Implementation of The Law Against Fraud Crimes in E-Commerce-Based Electronic Transactions

Elisabeth Saragih, Muhammad Arif Sahlepi, Muhammad Azhali Siregar

Abstract

Fraud is becoming increasingly prevalent with the times and technological advancements. Various laws and regulations have been enacted to address this issue, but it appears that these regulations have not been effective in addressing the increasing number of these crimes. This study aims to: first, identify law enforcement against e-commerce fraud; and second, analyze the obstacles in enforcing criminal law against e-commerce fraud. This study uses a normative juridical method through literature review by examining secondary data, such as laws and regulations, research results, scientific journals, and various related references. The results show that e-commerce fraud is essentially similar to conventional fraud, but differs in the evidence and means used because it involves electronic systems such as computers, the internet, and telecommunications devices. Therefore, law enforcement against this type of crime is still based on the Criminal Code (KUHP) and Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions. In addition, law enforcement against fraudulent acts in electronic-based transactions still faces a number of obstacles influenced by five main factors, namely laws and regulations, law enforcement officers, infrastructure or supporting facilities, community factors, and cultural factors.

***Keywords**:* Law Enforcement; Fraud; E-Commerce

Elisabeth Saragih[1]
Master of Law, Universitas Pembangunan Panca Budi, Indonesia
e-mail: elisabethsaragih086@gmail.com

Muhammad Arif sahlepi[2], Muhammad Azhali Siregar[3]
Master of Law, Universitas Pembangunan Panca Budi, Indonesia
e-mail: arifsahlepi@dosen.pancabudi.ac.id[2], azhalisiregar@dosen.pancabudi.ac.id[3]
2nd International Conference on Islamic Community Studies (ICICS)
Theme: History of Malay Civilisation and Islamic Human Capacity and Halal Hub in the Globalization Era
https://proceeding.pancabudi.ac.id/index.php/ICIE/index

Introduction

Advances in information and communication technology today have made it easier for people to convey and obtain information. Interaction and communication can be done without being hindered by distance, space, or time. Along with the rapid development of technology, people are required to be able to adapt and follow every change that occurs. Technology is no longer only used as a means of communication and social interaction, but has also evolved into a medium to carry out global business activities without borders. The real form of this development is the emergence of online trading activities through the internet network.

According to Ramli, trade activities carried out by utilizing internet media are known as electronic commerce or more popularly called *e-commerce* [1]. Meanwhile, Suhariyanto argued that e-commerce is a series of business activities that involve consumers, manufacturers, service providers, and intermediary traders by utilizing computer networks as the main media [2]. *E-Commerce* can also be understood as a process of buying and selling goods and services that is carried out through a computer network, namely the internet. At this time, it is undeniable that online buying and selling can be effective and efficient time so that someone can make buying and selling transactions with everyone anywhere and anytime. Moreover, the transaction is carried out without any face-to-face contact between the parties and they base the buying and selling transaction on a sense of trust with each other so that the buying and selling that occurs between the parties is carried out electronically (on-line) through the internet network.

Meanwhile, Melisa stated that the use of e-commerce in conducting business transactions provides various conveniences, both for business actors and consumers [3]. One of the reasons why transactions through e-commerce are more in demand than conventional trading patterns is that using e-commerce transactions can be done quickly, easily, and at a lower cost.

Kamlesh and Devani said that "a number of advantages can be obtained from this e-commerce, including [4]: First, the use of e-commerce allows for time savings, because business transactions between countries that usually require a few days in the conventional system can be completed in just a few minutes through internet services. Second, obstacles in the form of delays due to transportation obstacles can be avoided. Third, the risk of errors such as typos can be minimized because the e-commerce system has provided a standard format or model that does not need to be retyped. Fourth, time efficiency in business activities allows business actors to obtain more information related to their business, so that it can increase the effectiveness and efficiency of the company or business activities carried out.

Trade that utilizes the internet or online media, known as e-commerce (electronic commerce), is now part of the changing patterns of interaction in modern society. On the one hand, online trade has a positive impact on meeting human needs, because it is able to be effective and efficient in time. Through e-commerce, one can make buying and selling transactions with anyone, anywhere, and anytime without having to meet face-to-face. The transaction is based on mutual trust between the parties, so that the sale and purchase agreement is carried out electronically.

