

# Law Enforcement And Factors Background To The Crime Of Fraud In Online Selling Transactions In Indonesia

Apriyas Munik<sup>\*1</sup>, Fajar Ali Syabana<sup>2</sup>, Ewin Eka Wijayanto<sup>3</sup>, Ali Rasya<sup>4</sup>,  
Sufiarina<sup>5</sup>

<sup>#</sup>Tama Jagakarsa University  
Jakarta, Indonesia

<sup>1</sup> munik.munik@gmail.com

**Abstract** -The country of Indonesia is experiencing the growth of online shops which are developing very rapidly, several electronic transaction sites (e-commerce) or commonly called online shops which are well known especially to the people in Indonesia, including: Bukalapak.com, Tokopedia, OLX, Blibli.com, Elevenia, Lazada, Shopee, Berrybenka, Blanja.com, Zalora, JD.id and others. However, related to technological developments is one of the factors that can lead to crime. The forms of crime that exist are increasingly varied and more contemporary. Crime has been accepted as a fact, both in the simplest (primitive) society and in modern society, which is detrimental to society. The losses incurred can be in the form of losses in the sense of material or immaterial. Material losses, for example victims of crime and damage or destruction of property as well as the increased costs that must be incurred for handling it. Immaterial losses can reduce or lose public trust in the implementation of law enforcement carried out by law enforcers. With the development of technology, in reality crimes through the misuse of information technology are increasingly being committed. The type and mode of crime itself continues to grow. Criminal acts of fraud in online buying and selling transactions are currently growing with the times and technological advances. Legal regulations are made to anticipate this, but the existing regulations do not seem to reduce these crimes but have increased. Based on what has been described in the background above, the author tries to identify the following problems: What are the legal provisions against perpetrators of fraud in online buying and selling transactions? What are the factors behind the crime of fraud in online buying and selling transactions in Indonesia? In this journal the author uses a normative juridical approach, namely a method in which law is conceptualized as norms, rules, principles or dogmas. Legal provisions against perpetrators of criminal acts of fraud in online buying and selling transactions. As is known, the arrangements regarding electronic transactions regulated in Law no. 11 of 2008 concerning Information and Electronic Transactions and Law no. 19 of 2016 concerning Amendments to Law no. 11 of 2008 concerning Electronic Information and Transactions as the main basis for online buying and selling arrangements and Government Regulation Number 71 of 2019 concerning Electronic System and Transaction Operations. .

**Keywords** — Law Enforcement, Fraud Crimes, Online Buying and Selling Transactions.

## I. INTRODUCTION

At this time, the State of Indonesia, has experienced very rapid development in various fields, especially in the field of information technology. Technological developments make it easy for people to carry out activities to meet their needs and interact with other humans wherever they are. Technology apart from bringing advantages such as making it easy for people to carry out their activities, also causes disadvantages such as the rise of crimes committed through information technology. Technology has also had a significant influence on the understanding of crime, especially towards schools of criminology which emphasize the human factor, both physically and psychologically.

The trading system in the world has developed very rapidly, this is influenced by the development of internet-based technology known as e-commerce. The development of e-commerce is inseparable from the growth rate of the internet, because e-commerce runs through the internet network. One of the forms of the use of information technology that is highly developed, most influential and widest in scope is e-commerce (Electronic Transactions). E-commerce is a modern business model that is non-fiction (does not physically present business people) and non-sign (does not use an original signature).

Electronic transactions (e-commerce) are the dissemination, buying, selling, marketing of goods and services through electronic systems such as the internet or television, the world wide web (www), or other computer

networks. Electronic transactions may also involve electronic fund transfers, electronic data exchange, automated inventory management systems, and automated data collection systems.

The electronic transaction itself according to Article 1 point 2 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (State Gazette of the Republic of Indonesia of 2016 Number 251, Supplement to the State Gazette of the Republic of Indonesia Number 5952) for hereinafter referred to as the ITE Law, that electronic transactions are legal acts carried out using computers, computer networks, and/or other electronic media. In accordance with the above understanding, buying and selling activities carried out via a computer or mobile phone can be categorized as an electronic transaction.

In fact, the Internet has brought the world economy into a new chapter which is more popular with the term digital economy or digital economy (Richardus Eko Indrajit, 2001). Its existence is marked by the increasingly widespread economic activity that utilizes the internet as a medium of communication, collaboration and cooperation. Trade, for example, is increasingly relying on electronic transactions / electronic commerce (e-commerce) as a transaction medium and it is estimated that from 2003 to 2018 more than 95% (ninety-five percent) of all internet activities are electronic trading activities.

