Solving Cyber Crime in Online Buying and Selling in Cirebon City in Review of ITE Law and Islamic Law

[1]Didi Sukardi, [2]Farha Bayu Nugraha, [3]Ubaidillah, [4]Abdul Fatakh, [5]Leliya, [6]Muhammad Fadel Arrizky
Universitas Islam Negeri Siber Syekh Nurjati Cirebon
[1]didisukardimubarok@gmail.com, [2]bayufarha@gmail.com, [3]firlyubaidillah@gmail.com,
[4]abdulfatakh14@gmail.com, [5]leliya12@yahoo.co.id, [6]fadelarrizky18@gmail.com

Abstract

In the cybercrime crime of online buying and selling fraud, there is a case, one of which occurred in Cirebon City, so the police must solve the online buying and selling fraud cybercrime case. However, in practice, the police experienced several obstacles in its resolution. The method in this study is descriptive qualitative research with a case study approach. The data collection techniques carried out are observation, interviews and documentation. From the results of this study, it is known that the police from the Cirebon City Police, in handling criminal cases of online buying and selling fraud, carried out an investigation process by investigators. The investigation is carried out by checking the accounts of the perpetrators of online buying and selling scams to find evidence and track down the perpetrators. However, the police experienced several obstacles, from the limited special tools in uncovering criminal acts of online buying and selling fraud to the difficulty of finding evidence and tracking the perpetrators. Hence, the Cirebon City Police became less effective in solving online buying and selling fraud crimes.

Keywords: Cybercrime; Scams; E-commerce.

Abstrak

Dalam kejahatan cybercrime penipuan jual beli online terdapat sebuah kasus yang salah satunya terjadi di Kota Cirebon, sehingga pihak kepolisian harus menyelesaikan kasus cybercrime penipuan jual beli online tersebut. Namun dalam praktiknya, polisi mengalami beberapa kendala dalam penyelesaiannya. Metode dalam penelitian ini adalah penelitian deskriptif kualitatif dengan pendekatan studi kasus. Teknik pengumpulan data yang dilakukan adalah observasi, wawancara dan dokumentasi. Dari hasil penelitian tersebut diketahui bahwa pihak kepolisian Polres Cirebon Kota dalam menangani kasus pidana penipuan jual beli online telah melakukan proses penyidikan oleh penyidik. Penyidikan dilakukan dengan memeriksa rekening para pelaku penipuan jual beli online untuk mencari bukti dan melacak pelakunya. Namun polisi mengalami beberapa kendala, mulai dari terbatasnya alat khusus dalam mengungkap tindak pidana penipuan jual beli online hingga sulitnya menemukan bukti dan melacak pelakunya. Oleh karena itu, Polres Cirebon Kota menjadi kurang efektif dalam menuntaskan kejahatan penipuan jual beli online.

Kata Kunci: *Cybercrime; Penipuan; Perdagangan elektronik.*

.

INTRODUCTION

Information and communication technology is increasingly developing rapidly which provides many conveniences for mankind, especially since the discovery of the internet in 1969 and experiencing a boom a quarter of a century later. The Internet has had a far greater impact on computer-based communications than any other development and has encouraged business transactions via the Internet. World-scale companies are also increasingly utilizing Internet facilities. The development of the Internet is increasing day by day both technology and its use, bringing many impacts both positive and negative (Arifah 2011).

Business transactions via the Internet are one of the positive impacts arising from the development of technology. Business transaction activities via the internet also known as Electronic Commerce (E-commerce) is an activity that is widely carried out by everyone because electronic buying and selling transactions can streamline and streamline time so that someone can make buying and selling transactions with everyone anywhere and anytime (Arief and Sutrisni, 2014). The benefits of information and communication technology in addition to having a positive impact are also realized to provide opportunities to be used as a means of committing new crimes in cybercrime (Aryyaguna, 2017).

Cybercrime is a criminal act committed using computer technology as the main crime tool. Cybercrime is a crime that utilizes the development of computer technology, especially the internet. Cybercrime is defined as unlawful acts that utilize computer technology based on the sophistication of internet technology developments (Jannah and Naufal, 2012). In internet media, crimes that often occur are fraud in the name of buying and selling businesses using internet media that offer a variety of sales products that are sold below the average price. The scam uses a modus operandi in the form of selling various kinds of goods that are tempting for potential buyers because the price is so cheap and far from the original price. In the end, after the money is delivered, the ordered items are not received. In order to gain profit and enrich themselves, the perpetrators violate the rules and norms of the applicable law. Online businesses does make it easier for fraudsters to carry out their actions (Sumenge, 2013).

These negative impacts must be anticipated and overcome by laws related to the use of information and communication technology, namely Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law). The ITE Law is a comprehensive thought from the State with the political will to pay attention to and provide legal protection for users of information technology. Of course, this legal protection is not only to users of information technology that is used positively but how this law can prevent and reveal all forms of crime, one of which is fraud through electronic transactions (Sumadi, 2015). In addition, in Islamic trade law, sellers and buyers must be honest and must not deceive each other. Sellers and buyers must have the principle of not harming or deceiving others. Islam strongly condemns all forms of fraud in buying and selling transactions.

