampak-kejahatan-siber-pada-bisnis-ekonomi-digital/diakses> Tanggal 1 November 2022

<sup>3</sup> Edy Army, "Bukti Elektronik Dalam Perkara Peradilan," (Jakarta: Sinar Grafika, 2020), 179.

<sup>4</sup> Edy Army, op.cit., 3.

<sup>5</sup> Purwaningsih, E. " *Hukum Bisnis*," (Bogor Ghalia Indonesia, 2010), 57.

<sup>6</sup> Musa Darmin Pane, Sahat Maruli Tua Situmeang, Penegakan Hukum Cyber Crime Dalam Upaya Penanggulangan Tindak Pidana Teknologi Informasi, *Jurnal Loyalitas Sosial*, Vol. 3 No. 2, 2021, 95

<sup>7</sup> Dewi Bunga, Politik Hukum Pidana Terhadap Penanggulangan Cyber Crime, *Jurnal Legislasi Indonesia*, Vol.16 No.1. 2019, 3-6

degenerates into criminal activity in an effort to maximize profit even though it is prohibited.<sup>8</sup>

In the current era of trade and the industrial revolution 4.0, which is accompanied by rapid advances in technology and industry, it has affected various business sectors, including trade and banking activities. Electronic transactions are increasingly being carried out, including in the fields of trade and banking.<sup>9</sup> Legal actions are no longer based on concrete, cash and communal actions, but are carried out in cyberspace in an informal and individual way. This is also influenced by international life associations in the era of globalization, namely that the interaction between national legal provisions and international legal rules will increase because of the development of international traffic life association.<sup>10</sup> The author's motivation for undertaking this research is to better understand the legal remedies/*juridische inspanning* available to customers who feel they have been wronged or deceived by sellers or business actors in e-commerce transactions.

## 2. METHOD

This study uses the type of normative legal research (doctrinal research). Doctrinal legal studies analyzes authoritative texts (with binding legal force) and readers whose power is persuasive (reinforcement). Texts that have binding legal force are the main legal material that includes laws and regulations relevant to the research problem. in this regard, considering that this normative legal research analyzes the rule of law, the object under study is in the form of regulatory documents and library materials. in this case the object of this study is in the form of rules or literature related to absenteeism and corruption trials in the implementation of this study, the author uses several research approaches in a field of science so that research focuses on solving the problem following a predetermined scope.<sup>11</sup> The approach in this study consists of legal statute approach and conceptual approach. The legal approach according to the law is carried out by examining laws and regulations. The legal approach of this Act is used to examine the relevant statutes or statutes for criminal acts of cyber crime. Regarding the conceptual approach, it is carried out based on the principles of law obtained in the view of legal scholars or other legal doctrines by not deviating from the existing regulations this approach is necessary because there are no rules governing it. the application of the conceptual approach is to look for definitions of cyber crime that are available in law books, and other legal journals.

## 3. RESULTS AND DISCUSSION

Due to the fact that the use of e-commerce applications is not balanced by the application of high and accurate security technology and because e-commerce applications are highly susceptible to criminal/criminal activities, it is necessary to have an innovation at the security level to protect against and prevent crime. the prevalence of crime, fraud by employees, and cybercrime.<sup>12</sup>

---

<sup>8</sup> Kristina Virgi Kusuma Putri, Kerja Sama Indonesia Dengan Asean Mengenai Cyber Crime Security dan Cyber Resilience Dalam Mengatasi Cyber Crime, Jurnal Hukum Lex Generalis, Vo. 2 No. 7, 2021, 546

<sup>9</sup> Supanto, Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) dan Antisipasinya Dengan Penal Policy, Yustitia, Vol. 5 No.1 ,2016, 53

<sup>10</sup> Yudha Bhakti Ardhiwisastra, "Penafsiran dan Kosntruksi Hukum," (Bandung, alumni, 2000), 55.

<sup>11</sup> Soekanto, S, Pengantar Penelitian Hukum. (Jakarta, UI Press, 2018), 32

<sup>12</sup> CNBC Indonesia. 2022. Ada 5.000 Kasus Perbulan, Indonesia Emergency Kejahatan Siber. <https://www.cnbcindonesia.com/tech/20211011205453-37-283113/ada-5000-kasus-perbulan-indonesia-emergency-kejahatan-siber>. Diakses pada 01 November 2022.