According to the World Trade Organization (WTO), the scope of e-commerce includes the fields of production, distribution, marketing, sales and delivery of goods and or services via electronics, while the OECD (Organization or Economic Cooperation and Development) explains that e-commerce is a transaction based on processes and electronic data transmission. Apart from these two international institutions, the Alliance for Global Business, a leading trade association defines e-commerce as all value transactions involving the transfer of information, products, services or payments through electronic networks as a medium.

As a trade based on sophisticated technology, electronic transactions (e-commerce) have reformed conventional trade where interactions between consumers and companies that were previously carried out directly become indirect interactions. Electronic transactions (e-commerce) have changed the classical business paradigm by growing models of interaction between producers and consumers in the virtual world. Trading systems used in electronic transactions (e-commerce) are designed to sign electronically. Electronic signing is designed from the time of purchase, inspection and delivery. Therefore, the availability of correct and accurate information about consumers and companies in electronic transactions (e-commerce) is an absolute requirement, especially information regarding payments (Ade Maman Suherman, 2002).

In the world, related to the development of electronic transactions (e-commerce) has shown a very significant increase in recent years, not only in developed countries such as the European Continent but also in developing countries such as Malaysia, Thailand and Indonesia. Of course, with these developments, many advantages are offered by electronic transactions (e-commerce) which are difficult or cannot be obtained through conventional transaction methods. Basically, the advantages of using electronic transactions (e-commerce) can be divided into 2 (two) parts, namely advantages for traders and benefits for buyers (Abdul Halim Barkatullah and Teguh Prasetyo, 2005).

In the world, related to the development of electronic transactions (e-commerce) has shown a very significant increase in recent years, not only in developed countries such as the European Continent but also in developing countries such as Malaysia, Thailand and Indonesia. Of course, with these developments, many advantages are offered by electronic transactions (e-commerce) which are difficult or cannot be obtained through conventional transaction methods. Basically, the advantages of using electronic transactions (e-commerce) can be divided into 2 (two) parts, namely advantages for traders and benefits for buyers.

In line with this thought, according to (Arief Dikdik Mansur, 2005) the benefits for consumers who shop through electronic transactions include:

- a. Home Shopping. Buyers can make transactions from home so they can save time, avoid traffic jams, and reach shops that are far from locations;
- b. Easy to do. There is no need for special training to be able to shop or make transactions via the internet;
- c. Buyers have a very broad choice and can compare the products and services they want to buy;
- d. No time limit. Buyers can make transactions anytime 24 hours per day, 7 days per week;
- e. Buyers can look for products that are not available or difficult to obtain at traditional outlets/markets.

Through e-commerce, all the formalities commonly used in conventional transactions are reduced, besides, of course, consumers also have the ability to collect and compare information such as goods and services more freely without being limited by boundaries (borderless).

Until now, in Indonesia, the growth of online shops is growing rapidly, several electronic transaction sites (e-commerce) or commonly called online shops, which are well known especially to people in Indonesia, including: Bukalapak.com, Tokopedia, OLX, Blibli.com, Elevenia, Lazada, Shopee, Berrybenka, Blanja.com, Zalora, JD.id and others.

However, related to technological developments is one of the factors that can lead to crime. The forms of crime that exist are increasingly varied and more contemporary. Crime actually grows and develops in society,

there is no crime without society. Even though we know a lot about the various factors of crime that exist in society, what is certain is that crime is a form of human behavior that continues to experience development parallel to the development of society itself.

Crime has been accepted as a fact, both in the simplest (primitive) society and in modern society, which is detrimental to society. The losses incurred can be in the form of losses in the sense of material or immaterial. Material losses, for example victims of crime and damage or destruction of property as well as the increased costs that must be incurred for handling it. Immaterial losses can reduce or lose public confidence in the implementation of law enforcement by law enforcers (Agus Raharjo, 2002).

Crime is an anti-social act, not only in a developing society, but also in an advanced society (with more sophisticated technological equipment, of course). Crime is not only in the real world, but also in the virtual world, which is different from conventional crime, because it has been refined in such a way. The existence of a crime is identical to the existence of the human being himself, even though there is a possibility that the form or type of crime in each society is different (Agus Raharjo, 2002).