In the crime of buying and selling online, there is a case, one of which occurred in the city of Cirebon. One of the victims in the online buying and selling crime is named Galuh Agus Ferdiyanto who is a resident on Jalan Kesunean Tengah, RT 06 RW 08, Kasepuhan Village, Lemahwungkuk District, Cirebon City. The incident began when the victim intended to open a business by selling shoes so the victim was interested in buying shoes through one of the Instagram accounts, then the victim began ordering as many as 17 pairs of shoes to the owner of an Instagram account called BAL. IMPORT. After ordering the shoes the next day the victim made a transfer to the perpetrator's account number and the victim waited several days to

receive the ordered items, but after a long time of waiting the ordered items did not arrive and the victim tried to contact the perpetrator's number. When contacted, the perpetrator reasoned that he was subject to customs and the perpetrator also asked the victim to transfer money worth Rp. 1,000,000 again, with a suspicious feeling the victim refused it and suddenly the victim's WhatsApp number was blocked by the perpetrator, then the victim felt upset because he had transacted with the fraudster (Radarcirebon, 2019).

In relation to this case, the police in Cirebon City have an obligation to overcome to solve problems that occur among the community, so that Cybercrime cases using electronic media can be minimized, especially in Cybercrime cases that occur in online buying and selling such as online fraud. Based on the background of the above problem, the author is interested in conducting research on 1) How is the implementation of solving Cybercrime crimes in online buying and selling in Cirebon City? 2) What are the obstacles in solving Cybercrime in buying and selling online in Cirebon City? 3) How is the implementation of solving Cybercrime crimes in online buying and selling in Cirebon City viewed from Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE) and Islamic Law?

LITERATURE REVIEW

Research on cybercrime in buying and selling online is not new. However, it seems rare to find research that specifically discusses the implementation of solving Cybercrime crimes in online buying and selling in Cirebon City from the perspective of Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE) and Islamic Law. Here are some documented works related to the problems studied, namely, research conducted by Gahfuur Kurniawan Pangku Alam. This study illustrates that e-commerce-based fraud crimes are in principle the same as fraud in conventional ways, but the difference lies in the evidence or means of action, namely using electronic systems (computers, internet, telecommunication devices) (Alam, 2020).

Second, this research was conducted by Siti Aisah on "Law Enforcement of Online Fraud in Sleman Regency Yogyakarta Integratively". This study aims to determine the role of the Sleman Police in revealing the truth of the factors causing online fraud. As well as how to enforce and prevent online fraud crimes that occur in Sleman district (Aisah, 2019).

Third, this research was conducted by Satria Nur Fauzi and Lushiana Primasari. This study analyzes that there are three forms of fraud, namely: discount price fraud on National Online Shopping Day in 2015, fraud of goods not according to orders, and fraud pretending to sell goods. The laws and regulations that can be applied in this fraud case are Article 378 of the Criminal Code (KUHP), Article 28 paragraph 1 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions and Article 9 paragraph 1 of Law Number 8 of 1999 concerning Consumer Protection (Fauzi and Primasari 2018).

Of the three research topics described above, it turns out that there has been no research that specifically discusses the implementation of solving Cybercrime crimes in online buying and selling in Cirebon City Perspective of Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE) and Islamic Law. So, this study is different from previous studies. Therefore, it can be expected that this study can be a reference regarding the implementation of solving cybercrime crimes in online buying and selling in Cirebon City: Perspectives of Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE) and Islamic Law.

RESEARCH METHODS

In this study, researchers used descriptive qualitative research in the form of research with a case study approach. In this study, researchers will interpret "Implementation of Cybercrime Settlement in Online Buying and Selling in Cirebon City: Perspective of Law Number 11 of 2008 and Islamic Law" directly to the Cirebon City Police Police, by observation, review, describe, analyze data from research subjects in the field.

The source of data needed in this study is as primary data based on the results of in-depth interviews with the police at the Cirebon City Police Station, direct observation and documentation. Meanwhile, secondary data sources used in this study were obtained from books, journals and other data sources that have something to do with the discussion of the title of this study, as reference material or reference material. In this study, the observation made was by making direct observations to the Cirebon City Police to obtain valid data.

Second, an interview is a conversation directed at a particular issue and is an oral questioning process in which two or more people are physically confronted. Interviews are conducted to obtain as much data or information as possible and as clearly as possible to the research subject (Gunawan, 2019). The interview conducted in this study was an interview with the Cirebon City Police with no structure, where in this method it allows questions to take place flexibly, the direction of questions is more open, remains focused, so that rich information is obtained and the conversation is not rigid.

Third, documentation is a document that refers to materials such as photography, video, film, memos, letters, diaries, clinical case recordings and the like that can be used as supplement information as part of a case study whose main source of data is participant observation or interviews (Ahmadi, 2014). The documentation used in the research here is small notes, books, and pictures found by researchers at the Cirebon City Police Station.

In the process of scrutinizing the aforementioned study, researchers employ analytical descriptive analysis methods, a strategic approach aimed at acquiring precise and targeted data. This methodological choice holds paramount importance as it is instrumental in extracting information that carries substantive implications for the overall essence of the study. By delving into the intricacies of analytical descriptive analysis, the researchers meticulously extract specific data points, thereby ensuring a comprehensive and nuanced understanding of the subject matter at hand. This meticulous method not only contributes to the depth of the analysis but also serves as a pivotal factor in shaping the substantive content and outcomes of the study, thus underscoring its significance in the broader research framework.