However, on the other hand, online transactions also have a negative impact. Because the seller and buyer do not meet face-to-face or interact directly, there is a possibility that the goods or services received are not as expected, or the amount of money received by the seller is not appropriate or even not received at all. Therefore, the right to information in electronic-based transactions is a very important aspect in its implementation. According to Eko, freedom of information is one of the substances of human rights (HAM) that has been recognized by the United Nations (UN) as part of human rights. This is affirmed in Resolution 59 Paragraph (1) which states that "Freedom of information is a fundamental human right and is a mark of all freedoms that are the main concern of the United Nations."

Currently, the crimes that occur cannot be categorized as physical crimes alone, but today's crimes are also developing along with the modernization of life. Wahidi and Labib said that "Online business has become a trend today, but it is reprehensible for irresponsible parties

to commit a crime that causes harm to others"[5]. Ikka argues that in the Internet world, the potential for criminals to commit crimes is very large and very difficult to catch because among the people in this cyberspace, most of them are fictitious or the identity of each person is not real [6]. In order to gain profit and enrich themselves, the perpetrators violate the applicable rules and legal norms. Online business makes it easier for fraudsters to carry out their actions.

The lack of firmness and clarity in law enforcement against perpetrators of fraud crimes in online businesses is often the main factor that causes these crimes to continue to be repeated. The author views that legal problems related to online fraud are basically based on only two main legal provisions, namely Article 378 of the Criminal Code and Article 28 paragraph (1) of the Electronic Information and Transaction Law (ITE Law). Article 378 of the Criminal Code regulates fraudulent acts committed with the intention of benefiting oneself or others unlawfully through the use of false names, false positions, deception, or a series of lies. Meanwhile, Article 28 paragraph (1) of the ITE Law emphasizes that anyone who deliberately and without the right spreads false or misleading news that causes losses to consumers in electronic transactions can be subject to legal sanctions. These two articles are the main basis for cracking down on electronic-based fraudsters, although in practice there are still various obstacles in their implementation [7].

Problem Formulation

1. How is the implementation of law enforcement against *e-commerce-based fraud?*
2. What are the inhibiting factors in criminal law enforcement against *e-commerce-based fraud?*

Purpose of The Problem

1. To find out the implementation of law enforcement against *e-commerce-based fraud?*
2. To find out the inhibiting factors in criminal law enforcement against *e-commerce-based fraud?*

Research Methodology

This research is a normative legal research using a normative juridical approach, which aims to critically analyze criminal law norms related to e-commerce-based fraud crimes. The focus of this research is to explore and uncover forms of protection and law enforcement for victims of fraud in electronic-based transactions. According to Fajar and Achmad, normative legal research is carried out with the aim of providing legal arguments that can be used as a basis to determine whether an event is in accordance with or contrary to the law, as well as how the event should be viewed from a legal perspective.[8] Meanwhile, the normative juridical approach according to Soekanto and Mamudji is legal research conducted by examining literature materials or secondary data as basic materials to be researched by conducting a search of regulations and literature related to the problem being researched.[9]

The data used in this study is secondary data consisting of several types of legal materials. Primary legal materials include National Law, including the 1945 Constitution of the Republic of Indonesia, the Criminal Code (KUHP), the Criminal Procedure Code (KUHAP), Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions, as well as various other relevant laws and regulations. In addition, this research also uses secondary legal materials in the form of the opinions of criminal law experts obtained from various literature, scientific journals, and articles, both in print and electronic form. The tertiary legal materials used include legal dictionaries and legal encyclopedias related to the topic of e-commerce-based fraud.

The data obtained through the literature study was analyzed using a qualitative analysis method presented descriptively. The descriptive qualitative analysis approach in this study is intended not only to describe the data as it is, but also to verify secondary data through a check and re-check (triangulation) process. This step aims to find the suitability, common ground, and

accuracy of the various views studied, so that objective conclusions can be obtained and close to scientific truth based on the results of the existing analysis.