With the development of technology, in reality crimes through the misuse of information technology are increasingly being committed. The type and mode of crime itself continues to grow. Criminal acts of fraud in online buying and selling transactions are currently growing with the times and technological advances. Legal regulations are made to anticipate this, but the existing regulations do not seem to reduce these crimes but have increased.

## II. METHOD

In this journal the author uses a normative juridical approach, namely a method in which law is conceptualized as norms, rules, principles or dogmas. Data collection techniques are carried out through reviewing data obtained from legislation, text books, research results, magazines, articles and others.

## III. RESULT AND DISCUSSION

### 1. Legal Provisions Against Fraudulent Offenders in Online Buying and Selling Transactions.

Law is a socio-cultural phenomenon that functions to apply certain rules and patterns of behavior to individuals in society. If the law that applies in society is not in accordance with their needs and interests, then they will find a way out and try to deviate from the existing rules. All forms of deviant behavior that are disruptive and detrimental to social life are interpreted by society as evil attitudes and behavior. Law is a means in which values or concepts about justice, truth, social benefit and so on are contained.

According to Satjipto Raharjo, law enforcement is essentially an implementation of abstract ideas or concepts. Law enforcement is an effort to realize these ideas into reality. Soerjono Soekanto said that law enforcement is an activity of harmonizing the relationship of values described in the principles or views of solid values and attitudes as a series of final stages of value translation to create, maintain and maintain social peace. Concrete law enforcement is the application of positive law in practice as it should be obeyed.

If the essence of law enforcement embodies values or principles that contain justice and truth, then law enforcement is not only the duty of conventionally known law enforcers, but is the duty of everyone. Law enforcement is a process that involves many things. Therefore, the success of law enforcement will be influenced by these things. In general, as stated by Soerjono Soekanto, there are five factors that influence law enforcement, namely:

- a. The legal factor itself.
- b. Law enforcement factors, namely the parties that form and apply the law.
- c. Facility factors and facilities that support law enforcement.
- d. Community factors, namely the environment where the law applies and is applied.
- e. Cultural factors, namely as a result of work, creativity and taste based on human initiative in social life.

The five factors mentioned above are closely related to each other, because they are the essence of law enforcement and are also a benchmark for the effectiveness of law enforcement.

In another article, Soerjono Soekanto said that in order for the law to function properly, harmony is needed in the relationship between four factors, namely as follows:

- a) The law or regulation itself. The possibility is that there is a discrepancy in the laws and regulations regarding certain areas of life.
- b) The mentality of officers upholding the law. If the laws and regulations are good, but the mentality of law enforcers is not good, there will be disturbances in the law enforcement system.
- c) Facilities expected to support the implementation of the law. If the laws and regulations are good and the mentality of the enforcers is good, but the facilities are inadequate, then law enforcement will not work properly.
- d) Legal awareness, legal compliance and community behavior.

The four factors mentioned above are interrelated and form the core of the law enforcement system. If these four factors are examined carefully, it will be revealed that matters that affect the law enforcement system.

Today's world civilization is characterized by the phenomenon of technological progress, information and communication that takes place in almost all areas of life. The revolution produced by information and communication technology is usually seen from the point of view of the rapid development of information technology that must be anticipated with the laws that govern it. These negative impacts must be anticipated and mitigated by laws related to the use of information and communication technology.

For many people, electronic transactions are a new and popular terminology in Indonesia. Basically, electronic transactions are the result of developments in information and telecommunications technology, and significantly change the way humans interact with their environment, which in this case is related to the buying and selling mechanism.

In addition, the development of information technology has caused the world to become borderless and has caused significant social change to take place so quickly. Information technology is currently a double-edged sword, because in addition to contributing to increasing human welfare, progress and civilization, it is also an effective arena for acts against the law. Crime everywhere in various parts of the world is also experiencing very rapid development in line with the rapid advancement of science and technology.

Along with the progress of time and technology that is so rapid, as well as economic growth, accompanied by an increasing number of people in each region offset by difficult and narrow employment opportunities, this does not rule out the possibility of a person committing a crime. One form of crime that we often find against a background of a desire to make ends meet in the material sector is the crime of theft, embezzlement, fraud and extortion, both carried out compulsorily or because it is a habit which in the end is used as a livelihood to meet our needs, daily.

The criminal procedural law regulates the process of handling or enforcing cybercrime or in this case specifically fraud using social media, starting from investigations to court decisions.