Due to the spread of viruses that cause e-commerce applications to malfunction and result in material and immaterial losses for consumers, this cyber/cyber world workforce is largely to blame for the extreme inconvenience that consumers experience when conducting online business transactions. This will erode public confidence in e-commerce applications.<sup>13</sup>

Despite the fact that it is widely acknowledged that using e-commerce can boost productivity, efficiency, and cost savings, which can in turn promote competition in the business sector, when considering the elements that affect the growth and development of e-commerce, among others:<sup>14</sup>

- a) E-commerce has the ability to continuously/simultaneously reach more customers/consumers
- b) E-commerce has the ability to appropriately and accurately promote the innovation of sellers/business actors
- c) E-commerce can create/generate high efficiency, cheap / low cost, and informative
- d) International, intergalactic, and 24-hour e-commerce.

In e-commerce transactions, the following parties are involved:

- a) Seller is a business actor that runs personally or corporately
- b) Consumers/buyers are persons who use business actors' services, either personally or corporately.
- c) Acquirer is the billing intermediary.
- d) Issuer is the credit card companies/corporations made up of banks and non-bank financial institutions.<sup>15</sup>

Despite the fact that it The payment systems used in e-commerce are as follows:<sup>16</sup>

- a) Electronic cash such as token, net cash, visa cash, e-cash, millicent, cybercoin, and wordpay.
- b) Banking debit such as Bank *internet payment system* (BPIPS), FSTC *electronic check*.
- c) Credit system such as Paylater
- d) TI *Digital cash*
- e) *cyber cash*
- f) *first virtual*
- g) *Netchat*
- h) *E-gold*

In addition, there are a number of features of cybercrime, where such actions are carried out in the data space in cyberspace without permission or in an unlawful and unethical manner:

- a) Internet application network-connected equipment is used in *aquo* action.
- b) Behavior that results in material or immaterial losses

---

<sup>13</sup> Sugianto, Eddy Cahyono. 2019. *Ekonomi Digital: The New Face of Indonesia's Economy*. [https://www.setneg.go.id/baca/index/ekonomi\\_digital\\_the\\_new\\_face\\_of\\_indonesias\\_econo](https://www.setneg.go.id/baca/index/ekonomi_digital_the_new_face_of_indonesias_econo) my. Diakses pada 01 November 2022

<sup>14</sup> Getha Fety Dianari, Pengaruh Ecommerce Terhadap Pertumbuhan Ekonomi Indonesia, *Jurnal Bina Ekonomi* , Vol. 22 No. 1 Tahun 2018, 46-47

<sup>15</sup> Nida Rafa Arofah dkk, Internet Banking dan Cyber Crime : Sebuah Studi Kasus di Perbankan Nasional, *Jurnal Pendidikan Akutansi*, Vo. 18 No. 2, 2020, 112

<sup>16</sup> <https://www.daya.id/usaha/artikel-daya/keuangan/macam-macam-sistem-pembayaran-pada-bisnis-e-commerce> Diakses pada 01 November 2022

c) Both national and international actions are taken.<sup>17</sup>

Based on their actions, we should comprehend the several categories of cyber crime:<sup>18</sup>

- a) System Unauthorized access to computers and services, which is when a criminal (a hacker) illegally gains access to or infiltrates a computer network system without the owner's consent or with the aim to steal confidentially sensitive facts or information.
- b) Illegal contents, such as the kind of crime committed by entering information or data into an internet application that is false or a falsehood, unethical, and illegally formal, or that disturbs public order by slandering someone else and undermining their dignity.
- c) Data forgery, which is the crime of falsifying significant papers or data recorded in scriptless documents via the internet network, is meant for e-commerce documents and is committed with the intent to profit from the crime.
- d) Cyber espionage, a felony that involves illegal entry into a computer network system to conduct spying operations, is typically targeted at competitors in the e-commerce industry.
- e) By disrupting, deleting, or destroying data on computer programs connected to the internet network, cyber sabotage and extortion, crimes like these, are committed.
- f) Intellectual property offense, also known as HAKI, is the type of crime that involves violating another person's rights by illegally copying their website's webpage, which contains private information about their trading activities.
- g) Privacy violations: these crimes target a person's personal information or data that is kept in a personal data form and that, if discovered by others, could cause the victim both material and immaterial harm, such as credit card numbers and ATM PINs.
- h) Carding is a crime that involves using computer technology to carry out credit card transactions for other people or parties, harming them both materially and intangibly.