Discussion

3.1 Law Enforcement Against E-Commerce-Based Fraud

According to Abdulkadir Muhammad, law enforcement can be interpreted as an effort to implement the law properly, supervise its implementation so that violations do not occur, and take remedial action if violations occur, so that the law that has been violated can be re-enforced as it should [10].

Jimly Asshidiqie differentiates law enforcement into two definitions. In a narrow sense, law enforcement is understood as an activity to take action against any form of violation or deviation from laws and regulations carried out through the criminal justice process. This process involves the role of law enforcement officials such as the police, prosecutor's office, advocates or lawyers, and judicial institutions [11]. Meanwhile, in a broad sense, it is an activity to implement and apply the law and take legal action against any violation of the law committed by a legal subject either through judicial procedures or through arbitration procedures and other dispute resolution mechanisms (alternative disputes or conflict resolution)".

Machmud said that "law enforcement is closely related to compliance for users and implementers of laws and regulations, in this case both the public and state administrators, namely law enforcers" [12].

Based on the various opinions that have been expressed previously, it can be concluded that law enforcement is an effort that aims to realize order and legal certainty in society. These efforts are carried out by ordering the implementation of the functions, duties, and authorities of each law enforcement agency in accordance with their respective scope and proportions. In addition, law enforcement must also be based on a good cooperation system between relevant institutions so that the goals of law enforcement can be achieved optimally.

Meanwhile, Muladi argued that in law enforcement, a strong moral element is needed, because the relationship between morality and law enforcement greatly determines the success or failure in achieving legal goals. Furthermore, he explained that the moral and ethical aspects in criminal law enforcement are closely related to the law enforcement process itself, which is ideally a process of finding facts objectively, impartially, and carried out in the spirit of solving problems in a fair and proper manner [13].

According to Sudarto, the law serves to regulate people's lives in a proper and beneficial manner, by setting limits on what is allowed and what is prohibited. Thus, the law draws a firm line between actions that are in accordance with the provisions of the law and actions that are contrary to it where the aspect of the act that is against the law is the main focus in law enforcement itself. Therefore, law enforcement, especially in the field of criminal law, can be understood as a reaction to violations of the law. The efforts made by law enforcement officials in dealing with unlawful acts and resolving various problems that arise in the law enforcement process are the core of the implementation of law enforcement itself [14].

In the context of criminal law, basically criminal law is part of public law that regulates the public interest. It contains provisions that stipulate acts that are prohibited to be committed, accompanied by the threat of criminal sanctions for violators. Criminal law also regulates the conditions regarding when and how a crime can be imposed. The use of criminal law in community life is essentially part of law enforcement efforts, namely to enforce legal norms so that they function as a real guideline for behavior in various legal relations in society and the state. Viewed from the point of view of the subject, criminal law enforcement can be carried out by various parties at large, because basically law enforcement is a shared responsibility that involves all elements in the legal system.

Criminal law enforcement is currently an urgent need for fundamental changes to achieve better penal goals and oriented towards human values. This need is in line with the spirit of

reform which emphasizes the importance of realizing fair law enforcement against every form of criminal law violation. In the context of the reform era, law enforcement is not only understood as the application of regulations alone, but must also reflect the principles of openness, democracy, protection of human rights, and justice and truth in all aspects of society, nation, and state life.

In addition, the dynamics of people's rapidly developing lives, driven by increasing technological advances, demand positive laws to be able to adapt to these changes in order to remain relevant and provide legal certainty for all levels of society. Thus, it can be understood that the level of development of the society where the law is enforced affects the pattern of law enforcement itself, because in a rational modern society, the law is required to be more responsive, adaptive, and reflect substantive justice.