In buying and selling online, people can enter into online sales agreements through a leading e-commerce company in Indonesia, both Tokopedia, Lazada, Blibli.com, Bukalapak, Zalora, Shopee, Berrybenka, Kaskus and Traveloka, which are certainly leading online trading companies (e-commerce). commerce) or large marketplaces in Indonesia that already have a neatly structured system to prevent the occurrence of fraud prone so they tend to be safer, compared to buying and selling online either Facebook, messenger, telegram, WhatsApp, Instagram, Twitter, forums which of course have a very high risk of being vulnerable fraud because online buying and selling sites are not a leading e-commerce company in Indonesia, which of course does not have a neatly structured system to prevent the occurrence of fraud-prone so it tends not to be too safe against fraud.

As is known, the legal arrangements that have regulated the problem of fraud in online buying and selling agreements in Indonesian positive law are both arrangements regarding electronic transactions regulated in Law no. 11 of 2008 concerning Information and Electronic Transactions and Law no. 19 of 2016 concerning Amendments to Law no. 11 of 2008 concerning Information and Electronic Transactions as the main basis for online buying and selling arrangements, Government Regulation of the Republic of Indonesia Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions. However, with the existence of these legal arrangements, the fact is that society is still found to be prone to fraud in buying and selling online and until now it is still happening in various ways related to the digital world. In Indonesia, these legal arrangements are for anticipating, optimizing and the government and related agencies continue to try to suppress the occurrence of legal problems that often occur in online buying and selling, namely mainly the problem of fraud in buying and selling online which is still prone to fraud.

With the development of society and technology, there has been a change in the lifestyle and behavior of the world community, where initially a sale and purchase agreement was in the form of a conventional (written and oral) has now experienced development with the advent of electronic agreements or contracts. However, with the emergence of the development of electronic agreements or contracts, which were originally face-to-face (conventional) sale and purchase agreements have now switched to online sale and purchase agreements, online sale and purchase agreements in this case are not carried out directly but through online media without a face-to-face meeting, directly, then by switching the sale and purchase transaction process, the risk of legal problems is increasing, for example, the risk of fraud, default, oversight or misdirection in online buying and selling transactions.

Based on the provisions of Law Number 11 of 2008 which was amended to become Law Number 19 of 2016 concerning Information and Electronic Transactions, in law enforcement of criminal acts of fraud related to ITE and online networks, there are differences in the procedural law regarding the use of articles and in the stages of law enforcement.

In its development related to law enforcement for perpetrators of fraud by using online media facilities in Indonesia, it is very appropriate in its enforcement.

Investigations into computer crimes or especially through online media are very unique and special. This is due to the proof system using digital besides having to bring in experts and experts.

Article 43 paragraph 2 of the ITE Law regulates that investigations in the field of information technology and electronic transactions as described in paragraph 1 are carried out with due regard to protection of privacy, confidentiality, smooth running of public services, data integrity or data integrity in accordance with statutory provisions.

Considering that cybercrime cases have a special character, both the character of the crime and the perpetrators, so that the investigation can run efficiently and effectively, cooperation can be carried out in the investigation as stipulated in Articles 20 and 21 of Perkap No. 14 of 2012.

In order to minimize criminal acts or crimes within the scope of ITE and cyber, the establishment of a special cyber unit has a much needed role. This is in accordance with the provisions of Article 12 of Perkap No. 14 of 2012 concerning the Regulation of the Head of the Indonesian National Police which states regarding investigations by tracking user accounts for online fraud crimes. The formation of a special cyber unit turns out to be in fact still not able to solve the problem, there are still many cases that come in inversely proportional to cases that can be resolved up to the complete P21 file until the court hearing.

In connection with the process of examining digital evidence both during investigations and examinations in court, it is necessary to have adequate capabilities from law enforcement. In handling electronic data, special steps are needed so that the digital evidence does not change. At the filing stage, investigators in fraud cases using social media facilities will first include Article 45 of the ITE Law in conjunction with Article 28 paragraph 1 of the ITE Law before including Article 378 of the Criminal Code regarding fraud.