In the meanwhile, the following procedures are typically followed in cybercrime crimes:

- a) Gather and evaluate the data and information present in the target's computer network and operating system.
- b) Access the target's computer network or infiltrate against their rights.
- c) Looking for greater and more technologically advanced access on computer systems than the target's or victim's access
- d) Add a backdoor or get rid of all traces.<sup>19</sup>

It is illegal to commit fraud in online transactions. The law enforcement process is hampered by cybercrime for a number of reasons, including:<sup>20</sup>

- a) Due to space limitations and the ambiguity of the perpetrators' identities, it takes time for investigators to be able to apprehend offenders.
- b) Gathering evidence in light of the fact that online transactions are governed by the Criminal Code (*lex generalis*) and extra evidence allowed under the ITE Law (*lex specialist*)

---

<sup>17</sup> Wahid, Abdul dan M. Labib, “*Kejahatan Mayantara, Cyber Crime*,” (Bandung : Refika Aditama, 2010), 76.

<sup>18</sup> <https://www.hukumonline.com/klinik/a/waspada-kenali-macam-macam-kejahatan-di-internet-cl294> diakses Tanggal 01 November 2022

<sup>19</sup> Raharjo, A. “*Cybercrime, Pemahanan Dan Upaya Pencegahan Kejahatan Berteknologi*,” (Bandung: Citra Aditya Bakti, 2002), 199

<sup>20</sup> Aulia Putri Fadhila, Tinjauan Kriminologi Dalam Tindakan Penipuan E Commerce Berdasarekan Peraturan Perundangan Pada Masa Covid 19, Jurnal Suara Hukum Volume 3 No. 2 Tahun 2021, 280



- c) The infrastructure and facilities (advanced tools) available to investigators are not exploited to their fullest potential in gathering information and locating the criminals.
- d) Public awareness. Many individuals are still unaware of the proper way to conduct online transactions in order to avoid being duped by cybercriminals. People want to trade fast and easily but are duped by the promise of making a large profit when all that is being offered is a string of lies. For instance, cases of binomo, farehnhheit, and similar crimes have emerged where the public appears to be hypnotized by the luxury cars displayed by the suspect, even though their true purpose is to attract the victim's attention and persuade them to invest money in their business without first verifying whether the business has actually registered or merely a phony business.

The following are the types of fraud that frequently take place in e-commerce transactions:

- a) The incompatibility of the products/goods consumers obtain with what they requested.
- b) The use of fictitious business actors or consumers or the use of false identities.
- c) Fraudulent discounts or sales rates offered by commercial actors.

This fraudulent crime is defined as disseminating false or misleading information about product advertisements or consumer identities that results in material or immaterial losses for consumers/buyers as well as for business actors/sellers. Based on this, if there is a legal issue, the provisions of Article 45 A paragraph 1 UU ITE are applicable criminal law with a maximum penalty of six years in prison and/or a maximum fine of one billion rupiah, then first ma ITE and technical investigations continue to make reference to the CPC's rules.<sup>21</sup>

Likewise, if there is a legal issue in e-commerce transactions, civil law remedies must refer to the ITE Law in conjunction with the Consumer Protection Law in conjunction with the Trade Law, which also governs how to trade online. Then, the solution must look at the options for law or choice of law, which law is agreed upon or subject to which law is the law in the country of the business actor or using international law. For the sake of convenience for both parties, e-commerce transactions should be made with a written agreement/contract that is approved and signed by the parties. If the contract has been agreed, then legally formally arises rights and obligations between the parties who make the agreement, regardless of whether to use the legal process in litigation or non-litigation (alternative dispute resolution).<sup>22</sup>

Law No. 11 of 2008, which was later revised/updated to Law No. 19 of 2016 regarding ITE, serves as the legal foundation for cybercrime control. The criminal law provisions are specified in Articles 27 to 35, which define the form and nature of the offense. The law then regulates criminal threat in Articles 45 to 52, with each article's specifics as follows:

Concerning the offense of disseminating, propagating, or transferring unauthorized material.