THEORETICAL FRAMEWORK

Definition of Criminal Art

The definition of criminal acts in the Criminal Code (KUHP) is known as Strafbaar feit and the literature on criminal law often uses the term delict, while lawmakers formulate a law using the term criminal event or criminal act or criminal act (Wahyuni, 2017). The definition of the word strafbaar feit itself consists of three words, namely straf (criminal and legal), baar (can and may), and feit (actions, events, violations, and deeds) (Ilyas, 2012). Simons formulated strafbaar feit as an unlawful act that has been done intentionally by someone who can be held accountable for his actions and which by law has been declared a punishable act (Lamintang, 1997). Thus it can be concluded that criminal acts are prohibited by a rule of law, the prohibition of which is accompanied by threats (sanctions)

In the form of certain penalties for those who violate the prohibition.

Elements of a Criminal Act

In Criminal Law there are various elements to determine the existence of criminal acts, so they are generally formulated in criminal laws and regulations regarding prohibited acts and accompanied by sanctions. As for the elements of criminal acts, there are 5 (five) elements of criminal acts, namely: Behavior and consequences; certain things or circumstances that accompany the act; because these additional circumstances are called criminal aggravating elements; usually in the presence of certain deeds; and unlawful elements in the formulation of offenses (Moeljatno, 2015). Thus, the act of criminal acts must be committed with an element of guilt, because with this element of error can be related to the consequences of the act or to the circumstances in which it was committed.

Understanding Cybercrime

The term cybercrime currently refers to an act of crime related to cyberspace (cyberspace) and computers based on the sophistication of the development of internet technology as the main medium for committing crimes. In general, what is meant by cybercrime is an act without permission and against the law by using a computer as the main facility or target to commit crimes, with or without causing changes and or damage to the computer system used (Mansur 2009). In other words, cybercrime is an act that violates the law or a crime that utilizes the development of computer technology based on the sophistication and development of internet technology. Thus it can be concluded that cybercrime is a crime that violates the law by using computer technology (internet) as a means or tool in committing crimes, either to obtain profits or by harming other parties.

Legal Regulation of Cybercrime in Indonesia

Cybercrime is all criminal acts that use means or with the help of electronic systems. That means all conventional crimes in the Criminal Code (KUHP) as long as they use the assistance or means of electronic systems such as murder, or trafficking in persons, can be included in the category of cybercrime in a broad sense. Likewise, criminal acts in Law Number 3 of 2011 concerning Fund Transfer (Law 3/2011), as well as banking crimes and money laundering crimes in Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering (TPPU Law).

The regulation of cybercrime is also regulated in Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) as amended by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (Law 19/2016), the ITE Law does not provide a definition of cybercrimes but divides it into several groupings, that is:

1. Criminal acts related to illegal activities, namely, *Distribution or dissemination, transmission, and accessibility of illegal content, consisting of*:
    a. Decency (Article 27 paragraph (1) of the ITE Law);
    b. Gambling (Article 27 paragraph (2) of the ITE Law);
    c. Insult and/or defamation (Article 27 paragraph (3) of the ITE Law);
    d. Fake news that misleads and harms consumers (Article 28 paragraph (1) of the ITE Law);
    e. Causing hatred based on SARA (Article 28 paragraph (2) of the ITE Law);
        1) In any way make illegal access (Article 30 of the ITE Law);
        2) Illegal interception or interception of electronic

information or documents and electronic systems (Article 31 Law 19/2016).

2. Sending information containing threats of violence or intimidation aimed at personally (Article 29 of the ITE Law
3. Criminal acts related to interference, namely:
   a. Interference with Electronic Information or Documents (Article 32 of the ITE Law);
   b. Interference with Electronic Systems (Article 33 of the ITE Law)
4. Criminal acts facilitating prohibited acts (Article 34 of the ITE Law);
5. The criminal act of falsifying information or electronic documents (Article 35 of the ITE Law);
6. Additional criminal acts (accessory Article 36 of the ITE Law);
7. Objections to criminal threats (Article 55 of the ITE Law).

Cybercrime in the Perspective of Islamic Criminal Law

Terms such as; al-jarimah, aljinayah, al-janhah, or al-mukhalafah. The four terms have something in common, namely as an act against the law. And the difference is the classification of jurists on these deeds. This is when associated with cybercrime, then Cybercrime is part of the same object as the network, it's just that Cybercrime is a criminal act involving electronic media and the like, while the network is carried out as in conventional law.

Cybercrime certainly has its relevance to jarimah because in a country that applies Islamic law, of course, Cybercrime becomes the object of jarimah itself. It is said that the source of Islamic criminal law is a clear source of law because it comes from the Qur'an, if terminology is not affirmed in the Qur'an and Sunnah this cyber crime can be investigated through the qiyas method with cases similar or almost the same as previous cases that have been thoroughly explained in jinayah jurisprudence (Gunawan, 2018).

Cybercrime is a form of crime that appears in today's modern era. Thus, the crime of cybercrime according to the analysis of Islamic law (jinayat) can be punished with ta'zir. As for shari'i, ta'zir is intended as a sanction imposed on the basis of despotism, because it expressly does not include crimes contained in the Quran and Hadith, as had, Qisas, or kafarat (Jannah and Naufal, 2012).

Understanding Online Buying and Selling (E-Commerce)

Buying and selling online commonly referred to as e-commerce in electronic language means electronic science and all things related to the world of electronics and technology, while e-commerce is trade or commerce (Hediana and Aly 2016).