Cases of fraud by using social media facilities are often public prosecutors in carrying out or compiling their charges using alternative indictments. This is because so that the perpetrator cannot be separated from the mistakes he has made. Alternative indictments are composed of several layers that exclude each other so that the perpetrators are entangled with their indictments. Usually, public prosecutors in compiling alternative indictments in fraud cases using social media facilities first use Article 45 of the ITE Law in conjunction with Article 28 paragraph 1 of the ITE Law or Article 378 of the Criminal Code in conjunction with Article 55 of the Criminal Code regarding fraud. Based on this, the examination process is continued in accordance with the applicable procedural law.

The stage of examining evidence at trial in the ITE case is a crucial stage, where the public prosecutor must prepare evidence that can support the charges that have been made. In contrast to fraud cases in general, fraud using technology such as this case must also attach electronic evidence related to fraud carried out on social media by the perpetrator, whether it is usually in the form of screenshots of selling goods through the perpetrator's social media, or results of evidence of a transfer of funds if it has been transfer process occurs. The panel of judges during the examination must first examine the elements in the article on the ITE Law being charged and must present an ITE expert to obtain sufficient information so that there is no mistake in imposing and using the article in the decision.

An investigation was carried out to obtain deeper information regarding fraud cases using social media. The summons of the parties is then carried out to obtain information through the stages of examination by police investigators. Examination is intended with the aim of seeing and analyzing whether the actions of the perpetrators of fraud by using social media facilities are appropriate and fulfill all the elements contained in the formulation of laws or rules that have been stipulated. The first thing police investigators did was to analyze whether the actions of the perpetrators of fraud fulfilled the elements in Article 28 paragraph 1 of the ITE Law.

If the elements fulfill, then the investigator will carry out the filing which will later be submitted to the public prosecutor to be used as an indictment in the trial. If the elements in Article 28 paragraph 1 of the ITE Law are not fulfilled then the investigator will then look at and analyze related to Article 378 of the Criminal Code regarding fraud. The examination process is carried out in order to ensnare the perpetrator so that he cannot be separated from the responsibility for the actions he has committed. Other information obtained during the examination by investigators will be used as goods and evidence which will later be shown in court proceedings. Fraud cases using social media are usually in addition to social media accounts which are used as electronic evidence, the results of screenshots of account screens and also the results of the fund transfer transaction process are then used as strong evidence as in Article 5 paragraph 1 of the ITE Law which states that electronic information and/or Electronic documents are valid legal evidence tools.

An indictment in which the use of criminal articles includes two or more different articles. Fraud cases using online buying and selling facilities are generally subject to punishment under Article 45 paragraph 3 of the ITE Law in conjunction with Article 28 paragraph 1 of the ITE Law as the first indictment or Article 55 paragraph 1 of the Criminal Code in conjunction with Article 378 of the Criminal Code as the second indictment. The use of this article makes the suspect subject to multiple articles where the prison sentence will be different from the use of ordinary articles.

Law enforcement against perpetrators of online fraud is subject to Article 378 of the Criminal Code which carries a maximum prison sentence of four years. However, because in Article 378 of the Criminal Code the punishment is too light, the police also use Article 28 paragraph (1) and Article 45 paragraph (2). Regarding criminal acts of online fraud, even though the ITE Law and its Amendments do not specifically regulate criminal acts of fraud, related to the emergence of consumer losses in electronic transactions there is a provision in Article 28 paragraph (1) of the ITE Law jo. Article 45 A paragraph (1) Law 19/2016. So it can be concluded that perpetrators of fraud can be charged with Article 378 of the Criminal Code, but can also be charged with Article 28 paragraph (1) of the ITE Law and its amendments if the fraud is carried out online.

From the description above, the authors draw the conclusion that to anticipate, optimize or suppress the occurrence of legal issues that often occur in online buying and selling, especially the problem of fraud, businesses and consumers must comply with the rules of the ITE Law, especially those contained in Article 45 paragraph (2) PP No. 71 of 2019, in particular, must pay attention to good faith in online buying and selling transactions and the principle of prudence, so that online buying and selling agreements are not prone to fraud. The issue of good faith must be considered by the parties in buying and selling online because if one of the parties does not have good faith, it will result in legal consequences, which are prone to default or fraud.

As is known, the arrangements regarding electronic transactions regulated in Law no. 11 of 2008 concerning Information and Electronic Transactions and Law no. 19 of 2016 concerning Amendments to Law no. 11 of 2008 concerning Electronic Information and Transactions as the main basis for online buying and selling arrangements and Government Regulation Number 71 of 2019 concerning Electronic System and Transaction Operations. .