- a) Article 27 paragraph 1 of the Constitution contains regulations pertaining to decency.
- b) Article 27 paragraph 2 regulates gambling

---

<sup>21</sup> Praswtiyo, Muktar Zuhdy, Penegakan Hukum Oleh Aparat Penyidik Cyber Crime Dalam Kejahatan Dunia Maya (Cyber Crime) di Wilayah Hukum Polida DIY, International Journal Of Criminal and Criminology, Vol.1 No. 2, 2020, 85

<sup>22</sup> Sefitrios, Topik Yanuar Chandra, The Process and Performance Of Combating Cyber Crime In Indonesia, Jurnal Sosial dan Budaya Syar-i, Vol. 8 No. 4 , 2021, 980.

- c) Article 27 paragraph 3 of the Constitution regulates slander and defamation.
- d) In Article 27 paragraph 4, extortion threats are prohibited.
- e) Article 28 paragraph 1 regulates bogus news, misleading news, and fraud.
- f) Article 28 paragraph 2 of the SARA regulates incitement to hatred.
- g) Article 29 of the Constitution regulates threats of domestic violence.
- h) Article 30 of the Constitution regulates unauthorized access.
- i) Article 31 paragraph 1 regulates illegal interceptions and wiretapping.

#### Crime involving interference or interfering

- a) Interference with confidential data under article 32
- b) System interference as described in Article 33
- c) Providing resources for activities outlawed by article 34
- d) Article 35's reference to information manipulation or falsification
- e) Weighing - Article 52, Weighing Criminal Threats.
  - 1) The inquiry described in article 42 must be conducted in compliance with both the criminal provisions/regulations controlled in this legislation and the requirements of/rules of the criminal procedure law.
  - 2) The evidence for investigation, prosecution, and trial examination as governed by Article 44 is modified in accordance with the law or *ius constitutum*, which is (*lex generalis*), and is supplemented with electronic evidence as governed by the requirements of this Law as specific provisions (*lex specialist*).
  - 3) Articles 45 to 52, which regulate the criminal threat posed by cybercrime, carry the harshest penalties without establishing a minimum term.<sup>23</sup>

If we look from neighboring countries regarding the comparison of cyber crime laws in both Singapore and Malaysia, it turns out that the publication and distribution of illegal content using the internet, computers and technology is not considered a part of cyber crime. In Singapore, cybercrimes include the Computer Misuse Act which prohibits certain types of cybercrimes such as unauthorized access, disclosure of secrets, destruction or damage to computer systems or electronic data, and computer fraud. Same in Malaysia, the Computer Crime Act covers basically the same offenses as the Singapore Computer Misuse Act. Both countries do not have specific provisions on freedom of expression such as cyber defamation and hate because such violations are covered in the standard Criminal Code.<sup>24</sup>

With the development of current technology, it has given a new nuance in the field of evidence in court so that the evidence presented at trial is not only limited to physical evidence as regulated in the Criminal Procedure Code, which includes letter evidence or witness evidence but has also penetrated into the use of physical evidence. Evidence in the form of digital documents in the form of discs (CS, VCD, DVC) or in other evidence in the form of writings on social media and other electronic evidence.<sup>25</sup>

The birth of the ITE Law is a bit of progress in responding to and overcoming the current rise of cyber crime, especially in the law enforcement process if we look at Article 1 point (1) of the ITE Law, it is stated that electronic information is one or a collection of

<sup>23</sup> I Kadek Arya Sumadiyasa dkk, Pertanggungjawaban Pidana Pelaku Cyber Crime Dengan Konten Pornografi, *Jurnal Interprestasi Hukum* Vo. 2, No. 2, 2021, 375.

<sup>24</sup> Putnam, Tonya L and Elliot, David D. “ *International Responses to Cyber Crime. Sofare. D. Abraham and Goodman Seymour. E. [ed.] Transnational Dimension of Cyber Crime and Terrorism,*”(USA: Hoover Institution Press Publication,2001), 2.