E-commerce is a process of buying and selling products electronically by consumers and from company to company with computers as intermediaries for business transactions. Media that can be used in e-commerce activities is the World Wide Web internet (Maulana, Susilo and Riyad 2015).

Types of Crimes in E-Commerce

Crimes that occur in online buying and selling activities (e-commerce) include the following:

1. *Online fraud*: The characteristics are that the price of products that are in great demand is very low, sellers do not provide phone numbers, there is no response to inquiries via e-mail, and promising products are not available. The worst risk is that the winner of the auction who has sent a check or money or paid via credit card does not get the product, or obtains a product that is not what is desired or advertised.
2. *Online shopping marketing scams*: Its characteristics are profiteering from recruiting members and selling products fictitiously. The risk is that as many as 98% of investors fail or lose.

3. *Credit card fraud*: The characteristic is that there is a mysterious charge on the credit card bill for internet products/services that have never been ordered by the credit card owner. The risk is that the victim can take a long time to pay off.

Online Buying and Selling (E-Commerce) in Islam

In the Islamic view, e-commerce transactions actually have almost the same definition as conventional transactions, it's just that there are some rules and obligations that must be in accordance with Islamic principles and allowed in Islam, as mentioned in Q.S. Al-Jumu'ah 62:10.

فَإِذَا قُضِيَتِ ٱلصَّلَوٰةُ فَٱنتَشِرُواْ فِى ٱلْأَرْضِ وَٱبْتَغُواْ مِن فَضْلِ ٱللَّهِ وَٱذْكُرُواْ ٱللَّهَ كَثِيرًا لَّعَلَّكُمْ تُفْلِحُون

It means: "When the prayer has been performed, you will be scattered on the earth; seek the grace of God and remember God much so that you may be fortunate"

This verse explains that Allah allows His servants to carry out any activity as long as it does not contradict Islamic principles, including trade transactions or buying and selling. However, in making buying and selling transactions a Muslim must still uphold faith and fear Allah in all forms of trade.

Transaction (contract) is an important element in an engagement. In Islam, the issue of transactions is very firm in its application, and this proves that the existence of transactions should not be ruled out in every area of human life (Muslims), because of the importance of transactions in an agreement. An as-salam transaction is a form of transaction with a cash/synchronous payment system but the delivery of goods is suspended (Santoso, 2016).

From this description, e-commerce tends to have similarities with bai' as-salam when viewed from payments that are synchronized and delivery or delivery of goods that are deferred. In e-commerce transactions, after an agreement occurs between the seller and the buyer, the buyer will pay the agreed nominal goods. If the payment has proven to be paid off, then the seller then delivers the goods desired by the buyer.

It can be concluded that transactions through cyberspace or e-commerce are allowed according to Islam as long as they do not contain elements that can damage it such as tyranny, fraud, fraud, containing usury, things that are forbidden, and the like.

RESULT AND DISCUSSION

Implementation of Cybercrime Settlement in Online Buying and Selling in Cirebon City

Advances in information technology and electronic transactions today have provided convenience and benefits that are widely felt for mankind. The development of technology has had a positive impact that can be utilized in people's social lives and has entered various factors of life. However, in addition to having a positive impact, it is also realized to have a negative impact, namely a crime committed in cybercrime so it harms the community a lot.

E-commerce today has brought various changes to the business world in Indonesia, where e-commerce is in great demand and utilized for the needs of the community to can facilitate their daily lives. Although e-commerce has provided many conveniences and benefits for the community, in practice there are often crimes in the form of online fraud committed by irresponsible individuals by utilizing e-commerce. For example, cases of online fraud in buying and selling online through electronic media, for example:

Regarding the case of online buying and selling fraud through Instagram media, there is a case that occurred in Cirebon City reported in radarcirebon.com, one of the victims in the online buying and selling crime was named Galuh Agus Ferdiyanto who is a

resident on Jalan Kesunean Tengah, RT 06 RW 08, Kasepuhan Village, Lemahwungkuk District, Cirebon City. The incident began when the victim intended to open a business by selling shoes so that the victim was interested in buying shoes through one of the Instagram accounts, then the victim began ordering as many as 17 pairs of shoes from the owner of an Instagram account called BAL. IMPORT. After ordering the shoes the next day the victim made a transfer to the perpetrator's account number and the victim waited several days to receive the ordered items, but after a long time of waiting the ordered items did not arrive and the victim tried to contact the perpetrator's number. When contacted, the perpetrator reasoned that he was subject to customs excise tax and the perpetrators also asked victims to transfer money worth Rp. 1,000,000, with fraudsters. After that, the victim explained that initially, the victim was interested because of BAL's Instagram account. IMPORT already has more than 11 thousand followers or followers and the account also has many testimonials containing customer satisfaction (Radarcirebon, 2019).

Another example of online fraud in e-commerce through Instagram media, here is a confession from one of the victims (Agung 20 years old), where he wanted to buy goods in the form of JPX branded motorcycle helmets, before deciding to buy he made sure first by looking at the testimonials and proof of transfer uploaded, judging from the large number of followers on the sales account and with a fairly convincing appearance and evidence, he decided to buy the helmet. After making an offer and acceptance from the seller, he also transferred Rp.400,000 to the seller through the account number provided by the seller, but after a few days of waiting for the goods did not come and when he tried to contact through the seller's WhatsApp number, it turned out that the victim's number had been blocked by the seller, and the Instagram account changed its name with the aim of tricking the victim. The victim felt disappointed and very aggrieved, but he did not report this to the authorities (Agung, 2023).