## 2. Factors Behind the Crime of Fraud in Online Buying and Selling Transactions in Indonesia.

With the promulgation of Law Number 11 of 2008 Concerning Electronic Information and Transactions (UU ITE), namely the first Law in the field of Information Technology and Electronic Transactions as a product of legislation that is urgently needed and has become a pioneer laying the basis for regulation in the field of utilization of Information Technology and Electronic Transactions.

Law Number 11 of 2008 concerning Information and Electronic Transactions was later revised and updated to become Law Number 19 of 2016 concerning Information and Electronic Transactions.

Law No. 19 of 20016 concerning Electronic Information and Transactions is included in Article 28 Paragraph 1: "Every person intentionally and without right spreads false and misleading news that results in consumer losses in electronic transactions." And as for the provisions for criminal sanctions for online business fraud, it is contained in Article 45A paragraph (1) which reads "Every person intentionally and without rights distributes and/or transmits and/or makes Electronic Information and/or Electronic Documents accessible that have the content as intended in Article 28 paragraph (1) shall be punished with imprisonment for a maximum of 6 (six) years and/or a maximum fine of Rp. 1,000,000,000.00 (one billion rupiah)."

Provisions regarding online business fraud which can be regulated in provisions through the Criminal Code (KUHP) are included in article 378 paragraph 1, namely "Anyone who with the intention to unlawfully benefit himself or others by using a false name or dignity (hoedanigheid ) fraudulent, by means of deception, or a series of lies, to induce another person to hand over something to him, or to give him a debt or write off a receivable, is threatened, for fraud, with a maximum imprisonment of four years.

Criminal law enforcement within the framework of the criminal justice system in Indonesia, which until now is still based on Law Number 8 of 1981 concerning Criminal Procedure Code (KUHP), is felt to have not represented various interests. For example, regarding the interests of victims in the criminal justice process as represented by the Public Prosecutor, there are still striking differences with the interests of the perpetrators of criminal acts. Therefore, the goal to be achieved in the criminal justice system as stated by Mardjono Reksodipoetro, namely, among other things, is to resolve criminal cases that have occurred so that the community is satisfied that justice has been upheld, it is unlikely that this will be carried out properly.

Taking the notion of law enforcement according to Satjipto Rahardjo, that law enforcement is a process to make legal wishes come true. While the wishes of the law itself are the thoughts of the legislature which are formulated in legal regulations, 85 then the process of law enforcement by law enforcement officials here is closely related to existing legal regulations. Therefore, according to Satjipto Rahardjo, the formulation of the thoughts of lawmakers as outlined in legal regulations will also determine how law enforcement is carried out.

With this, current technological advances are a double-edged sword, because in addition to contributing to increasing prosperity, progress and civilization. However, it can also increase the crime rate. Cases of acts of fraud are increasing in number every year and the modes used are also varied to the point of creating unrest for the community. How not, the modes that are widely used especially in terms of buying and selling through social media facilities or by means of online media, where one of them is social media is a place for everyone to interact with other people in today's technological era.

The Criminal Code itself in article 378 enforces that someone who commits a crime of fraud is threatened with criminal sanctions. Even so, it is still felt to be ineffective in enforcing the offenders, because in criminal

law enforcement it is not only enough to regulate an act in a law, but also requires legal officials as executors of statutory provisions and institutions authorized to deal with a crime such as the police, prosecutors, courts, fraud cases have recently been growing and often occur even though this crime has been regulated in the Criminal Code, one type of crime in the cyber field is fraud in the form of buying and selling/online business on the internet. This type of fraud is happening more and more, partly due to the large number of people who want to fulfill their needs in an easy way and save time and money.

Fraud can be done in various ways, ranging from simple ways to complex ways. Cyber activities are virtual but can be categorized as real legal actions and actions. This fraud is a cyber crime that takes advantage of weaknesses in terms of security and habits when surfing the internet. The crime of fraud using the internet is included in the Illegal Content crime group in the study of information technology abuse in the form of Computer Related Fraud, Illegal Content is a crime by entering data or information into the internet about something that is incorrect, unethical, and can be considered unlawful or disturbing public order. And this Computer Related Fraud is interpreted as fraud or is a fraud that is made to gain personal gain or to harm other people. For example, the spread of fake and misleading news via the internet. We often find this happening in the cyber world in the process of buying and selling online. Where the buyer is often harmed by the acts of fraudulent sellers who do not carry out their obligations as sellers.