<sup>25</sup> Miftakur Roham, Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya Dalam Sistem Hukum Indonesia, *Alqanun: Jurnal Pemikiran dan Pembaharuan Hukum Islam*, Vol.23 No.1 , 2020, 405-207.

electronic data, including but not limited to written information. , sounds, pictures, maps, photo designs, electronic data interchange (EDI), electronic mail (electronic mail, telegram, telex, telecopy or the like, letters, signs, numbers, access codes, symbols or processed perforations that have meaning or can be understood by those who can understand it.<sup>26</sup>

In Article 1 point (4) of the ITE Law states that any electronic information created, forwarded, sent, received, or stored in analog, digital, electromagnetic, optical or similar forms that can be seen, displayed and/or heard through a computer or electronic system. , including but not limited to writings, letters, pictures, maps, designs, photographs or the like, letters, numerals, access codes, symbols or perforations that have meaning or meaning that can be understood by people who are able to understand.

From the understanding of Article 1 paragraphs 1 and 4 of the ITE Law, there are differences between electronic information and electronic documents which are the basis for both, namely:

- a) In principle, electronic information can be distinguished but cannot be separated from electronic documents.
- b) Electronic information is data or a collection of data in various forms
- c) Electronic documents are containers or packages of electronic information
- d) For example, if we talk about music files in the form of mp3 then all information or music that comes out of the file is electronic information while the documents from the file are mp3.

If we look back at the comparison between the Criminal Code, precisely in articles 310, 311 and the ITE Law, it turns out that the criminal threat of the ITE Law is higher than the Criminal Code. Changes to the legislative framework relating to ITE from Law No. 11 of 2008 that was amended/stipulated into Law No. 19 of 2016 are in the provisions of articles: 1, 26, 31, 40, 43, and 45 paragraphs (A) and (B), which are the same and do not apply the threat of minimum punishment.

#### 4. CONCLUSION

In the Republic of Indonesia, which is a state of law, law enforcement against cybercriminals is crucial. In order to safeguard the rule of law and protect consumers who become victims of cybercrime, criminal punishments that are proportionate to the actions of cybercriminals must be imposed. According to the summary below, there isn't a single passage that focuses on how to conduct e-commerce transactions, but instead, most of the discussion is focused on general issues. This is also true for legal annexes; why only use the bare minimum of ketua annexes to create minimal annexes is beyond me. As a result, the relevant apparatus now has the opportunity to practice Islamic law in order to provide authoritative guidance on the subject. In keeping with the aforementioned, e-commerce use, which is recognized to be international and devoid of geographic limits, has a significant economic impact on international trade. Therefore, efforts to upgrade information technology devices must be made in tandem with the internet's rapid development in order to provide security and ease for e-commerce transactions. Regarding legal actions against cybercrime in e-commerce transactions, these include filing reports or complaints in accordance with the ITE Law and the Criminal Code. In contrast, legal actions against cybercrime that can be taken in a civil manner include filing a lawsuit with the court if the

---

<sup>26</sup> Andi Winjaya Laksana, *Pemidanaan Cyber Crime Dalam Perspektif Hukum Pidana Positif*, Jurnal Hukum Unissula, Vol. 35 No. 1, 2019, 62.



dispute is agreed upon in the contract or agreement the dispute is filed in later forms of litigation, if agreed through non-litigation, can file a lawsuit/application to the court.