Based on this case, the police at the Cirebon City Police Station have an important role in overcoming to solve problems that occur in the community, so that cybercrime cases using electronic media can be minimized, especially in cases of cybercrime that occur in online buying and selling such as online fraud. Regarding cybercrimes, the legal provisions used still refer to the Criminal Procedure Code and the Law on Electronic Information and Transactions (ITE Law).

The implementation of solving cybercrime crimes in online buying and selling, it is carried out with an investigation process by investigators in the police. The main role of the investigator is to find and collect evidence that with that evidence makes light of the criminal act that occurred and to find the suspect.

Investigation is the first stage carried out by investigators in the process of investigating criminal acts. Based on an interview with Mr. Rajasa Wahyu Abadi as an Investigator at the Cirebon City Police said, "The investigation conducted by the Cirebon City Police into the crime of online buying and selling fraud was carried out by the Police of the Certain Crime Unit (Tipidter)" (Abadi, 2023). Then continued, "In an investigation regarding online buying and selling fraud cases, there must be a complaint from the public first to the police then cyber patrols will be carried out through social media both on Facebook, Instagram, Twitter, and Tiktok by checking accounts suspected of committing online fraud to track down the perpetrators and find electronic evidence. But even by checking the accounts also at the Cirebon City Police Station many experience obstacles and difficulties, due to limited tools in finding evidence and tracking perpetrators and cases related to cybercrime, the handling is different from ordinary or conventional criminal cases" (Abadi, 2023).

Based on the explanation above, in investigations related to cases of cybercrime or online buying and selling fraud, strong evidence is needed to track down the perpetrators and look for electronic evidence. However, in doing so, the police at the Cirebon City Police Station experienced many obstacles and difficulties so they needed technological facilities and capabilities in the field of computers or cyber experts.

As stated by Mr. Rajasa Wahyu Abadi an Investigator at the Cirebon City Police that "The investigation carried out by the police does not know the boundaries of the area. Therefore, it is necessary to cooperate with other law enforcement officials or cyber units that are at least in the Polda. This is necessary to track down the perpetrators and collect electronic evidence so that the investigation process will continue even deeper by tracing the source of the electronic documents" (Abadi, 2023).

In practice, Mr. Rajasa Wahyu Abadi as an Investigator at the Cirebon City Police said that the steps taken in handling cybercrime cases are (Abadi, 2023).

1. Making a police report, then calling witnesses from the owner of the IP Address or Internet Service Provider (ISP)
2. Inspect the crime scene or locus delicti used by the perpetrator, then track, collect and confiscate existing electronic evidence such as mobile phones, hard drives, and others.
3. Conduct examinations of witnesses and experts who have expertise in the field of ITE or Cyber Unit.
4. Examination of suspects, who have previously been arrested and detained based on sufficient evidence or evidence.
5. Filing and application of criminal articles in accordance with the criminal act committed by the suspect.
6. Prepare a case report, that is, after all physical evidence has been collected and documented and interrogation has been carried out. The report contains investigation reports, electronic evidence documents, digital forensic expert reports, statements of witnesses, suspects, and experts, crime scene reports, and printouts of digital evidence.
7. Examination of the case file by the public prosecutor
8. Make a decision to sue if the case file is declared complete

Based on the description above, cybercrimes that use internet facilities to trap criminal offenders require strong evidence, in finding evidence, investigators will track the whereabouts of the perpetrators by tracing the perpetrator's IP Address based on IP Address logs stored on the website/homepage manager server that is used as a means for perpetrators to commit cybercrimes. Through IP Address can make it easier to find information and track digital traces. In addition, Mr. Rajasa Wahyu Abadi as an Investigator at the Cirebon City Police said "In tracking the perpetrators and searching for evidence can be done using IP Address, Mobile Number, Account Number and E-mail."

The proof system for cybercrime crimes is the main evidence tool that can be submitted directly into evidence in court, considering that technology-based cybercrime crimes certainly leave digital traces or electronic documents or printouts so that they can be used as main evidence and strong evidence (Jayantari and Sugama 2019).

For the perfection of the legal power of proof of electronic document evidence, judges need evidence other than electronic documents to be more convincing to determine the truth of a cybercrime and determine the culprit so that there is no mistake in making decisions, then the judge can ask for expert help by obtaining

information from cyber experts. In addition, the judge can also request additional evidence that is deemed necessary and strengthen the judge's opinion, the perfection of the proof has been stated in Article 183 of the Code of Criminal Procedure provided that, "A judge may not convict a person unless by at least two valid pieces of evidence, he or she has a reasonable belief that a crime actually occurred and that the defendant is guilty of committing it" (Jayantari and Sugama, 2019). So the evidentiary power of electronic documents in a trial will be perfect if it is equipped with other supporting evidence that can convince the judge.