Muladi said that "Criminal law enforcement is always felt to be in contact with morals and ethics, this is based on four reasons, namely [15]:

1. The criminal justice system typically involves Use coercion or violence (coercion) with the possibility of an opportunity to abuse power (Abuse of power);
2. Almost all professionals in criminal law enforcement are government servants who have special obligations to the public they serve;
3. For everyone, ethics can be used as a tool to help solve ethical dilemmas that a person faces in his professional life (enlightened moral judgment);
4. In professional life it is often said that a set ethical requirementments are as part of its meaning

Based on the theory in criminal law regarding the crime of fraud, there are two points of view that can be considered, namely the linguistic understanding and the juridical understanding. Etymologically, the root word for fraud is "deception," which means dishonest, false, or false deeds or words committed with the intent to mislead, outwit, or gain certain benefits in an improper way. Fraud in the sense of language is a fraudulent process, method, or act that aims to deceive or deceive other parties.

Furthermore, in the juridical sense, the definition of fraud is included in the formulation of criminal acts in the Criminal Code, but nevertheless the formulation of fraud in the Criminal Code is not a definition but only to establish the elements of an act so that it can be said to be fraud and the perpetrator can be punished.

Article 378 states that *"Whoever with the intention of benefiting himself or others against his rights, uses a false name or character or uses deception or a contrivance of false words, induces another person to hand over an object or enter into a debt agreement or cancels a receivable, because he has wrongfully committed fraud, shall be punished with imprisonment for a term of not more than four years".*[16]

However, if you look at the criminal acts of fraud that have currently undergone development, it is felt that it is difficult in terms of proof if law enforcement officials are only guided by the articles in the Criminal Code.

Fraud that occurs in today's cyber world can be carried out in a variety of ways, ranging from simple to complex. Simple forms of fraud can be in the form of sending false information (fake news), unauthorized identity disguise (impersonation), or deceptive actions through internet media with the aim of obtaining personal gain. Meanwhile, more complex forms of fraud usually involve an organized modus operandi, carried out by groups or networks that have a specific division of roles and work systems. Seeing these developments, the provisions regarding fraud as stipulated in the Criminal Code (KUHP) are considered to have limitations in accommodating the characteristics, modes, and provision of sanctions for fraudulent crimes committed through electronic or e-commerce-based media.

In line with this, Maskun and Wiwik said that there are two important things that need to be considered in the context of fraud in cyberspace. First, cybercriminals generally commit fraud aimed at computer systems, not directly at individuals. Second, the series of actions

carried out by the perpetrators of criminal acts is difficult to classify into the forms of acts as stipulated in the Criminal Code (KUHP), because the provisions in the Criminal Code are basically designed to ensnare acts committed against humans, not against computer systems or electronic devices.[17]

Therefore, in order to provide legal certainty and strengthen law enforcement efforts against fraud crimes based on e-commerce activities, the Government of Indonesia enacted Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law). Furthermore, to adapt to technological developments and the legal needs of the community, the regulation has been amended through Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (Law 19/2016).

As a special law (lex specialis derogat legi generali), the Electronic Information and Transaction Law (ITE Law) functions as a guideline as well as a legal basis for the public to carry out activities in cyberspace. In addition, the ITE Law is related to a number of provisions in the Criminal Code (KUHP) which play a role in simplifying the process of resolving cases involving information technology elements. In facing the challenges and dynamics of global communication, the existence of this law is expected to function as an ius constituendum, namely laws and regulations that are adaptive and anticipatory to technological developments and various problems that arise, including the negative impact of information technology advances that have wide implications on people's lives.

Regarding the legal protection provided by the ITE Law, it is also felt that it does not directly regulate the crime of conventional fraud or the crime of online fraud.However, related to the definition of fraud that has an impact on the occurrence of victim losses in electronic transactions, there is a provision that regulates these losses in Article 28 Paragraph (1) of the ITE Law which states that "Everyone intentionally, and without the right to spread false and misleading news that results in consumer losses in Electronic Transactions". Suseno argued that "The elements in Article 28 Paragraph (1) of the ITE Law are identical and have some similarities to the conventional fraud crime regulated in Article 378 of the Criminal Code and have special characteristics, namely the recognition of evidence, electronic media, and the expansion of jurisdiction in the ITE Law".[18]

In the Electronic Information and Transaction Law (ITE Law), it is emphasized that electronic information, electronic documents, and printed results are recognized as valid legal evidence. This provision is a form of expansion of the evidence system regulated in the procedural law in Indonesia, where previously the evidence had not been recognized in conventional courts. With this recognition, the information and/or electronic documents along with their printed results now have a legal status equivalent to other evidence in court, thus increasing the type of evidence that can be used in the law enforcement process.