## REFERENCES

### *Journal Article*

- Aulia Putri Fadhila, Tinjauan Kriminologi Dalam Tindakan Penipuan E Commerce Berdasarekan Peraturan Perundangan Pada Masa Covid 19, Jurnal Suara Hukum Volume 3 No. 2 Tahun 2021, p.280
- Getha Fety Dianari, Pengaruh Ecommerce Terhadap Pertumbuhan Ekonomi Indonesia, Jurnal Bina Ekonomi , Vol. 22 No. 1 Tahun 2018, p.46-47
- Supanto, Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) dan Antisipasinya Dengan Penal Policy, Yustitia, Vol. 5 No.1 ,2016,p. 53
- Andi Winjaya Laksana, Pemidanaan Cyber Crime Dalam Perspektif Hukum Pidana Psositif, Jurnal Hukum Unissula, Vol. 35 No. 1, 2019, p. 62.
- Miftakhur Roham, Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya Dalam Sistem Hukum Indonesia, Alqanun: Jurnal Pemikiran dan Pembahruan Hukum Islam, Vol.23 No.1 , 2020, p. 405-207.
- Dewi Bunga, Politik Hukum Pidana Terhadap Penanggulangan Cyber Crime, Jurnal Legislasi Indonesia, Vol.16 No.1. 2019, 3-6.
- Musa Darmin Pane, Sahat Maruli Tua Situmeang, Penegakan Hukum Cyber Crime Dalam Upaya Penaggulangan Tindak Pidana Teknologi Informasi, Jurnal Loyalis Sosial, Vol. 3 No. 2 ,2021, p. 95.
- Sefitrios, Topik Yanuar Chandra, The Process and Performance Of Combating Cyber Crime In Indonesia, Jurnal Sosial dan Budaya Syar-i, Vol. 8 No. 4 , 2021, p. 980.
- Praswtiyo, Muktar Zuhdy, Penegakan Hukum Oleh Aparat Penyidik Cyber Crime Dalam Kejahatan Dunia Maya (Cyber Crime) di Wilayah Hukum Polida DIY, International Journal Of Criminal and Criminology, Vol.1 No. 2, 2020, p.85.
- I Kadek Arya Sumadiyasa dkk, Pertanggungjawaban Pidana Pelaku Cyber Crime Dengan Konten Pornografi, Jurnal Interpretasi Hukum Vo. 2, No. 2, 2021, p. 375.
- Nida Rafa Arofah dkk, Internet Banking dan Cyber Crime : Sebuah Studi Kasus di Perbankan Nasional, Jurnal Pendidikan Akutansi, Vo. 18 No. 2, 2020, p. 112.
- Kristina Virgi Kusuma Putri, Kerja Sama Indonesia Dengan Asean Mengenai Cyber Crime Security dan Cyber Resilience Dalam Mengatasi Cyber Crime, Jurnal Hukum Lex Generalis, Vo. 2 No. 7, 2021, p. 546.

### *Book*

- Edy Army , 2020. Bukti Elektronik Dalam Perkara Peradilan, (Jakarta :Sinar Grafika, 2020).
- Purwaningsih, E. *Hukum Bisnis*, (Bogor :Ghalia Indonesia, 2010).
- Raharjo, A. *Cybercrime, Pemahanan Dan Upaya Pencegahan Kejahatan Berteknologi*. (Bandung : Citra Aditya Bakti, 2002).
- Wahid, Abdul dan M. Labib. *Kejahatan Mayantara, Cyber Crime*. (Bandung : Refika Aditama, 2005).

Yudha Bhakti Ardhiwisastra. *Penafsiran dan Kosntruksi Hukum*, Bandung: Alumni, 2000)

Soekanto, S, Pengantar Penelitian Hukum. (Jakarta, UI Press, 2018).

*Thesis, Web Page, and Others*

[https://eptik9.wordpress.com/2018/05/22/contoh kasus cybercrime dan penyelesaiannya E-Commerce Dalam Kejahatan Bisnis](https://eptik9.wordpress.com/2018/05/22/contoh-kasus-cybercrime-dan-penyelesaiannya-E-Commerce-Dalam-Kejahatan-Bisnis). (Fudji Sri Mar'ati)

<https://www.ui.ac.id/dampak-kejahatan-siber-pada-bisnis-ekonomi-digital/> diakses Tanggal 01 November 2022

CNBC Indonesia. 2022. Ada 5.000 Kasus Perbulan, Indonesia Emergency Kejahatan Siber. <https://www.cnbcindonesia.com/tech/20211011205453-37-283113/ada-5000-kasus-perbulan-indonesia-emergency-kejahatan-siber>. Diakses pada 01 November 2022.

<https://www.daya.id/usaha/artikel-daya/keuangan/macam-macam-sistem-pembayaran-pada-bisnis-e-commerce>

Putnam, Tonya L and Elliot, David D. . *International Responses to Cyber Crime*. Sofare. D. Abraham and Goodman Seymour. E. [ed.] *Transnational Dimension of Cyber Crime and Terrorism*. (USA :Hoover Institution Press Publication, ,2001).