Obstacles in solving cybercrime in buying and selling online in Cirebon City

In the implementation of solving cybercrime crimes in online buying and selling at the Cirebon City Police Station, there are obstacles in the resolution process, based on the results of research and interviews with Mr. Rajasa Wahyu Abadi as an Investigator at the Cirebon City Police regarding obstacles in solving cybercrime crimes in online buying and selling consisting of several obstacles including the following (Abadi, 2023):

1. Limited cybercrime special tools owned by the police to support investigators' infrastructure in uncovering online buying and selling fraud. And with the limitations of these tools, it takes a long time to uncover the criminal act of online buying and selling fraud or it can be said to be difficult to resolve. In addition, the tools needed require a fairly large cost.
2. There are still few law enforcers who understand about information technology or there is still a lack of experts in the field of computers / cyber experts. So that the police at the Cirebon City Police Station need cooperation with other law enforcement/cyber units that are at least in the Polda to uncover online buying and selling fraud.
3. The absence of a special unit focused on handling cybercrime cases, especially in online buying and selling fraud. At the Cirebon City Police Secretariat in handling criminal cases carried out by the Certain Crime Unit (Tipidter) which includes all criminal offences.
4. It is difficult to find evidence in handling online buying and selling fraud crimes, because evidence in the form of electronic information evidence and electronic documents via the internet so that if there is not enough evidence in online buying and selling fraud, the investigation and investigation process stops.
5. It is difficult to trace the perpetrator through the account number because banking is restricted by the Law regarding the privacy of bank customers so that the Bank will not provide the identity of its customers before the consent of the customer. Despite knowing that the registered account belongs to the perpetrator, the bank still has a provision that it is customer privacy.
6. It is difficult to track down the perpetrator because of the fake identity and mobile phone number that is no longer active or has been discarded, making it difficult for the police to track the whereabouts of the perpetrator

Based on the description above, it can be seen that in solving the crime of online buying and selling fraud, there are several obstacles that occur at the Cirebon City Police Station, from the limitations of special tools as a means of infrastructure for investigators in uncovering online buying and selling fraud crimes, to the difficulty of finding evidence and tracking down perpetrators. So, from these obstacles, it becomes less effective for the Cirebon City Police in implementing the resolution of cybercrime crimes in online buying and selling.

The implementation of solving cybercrime crimes in online buying and selling in Cirebon City is seen from Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE) and Islamic Law

Current technological developments have caused many positive impacts on life, one of which is the way of transactions for Indonesian people who have begun to change from conventional transactions (sellers and buyers face to face, using cash, requiring a place/store) to electronic transactions that open wider opportunities for business actors to expand their business with lower costs, easier buying and selling processes, and has a wider consumer reach (Solim, 2019). In addition, technological developments also have other impacts such as the emergence of crime through the internet or cybercrime, one of which is crime in the form of fraud in buying and selling online.

The perspective of Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE)

The crime of online buying and selling fraud is included in the group of illegal content crimes in the study of misuse of information technology in the form of computer fraud, a fraud or a fraud made to obtain personal gain or to harm others, while illegal contents is a crime by entering data or information on the internet about something that is not true, unethical, and can be considered to violate the law or disturb public order (Maskun, 2014).

In general, fraud has been regulated as a criminal offense by Article 378 of the Criminal Code which reads:

"*Whosoever with intent to benefit himself or others unlawfully, by using a false name or false dignity, by deceit, or a series of lies, moves another person to deliver anything to him, or to give a debt or write off a receivable shall be punished with fraud with imprisonment for not more than four years.*"

The understanding of the article is still general, which is reserved for things in the real world. Unlike the fraud on the internet regulated in the ITE Law, this fraud has a narrower space than the arrangements in the Criminal Code. The ITE Law regulates fake news and misdirection through the internet, fake news and misdirection can be equated with fraud regulated in Article 378 of the Criminal Code.

In its regulation in Article 28 (1) of Law Number 11 of 2008 as amended into Law Number 19 of 2016 concerning Information and Electronic Transactions which reads:

"Everyone intentionally and without rights disseminates false and misleading news that results in consumer losses in electronic transactions."

For violations of Article 28 (1) of the ITE Law, criminal threats are carried out as stipulated in Article 28 jo 45 paragraph (2) of the ITE Law: "Any person intentionally and without rights disseminating false and misleading news that results in consumer losses in electronic transactions, shall be punished with a maximum of six years or a maximum fine of Rp. 1,000,000,000.00 (one billion rupiah)."

The application of article 28 of the ITE Law is in accordance with the principle in criminal law, namely the specialist derogate legi generalis that special provisions override special provisions. In this case, the provisions in the Criminal Code cannot be applied because there is no element of electronic fraud, so the special provisions in the ITE Law are in accordance with the criminal act of fraud through social media because it is related to technology (Iqbal, 2012).

For proof, law enforcement officials use electronic evidence of funds or printouts as an expansion of evidence, which is contained in Article 5 paragraphs (1), (2) of the ITE Law:

1. Electronic Information and/or Electronic Documents and/or printouts thereof constitute valid legal evidence.
2. Electronic Information and/or Electronic Documents and/or printouts as referred to in paragraph (1) shall constitute an expansion of valid evidence in

accordance with the applicable Procedural Law in Indonesia (Law Number 11 of 2008).

Basically, it can be concluded that the ITE Law provides protection for victims of online buying and selling fraud via the internet in the form of providing criminal sanctions to perpetrators of fraud through the internet. Criminal sanctions provided by the ITE Law are in the form of imprisonment and fines.