In addition, in the context of law enforcement, there is important material in the ITE Law, namely recognition of the expansion of legal evidence in accordance with the procedural law applicable in Indonesia. The expansion in question is the recognition of information, documents and electronic signatures as evidence. This means that now there is one more piece of evidence that can be used in court. Information and electronic documents as well as electronic signatures that are part of it can be valid evidence as affirmed in Article 5 Paragraph (1) of the ITE Law.

Juridical recognition through Article 5 Paragraph (1) of the ITE Law on electronic evidence actually has the juridical effect of recognizing the electronic evidence as part of the evidence that has been in force so far. The recognition of electronic evidence is a step forward in the law of evidence. If there is a civil case that disputes an electronic document in the form of an electronic contract, then the document can be used as a reference for the parties to resolve the case or the judge who will later decide the case.

In the end, to ensnare the perpetrators of e-commerce-based crimes , the legal basis that can be given to the perpetrators is Article 378 of the Criminal Code. However, Article 378 of the Criminal Code regarding fraud cannot be used to burden perpetrators of online fraud crimes

to account for their actions, because there are several obstacles in imposing criminal sanctions on perpetrators of criminal acts such as obstacles in proving evidence that are limited by the Criminal Code. Therefore, to strengthen the legal basis, it can be added with article 28 paragraph (1) juncto article 45 paragraph (2) of the ITE Law.

Although the ITE Law does not explicitly regulate specific provisions regarding fraud crimes, in certain contexts this law can still be used as a basis to ensnare perpetrators to account for their actions in the case of online fraud that occurs in e-commerce activities or online buying and selling transactions. This is in line with the essence of the establishment of the ITE Law, namely as an instrument of legal protection for consumers in carrying out electronic transaction activities in order to create certainty, security, and justice in the digital space.

Article 28 Paragraph (1) of the ITE Law can basically only be applied to fraudulent crimes that occur in the context of electronic transactions or online buying and selling, because the article specifically regulates the spread of false and misleading news that results in losses for consumers in electronic transactions. Meanwhile, Article 378 of the Criminal Code is used to ensnare perpetrators of conventional fraud that is carried out directly without involving electronic media. Thus, Article 28 Paragraph (1) of the ITE Law can be said to be a lex specialis that regulates specifically the crime of fraud in electronic transactions, while Article 378 of the Criminal Code is a lex generalis that regulates fraud in general.

3.2 Obstacles In Law Enforcement Against E-Commerce-Based Crimes

If you look at the existing legal factors, currently law enforcement apparatus do use the Criminal Code, Criminal Code, ITE Law and other related laws as a legal basis in ensnaring e-commerce-based fraudsters, but in its implementation with many existing articles applied to perpetrators, there are many multiinterpretations for law enforcement officials so that in its implementation one article is needed that specifically regulates fraud-based crimes e-commerce that can be included in the ITE Act [19].

For example, in Article 28 Paragraph (1) of the ITE Law, it is stated that "Every Person intentionally, and without the right to spread false and misleading news that results in consumer losses in Electronic Transactions." Meanwhile, Article 378 of the Criminal Code states that "Whoever with the intention of unlawfully benefiting himself or others, by using a false name or false dignity, by deception, or a series of lies, moves another person to hand over something to him, or to give a debt or write off a debt, is threatened with fraud with a maximum prison sentence of four years" [20].

From the formulations of Article 28 Paragraph (1) of the ITE Law and Article 378 of the Criminal Code, we can know that both regulate different things. Article 378 of the Criminal Code regulates fraud, while Article 28 Paragraph (1) of the ITE Law regulates fake news that causes consumer losses in electronic transactions. However, the formulation of Article 28 Paragraph (1) of the ITE Law does not require the existence of an element of self-benefit or others as stipulated in Article 378 of the Criminal Code regarding fraud so that in proving it it is felt that there are still difficulties or even multiple interpretations for law enforcement officials to ensnare perpetrators of e-commerce-based fraud crimes. Therefore, a more specific article is needed that can be included in the ITE Law to ensnare perpetrators of *e-commerce-based* fraud [21].