Social media facilities as targets for perpetrators to carry out their actions are not without reason, the law has not yet accommodated and has left no evidence in the process. If it is related to criminology, we can see the extent to which the fraudulent crime was committed and know all aspects and causes of a criminal act being committed. In this regard, the author has conducted interviews with various sources who are competent in their fields to discuss the factors behind the occurrence of criminal acts of fraud through these social media facilities.

Whereas there are several factors that cause a person to commit a criminal act of buying and selling fraud by using internet media facilities or also through social media in particular, including:

1. Culture culture;
2. Driving factors; And
3. Economy.

Cultural factors are the main factor in the occurrence of acts of fraud, especially through social media facilities in society. In Indonesia, there is often a shift in old culture into a culture that is considered new or modern by society. This cultural shift has an impact on the misuse of knowledge regardless of who is responsible for doing it.

Culture is not just a collection of behaviors and concepts of thought that are open to each other but are interpreted as a special category so that in it there are social values that are in sync with laws or norms, attitudes that influence the running of the law, including respect or disrespect for the law, and many others.

Legal culture can show how the attitudes of people's behavior towards legal issues or legal events that occur and are carried into society. Criminal acts of fraud using social media facilities are classified as new types of fraud crimes that are happening at this time. This crime is an example that crime or criminal acts can evolve or develop following more modern cultural changes.

With a lack of public legal awareness Legal awareness is awareness of what we should or shouldn't do with regard to the rules or laws that apply in society. Currently, public legal awareness is still considered to be lacking in relation to cybercrime activities. This is due to a lack of understanding regarding cybercrime, both its actions and the effects it causes. Many people are less or not aware of the actions they are taking related to activities in cyberspace. Starting from the rampant acts of defamation to acts of hijacking other people's social accounts. These small acts are considered normal and commonplace in society, and even tend to be used as a joke.

Through an understanding of cybercrime, society plays an important role in efforts to overcome cybercrime. Without understanding, cybercrime perpetrators will run rampant because people don't know what they are really doing, so in the end they are deceived, their accounts are compromised and various other losses.

Security Cybercrime perpetrators will certainly feel safe when carrying out their actions, this is none other than because the media used in carrying out crimes is in the form of internet access which is commonly used anywhere, be it closed or open places. The lack of a security system from the internet makes anyone free to express themselves in cyberspace without the need for restrictions, thus encouraging the growth of cyber crime.

In this study, the authors conclude that there are several factors behind the criminal act of fraud in online buying and selling transactions, one of which is the economic factor being the main trigger for a crime committed by someone. Increasing needs, a consumptive lifestyle and the skyrocketing cost of living, are then used as an excuse or make economic factors the reason for everyone to do something that is beyond the reasonable logic of normal good thinking.

#### IV. CONCLUSION

a. Legal provisions against perpetrators of criminal acts of fraud in online buying and selling transactions. As is known, the arrangements regarding electronic transactions regulated in Law no. 11 of 2008 concerning Information and Electronic Transactions and Law no. 19 of 2016 concerning Amendments to Law no. 11 of 2008 concerning Electronic Information and Transactions as the main basis for online buying and selling arrangements and Government Regulation Number 71 of 2019 concerning Electronic System and Transaction Operations. . Because law enforcers have not been able to properly implement these legal arrangements to anticipate, optimize or suppress the occurrence of legal problems that often occur in online buying and selling, namely mainly the problem of fraud in online buying and selling which is still prone to fraud. Law enforcement against perpetrators of online fraud is subject to Article 378 of the Criminal Code which carries a maximum prison sentence of four years. However, because in Article 378 of the Criminal Code the punishment is too light, the police also use Article 28 paragraph (1) and Article 45 paragraph (2). Regarding criminal acts of online fraud, even though the ITE Law and its Amendments do not specifically regulate criminal acts of fraud, related to the emergence of consumer losses in electronic transactions there is a provision in Article 28 paragraph (1) of the ITE Law jo. Article 45 A paragraph (1) Law 19/2016. So it can be concluded that perpetrators of fraud can be charged with Article 378 of the Criminal Code, but can also be charged with Article 28 paragraph (1) of the ITE Law and its amendments if the fraud is carried out online.

b. There are several factors behind the criminal act of fraud in online buying and selling transactions, one of which is the economic factor which is the main trigger for a crime committed by someone. Increasing needs, a consumptive lifestyle and skyrocketing costs of living, are then used as an excuse or make economic factors the reason for everyone to do something that is beyond the reasonable logic of normal good thinking.