Islamic Legal Perspectives

Islam forbids all forms of criminal acts including all forms of fraud. Fraud is a crime committed by someone by lying to others or deceitful to see against the right in order to obtain greater benefits for his person, both goods and money (Ali, 2012). The legal basis for someone who commits fraud or lies is found in the Qur'an Surat An-Nisa verse 29:

يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَأۡكُلُوٓاْ أَمۡوَٰلَكُم بَيۡنَكُم بِٱلۡبَٰطِلِ إِلَّآ أَن تَكُونَ تِجَٰرَةً عَن تَرَاضٖ مِّنكُمۡۚ وَلَا تَقۡتُلُوٓاْ أَنفُسَكُمۡۚ إِنَّ ٱللَّهَ كَانَ بِكُمۡ رَحِيمٗا

It means: "Oh people, do not eat one another's property in a foolish way, unless consensual trade is conducted."

Islamic Sharia prohibits fraud which is the act of eating other people's property by bathil, fraud usually occurs in transactions in the field of muamalah such as buying and selling. Islam forbids any muamalah mixed with tyranny, deception, deception, obscurity and other things that are forbidden and forbidden by Allah SWT (Janwari, 2005). In any form of muamalah there should be no deceit or something that causes one party to feel aggrieved by the other.

The hadith narrated by Jabir (r) about the punishment for perpetrators of fraud is as follows:

وَعَنْ جَابِرٍ رضي الله عنه ، عَنِ النَّبِيِّ صلى الله عليه وسلم قَالَ : (لَيْسَ عَلَى خَائِنٍ وَلاَ مُنْتَهِبٍ، وِلاَ مخْتَلِسٍ ، قَطْعٌ) رَوَاهُ أَحمْدُ، وَالأَرْبَعَةُ،وَصَحَّحَهُ التِّرْمِذِيُّ ، وَابْنُ حِ بَّان

It means: "Jabir (r) narrated, the Prophet Muhammad (peace be upon him) said: there is no punishment for cutting off hands for traitors, pickpockets and robbers on the street" (HR. Ahmad, Abu Daud, An-Nasai, At-Tirmudzi and Ibn Majah). The hadith is shahih according to Tirmidhi and Ibn Hibban (Rahmi, 2018).

Regarding the hadith above, it can be equated between traitor and fraud. So the punishment that can be given to the perpetrators of this fraud crime is ta'zir. Jarimah ta'jir is a sanction of punishment of jarimah not expressly specified in the Qur'an and Sunnah, hence it is handed over to the ijtihad of man or society based on the benefit of the ummah according to circumstances, time and place. Similarly, in cybercrime cases because the judge has authority over him.

Given that in Indonesia the stipulated law refers to positive law and there has been a special regulation regarding cybercrime, namely the ITE Law, so that the punishment also refers to the law, not to Islamic criminal law, the sanctions that have been set in Islamic criminal law can be set to be jarimah ta'zir sanctions, where the application of jarimah ta'zir punishment depends on the authority of the ruler (judge) in solving problems regarding cybercrime crimes, namely buying and selling fraud Online.

CONCLUSION

Based on the results of the above research regarding the implementation of solving Cybercrime crimes in online buying and selling in Cirebon City, the perspective of Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE) and Islamic law can be concluded that, first, current technological developments have provided many conveniences by using electronic media, but it also has a negative impact with the emergence of crimes that occur in cybercrime (cybercrime) One of them is online buying and selling scams. This online buying and selling fraud crime has many cases that occur among the community, as has happened in the Cirebon City area,

causing losses to the community. Therefore, the police from the Cirebon City Police are needed to handle cases of fraud in online buying and selling by conducting an investigation process by investigators. The investigation process is carried out by checking the accounts of perpetrators of online buying and selling fraud in order to find evidence and track down the perpetrators. However, the police experienced several obstacles or difficulties due to limited tools to find electronic evidence and track down perpetrators, so cases of online buying and selling fraud were difficult to resolve.

Second, in solving the crime of online buying and selling fraud, there are several obstacles that occur at the Cirebon City Police Station from the limitations of special tools as a means of infrastructure for investigators in uncovering online buying and selling fraud crimes, to the difficulty of finding evidence and tracking down perpetrators. So, from these obstacles, it becomes less effective for the Cirebon City Police in implementing the resolution of cybercrime crimes in online buying and selling.

Third, the perspective of Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE) is that the existence of the ITE Law provides protection for victims of online buying and selling fraud via the internet in the form of providing criminal sanctions to perpetrators of fraud through the internet. Criminal sanctions provided by the ITE Law are in the form of imprisonment and fines. While in the Perspective of Islamic Law the punishment that can be given to perpetrators of this fraud crime is ta'zir. The law that is determined refers to positive law and there has been a special regulation regarding cybercrime, namely the ITE Law, so that the punishment also refers to the law, not to Islamic criminal law, then the sanctions that have been set in Islamic criminal law can be set to be jarimah ta'zir sanctions, where the application of jarimah ta'zir punishment depends on the authority of the ruler (judge) in solving problems regarding cybercrime crimes, namely online buying and selling fraud.