It can be understood that the capabilities of law enforcement officers today are no longer comparable to the capabilities of law enforcement officers in the past. Law enforcement officials are currently required to keep up with the times and existing technological developments so that crimes that develop can also be minimized. In addition, the understanding of the articles in the existing positive law should be taken seriously by law enforcement officials so that there are no more multiple interpretations in implementing articles against the perpetrators of *e-commerce*-based fraud [22].

The infrastructure factor is also felt to be one of the factors of weak law enforcement against the crime of fraud. For example, the computer facilities currently available only function as administrative activities, while e-commerce-based crimes are carried out using computers that are networked and have a high and complex technological capacity so that it is still difficult for law enforcement officials to track, detect or compensate for the activities of the perpetrators of these crimes. The same can also be seen in the lack of ability and skills of law enforcement officials in the field of computers which results in tactical, technical investigations, prosecutions and examinations in the courts not being mastered because it concerns the systems in the computer [23].

Furthermore, the community factor is also felt to be an obstacle in law enforcement against e-commerce-based fraud crimes where there are still many people who are reluctant to report fraudulent crimes, causing difficulties for law enforcement officials to take action against the perpetrators of these crimes. Another factor that the public feels is that when the problem is brought to the court process, it is feared that it will require larger funds during the procedural process compared to the losses suffered.

Therefore, existing rules or legal norms should be able to direct the community to the rules in living in society and the state properly. Laws in the form of laws or regulations are generally designed based on certain assumptions. However, the circumstances or culture that exist in society are not always in accordance with expectations, so unexpected circumstances can arise at all. The current law is not necessarily able to answer the cultural problems of society that are changing and developing now or in the future, so there needs to be a change or the creation of new legal rules to answer these problems [24].

Widodo said that "crime is very closely related to the development of society. Crime has become part of the culture itself". This means that the higher the culture and the more modern a nation is, the more modern the crime is in its form, nature and way of execution.

The obstacles described earlier must at least be minimized immediately because talking about the current technological development is also allegedly very fast so that there needs to be a more progressive legal rule to overcome these obstacles.

In the end, law enforcement efforts in handling e-commerce-based fraud crimes still require synergy between a participatory community and law enforcement officials who are democratic, transparent, responsible and human rights-oriented, so that it is hoped that it can truly realize an Indonesian civil society with social justice. The legal rules that are currently in force should also need to be observed and understood by law enforcement officials and implemented as well as possible so that these problems can be minimized and eliminated [25].

Conclusion

1. E-commerce-based fraud is in principle the same as fraud in conventional ways. It's just that the difference lies in the evidence or the means of doing it, namely using electronic systems (computers, internet, telecommunication devices). Therefore, law enforcement regarding this criminal act of fraud should still be accommodated by the Criminal Code through article 378, and to strengthen the legal basis, it can also be accommodated through Article 28 paragraph (1) of Law Number 19 of 2016 concerning Information and Electronic Transactions. As a special law (Lex Specialist Derogat Lex Generale), the ITE Law can at least be a guideline and legal basis for members of the public in their activities in the cyber world. In addition, the ITE Law also has links to several articles regulated in the Criminal Code which aim to make it easier to resolve a case. Given the challenges and demands of the development of global communication, the law is expected to be an ius constituendum, namely laws and regulations that are accommodating to developments and anticipatory to problems, including the negative impact of information technology advances that have a wide impact on society.

2. Furthermore, related to obstacles in law enforcement against E-Commerce-based crimes , it is still in accordance with five factors that affect law enforcement, namely first, the legal factor itself where there are still rules that have not been specifically explained for e-commerce-based fraud crimes, second, law enforcement factors where there are still law enforcement officials who do not understand the existing rules so that in their implementation it is still multi-interpretation, the three factors of facilities and infrastructure that support law enforcement that can help uncover these criminal acts, the four factors of society where there is still a lack of public awareness to provide information or reports on the problems faced and the reluctance of the community to process in the courts; and cultural factors where the higher the culture and the more modern a nation is, the more modern the crime is in its form, nature and way of implementation.