#### REFERENCES

- [1] Aruan Sakidjo dan Bambang Poernomo, Hukum Pidana : Dasar Aturan Umum Hukum Pidana Kodifikasi, Jakarta: Ghalia Indonesia, 1988
- [2] Arief, Barda Nawawi, Pembaharuan Hukum Pidana Dalam Perspektif Kajian Perbandingan, Bandung: Citra Aditya;2005.
- [3] Arief, Barda Nawawi, Beberapa Aspek Kebijakan Penegakan dan Pengembangan Hukum Pidana, PT Citra Aditya Bakti : Bandung, 1998.
- [4] Bambang Waluyo, Pidana dan Pemidanaan, Sinar Grafika, Jakarta, 2008.
- [5] Budi Suhariyanto, Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan Dan Celah Hukumnya, Jakarta: Rajawali Pers, 2012.
- [6] Djoko Prakoso, Bambang Riyadilani, Amir Muhsin, Kejahatan-kejahatan yang Merugikan dan Membahayakan Negara, Bina Asara, Jakarta 1987.
- [7] Departemen Pendidikan Nasional dan Balai Pustaka, Kamus Besar Bahasa Indonesia, Jakarta: Balai Pustaka, 2001
- [8] Hamzah, Andi. Asas-asas Penting dalam Hukum Acara Pidana, Surabaya, FH Universitas 2005.
- [9] Hari Sasangka, Lili Rosita, Hukum Pembuktian dalam Perkara Pidana,Bandung:Mandar Maju, 2003
- [10] Lamintang, P. A. F. dan Samosir, C. D., SH, Hukum Pidana di Indonesia, PT. Eresco, Jakarta-Bandung,1997.
- [11] Mardjono Reksodipoetro, Bahan Bacaan Wajib Matakuliah Sistim Peradilan Pidana, Pusat Dokumentasi Hukum UI, Jakarta, selanjutnya disebut Marjono Reksodipoetro II, 1983.
- [12] Moeljanto, Kitab Undang-Undang Hukum Pidana, Bumi Aksara,Jakarta,2005.
- [13] Mahayani, Dimitri, 2000, Menjemput Masa Depan, Futuristik dan Rekayasa Masyarakat Menuju Era Global, Bandung: Rosda;
- [14] Makarim, Edmon. Kompilasi Hukum Telematika. Jakarta. Raja Grafindo Persada. 2000.
- [15] Maskun, Kejahatan Siber (Cyber Crime) Suatu Pengantar, Jakarta: Kencana 2013.
- [16] Moeljatno, KUHP (Kitab Undang-undang Hukum Pidana),Jakarta: Bumi Aksara, 2007.
- [17] Muladi dan Barda Nawawi Arief, Teori-teori dan Kebijakan Pidana, Bandung: Alumni, 20005.
- [18] Muladi, Lembaga Pidana Bersyarat, Bandung: Alumni, 2008.
- [19] Romli Atmasasmita, Peradilan Pidana, Perspektif Eksistensialisme dan Abolisionisme, Binacipta, Bandung,1996.
- [20] Rusmana, Agus. Penipuan Dalam Interaksi Melalui Media Sosial, Vol.3 No.2, Desember 2015.



- [21] Sudarto, Hukum dan Hukum Pidana, Alumni, Bandung,1986.
- [22] Soejono Dirjosisworo, Sosio Kriminologi. Amalan Ilmu-Ilmu Sosial Dalam Studi Kejahatan. Seminar Baru, Bandung, 2007.
- [23] Setiawan, Deris. Sistem Keamanan Komputer, Jakarta: PT.Elex Media Komputindo, 2005.
- [24] Sitompul, Josua. Cyberspace Cybercrime Cyberlaw Tinjauan Aspek Huku Pidana, Jakarta: Tatanusa, 2012.
- [25] Sodiki, Achmad. Kejahatan Mayantara,Bandung: PT.Refika Aditama, 2010.
- [26] Soekanto, Soerjono. Faktor-faktor yang Mempengaruhi Penegakan Hukum,Jakarta, Rajawali,1983.
- [27] Tubagus Ronny Rahman Nitibaskara, Ketika Kejahatan Berdaulat: Sebuah Pendekatan Kriminologi, Hukum dan Sosiologi, Peradaban, Jakarta 2001.