REFERENCES

Ahmadi, Rulam. (2014) Metodologi Penelitian Kualitatif. *Yogyakarta: Ar-Ruzz Media, 2014.*

Aisah, Siti. (2019). "*Penegakan Hukum Tindak Pidana Penipuan Online Di Kabupaten Sleman Yogyakarta Secara Integratif*", (Skripsi Sarjana, Universitas Ahmad Dahlan)

Ali, Zainuddin. (2012) Hukum Pidana Islam. *Jakarta: Sinar Grafika*

Amaliah, Dista Arifah. (2011) "Kasus Cybercrime Di Indonesia", *Jurnal Bisnis dan Ekonomi (JBE) 18*(2) September 2011.

Ayu, Gusti Shabaina Jayantari & Dewa Gede Dana Sugama, "Kekuatan ALat Bukti Dokumen Elektronik dalam Tindak Pidana Berbasis Teknologi dan Informasi (*Cyber Crime*)", *Program Kekhususan Peradilan Fakultas Hukum Universitas Udayana.*

Dharma, Adhi Aryyaguna. (2017) "*Tinjauan Kriminologis Terhadap Kejahatan Penipuan Berbasis Online (Studi Kasus Unit Cybercrime Reskrimsus Polda Sulsel)*" (Skripsi Sarjana, Universitas Hasanuddin Makassar).

an, Hendra. "Tindak Pidana Penipuan Dalam Persfektif Fikih Jinayah", *Jurnal El-Qanuny: Jurnal Ilmu-Ilmu Kesyariatan dan Pranata Sosial 4*(2) Desember 2018.

Hediana, Runto & Ahmad Dasuki Aly, "Transaksi Jual Beli Online Perspektif Ekonomi Islam", *Jurnal Penelitian Hukum Ekonomi Syariah 3*(2) 2016.

https://www.hukumonline.com/klinik/a/landasan-hukum-penanganan-icybercrime-i-di-indonesia-cl5960#_ftn1

https://www.radarcirebon.com/2019/04/10/tertipu-beli-sepatu-lewat-instagram-warga-kesunean-gagal-buka-usaha/

Ilyas, Amir. (2012) Asas-asas Hukum Pidana. *Yogyakarta: Rangkang Education.*

Iqbal, Muhammad. "Media Sosial sebagai Sarana Tindak Pidana Penipuan", *Fakultas Ilmu Sosial, Universitas Islam Kuantan Singingi*.

Jannah, Sofwan & M. Naufal. "Penegakan Hukum Cybercrime Ditinjau Dari Hukum Positif Dan Hukum Islam" *Al-Mawarid 12*(1) Feb-Agust 2012.

Janwari, Yadi. (2005) Asuransi Syari'ah. *Bandung: Pustaka Bani Quraisy.*

Kurniawan, Gahfuur Pangku Alam. (2020). *"Analisis Yuridis Penegakan Hukum Pidana Terhadap Tindak Pidana Penipuan Bisnis Online*" (Skripsi Sarjana, Universitas Muhammadiyah Palembang).

Lamintang, P.A.F. (1997) Dasar-dasar Hukum Pidana Indonesia. *Bandung: Citra Aditya Bakti.*

M. Arief, Dikdik Mansur, Elisatris Gultom. (2009) Cyber Law Aspek Hukum Teknologi Informasi. *Bandung: PT. Refika Aditama.*

Maskun. (2014) Kejahatan Siber (Cyber Crime) Suatu Pengantar. *Jakarta: Kencana.*

Miftah, Shabur Maulana, Heru Susilo & Riyad, "Implementasi E-Commerce Sebagai Mediapenjualan Online", *Jurnal Administrasi Bisnis (Jab) 29*(1) Desember 2015

Moeljatno. (2015) Asas-Asas Hukum Pidana. *Jakarta: PT Rineka Cipta.*

Monica, Melisa Sumenge "Penipuan Menggunakan Media Internet Berupa Jual-Beli *Online*" *Lex Crimen 2*(4) Agustus 2013

Nur, Satria Fauzi, Lushiana Primasari, "Tindak Pidana Penipuan Dalam Transaksi Di Situs Jual Beli *Online* (E-Commerce)", *jurnal Recidive 7*(3), Sept.- Des 2018

Raco, J.R. *Metode Penelitian Kualitatif Jenis, Karakteristik, dan Keunggulannya*. Jakarta: PT. Grasindo, 2010.

Rahmi, Nailul. "Hukuman Potong Tangan Perspektif Al-Qur`An Dan Hadis", *Jurnal Ulunnuha 7*(2), Desember 2018.

Santoso, Sugeng. "Sistem Transaksi E-Commerce Dalam Perspektif Kuh Perdata Dan Hukum Islam", *Ahkam 4*(2), November 2016

Solim, Jevlin, dkk. "Upaya Penanggulangan Tindak Pidana Penipuan Situs Jual Beli *Online* Di Indonesia" *Jurnal Hukum 14*(1) Januari-Juni 2019.

Sumadi, Hendy. "Kendala Dalam Menanggulangi Tindak Pidana Penipuan Transaksi Elektronik Di Indonesia" *Jurnal Wawasan Hukum, 33*(2) September 2015.

Undang-Undang Republik Indonesia (2008). Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE)

Wahyuni, Fitri. (2017) Dasar-dasar Hukum Pidana Di Indonesia. *Tanggerang Selatan: PT. Nusantara Persada Utama*.

Zainol, Moh. Arief & Sutrisni, "Perbuatan Melawan Hukum Dalam Transaksi Jual-Beli Melalui Internet Ditinjau Dari Buku III KUHPerdata" *Jurnal Jendela Hukum* 1(2) September 2014.