References

[1] Abdul Wahidi And M. Labib, Cybercrime (Bandung: Refika Aditama, 2005).
[2] Abdulkadir Muhammad, Ethics of the Legal Profession (Bandung: Pt. Citra Aditya Bakti, 2006).
[3] Agnes Debora Elisabeth Kaunang, "Spreading misleading fake news resulting in consumer losses in electronic transactions is a criminal offense according to the ITE Law (Supreme Court Decision Number 3905 K/PID. Sus/2022)," Lex Privatum 13, No. 4 (2024).
[4] Agus Kasiyanto and Thon Jerri, "Law Enforcement Against Perpetrators of Fraud Crimes Committed through Electronic Media," Journal de Facto 4, no. 2 (2017): 222–44.
[5] Ahmad M. Ramli, Cyber Law and IP in the Indonesian Legal System (Bandung: Refika Aditama, 2004).
[6] Budi Suhariyanto, Information Technology Crime (Cybercrime), The Urgency of Regulation and Its Legal Loopholes (Jakarta: Rajawali Press, 2012).
[7] in creating a competitive market based on business competition law," Journal of Business Law Bonum Commune I, no. 1 (2018): 28–38.
[8] Eko Noer Kristiyanto, "The Urgency of Information Disclosure in the Implementation of Public Services," Journal of De Jure 16, no. 2 (2016): 231–244.
[9] Fandy Ardiansyah, "Criminal Liability of Perpetrators of Preparatory Acts in Terrorism Crimes," Media Iuris 2, No. 3 (2020).
[10] Hendy Sumadi, "Obstacles in Overcoming the Crime of Electronic Transaction Fraud in Indonesia," Journal of Insight Yuridika 33, no. 2 (2015): 175–203.
[11] Ikka Puspitasari, "Criminal Liability of Perpetrators of Online Fraud in Positive Law in Indonesia," Journal of Humani 8, No. 1 (2018): 1–14.
[12] Jimly Asshidiqie, Constitutional Law and the Pillars of Democracy, Fragments of Legal Thought, Media and Human Rights (Jakarta: Constitution Press and Pt. Syaamil Cipta Media, 2006).
[13] K Kamlesh And Nag Devjani, E-Commerce The Cutting Edge Of Business (New Delhi: Tata Mc.Grawhill Publishing Company Limited, 1999).
[14] Laurensius Arliman, Law Enforcement and Community Awareness (Deepublish, 2015).
[15] Maskun and Wiwik Meilararti, Legal Aspects of Internet-Based Fraud (Bandung: Keni Media, 2017).
[16] Mukti Fajar and Achmad Yulianto, Dualism of Normative and Empirical Law Research (Yogyakarta: Pustaka Siswa, 2017).
[17] Initially, Human Rights. (Bandung: Pt. Refika Aditama, 2009).
[18] Republic of Indonesia, Criminal Code (Law Number 1 of 2023 concerning the Criminal Code), Article 378.

[19] Republic of Indonesia, Law No. 11 of 2008 concerning Information and Electronic Transactions (Indonesia, 2008).
[20] Shahrul Machmud, Indonesian Environmental Law Enforcement (Yogyakarta: Graha Ilmu, 2012).
[21] Sigid Suseno, Jurisdiction of Cyber Crime (Bandung: Pt. Refika Aditama, 2012).
[22] Soerjono Soekanto And Sri Mamudji, Normative Law Research (Jakarta: Rajawali Press, 2001).
[23] Sudarto, Kapita Selekta Criminal Law (Bandung: Alumni, 1996).
[24] Tanti Kirana Utami et al., "The Influence of Legislative Theory on the Dynamics of Legal Norms in the Indonesian Legal System," Ius Publicum 5 Law Journal, no. 2 (2024): 264–93.
[25] Tony Yuri Rahmanto, Jhrs Kav, and South Jakarta Kuningan, "Law Enforcement Against Fraud Crimes Based on Electronic Transactions," Journal of De Jure Legal Research 19, no. 1 (2019): 31.