
Law Enforcement of Criminal Fraud in Online Buying and Selling in Surakarta

Ibrahim Nurrohman¹, Muchamad Iksan²¹ Muhammadiyah University of Surakarta (C100180074@ums.ac.id)² Muhammadiyah University of Surakarta (mi214@ums.ac.id)

ABSTRACT

The purpose of this study is to investigate the law enforcement agencies against online trading fraud in Surakarta Police Station, to know the obstacles in cracking down on online trading fraud in Surakarta Police Station, and to know from the perspective of online trading. Makassid Shariah. The approach method used in this paper is the legally demonstrative approach. This type of research in this article is descriptive research. Data sources have primary and secondary data. The findings obtained indicate that the legal protection of victims in Indonesia's statutory law includes several laws, including the Constitution of 1945, Law No. 13 of 2006 on Protection of Witnesses and Victims, and Law No. 39 of 1999 on Human Rights and Human Rights. Indicates that it is stipulated by a certain law. Law No. 11 of 2008 on Information and Electronic Transactions. As a strategic step to overcome these technical hurdles, it is critical that authorities build expertise in cybercrime and network security. Islamic law, as verse 105 of the Koran Surah an-Nar and the Hadith of the Prophet, clearly states regarding fraud in sales transactions: Those who do treason and manipulation. ", the place of hell. (narrated by Ibn Hiban).

Keywords: Online trading, fraud, law enforcement

INTRODUCTION

Fraud committed online, also known as internet fraud or cyber scam, is a crime that involves the use of technology and the internet to defraud others with the goal of stealing money, personal information, or other valuable resources. Traditional fraud crimes refer to fraud committed outside the online or internet environment. The following is an explanation of traditional fraud crimes in general: Traditional fraud involves deception or misappropriation that occurs in direct interaction between the fraudster and the victim, without involving electronic media. The difference between traditional and online fraud crimes lies in the way they are carried out and the media used (Prasetyo 2014).

Laws regarding online fraud, such as fraud via the internet or online platforms, can vary depending on the jurisdiction or country in question. It is important to note that laws regarding online fraud are constantly evolving (Primasari 2018). The following are some examples of online buying and selling fraud that you need to be aware of: a) Payment Fraud: Fraudsters pose as buyers and offer fake payments or try to steal your financial information. They may use fake checks, fake transfer instructions, or unauthorized online payment methods. b) Goods or Services Fraud: Fraudsters offer goods or services through online platforms, but after receiving payment, they do not deliver the promised goods or services. They may also sell counterfeit or defective items that do not match the description. c) Identity Fraud: Fraudsters use fake identities or steal other people's identities to conduct online transactions. They may use stolen personal information to gain financial gain or carry out other illegal activities (Solim, et. all, 2019).

Article 378 of the Indonesian Criminal Code (KUHP) regulates fraud in a general context, including fraud in online buying and selling. The article states: "Anyone who deliberately deceives someone, with the intention of benefiting himself or another person, or with the intention of harming another person, will be punished for fraud with a maximum imprisonment of 4 (four) years and 8 (eight) months." In the context of online buying and selling fraud, Article 378 of the Criminal Code can be applied if a person

intentionally deceives another party in a buying and selling transaction carried out online with the intention of gaining a profit for himself or another person, or to harm another party.

The criminal act of online buying and selling fraud can be related to articles in the Criminal Code (KUHP) and Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE) in Indonesia. Article 378 of the Criminal Code: This article regulates criminal acts of fraud in general, including in the context of online buying and selling fraud. Article 378 of the Criminal Code (KUHP) is one of the articles that regulates criminal acts of fraud.

Article 378 of the Criminal Code stipulates that someone who intentionally uses a false name, deception, loses consciousness, abuses trust, or uses a fake document to mislead another person and unlawfully deprive or take control of another person's property or the right to that property, or misleads another person. other people into debt or dependents with the intention of causing loss, can be charged with the crime of fraud.

Article 28 in Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE) explains that every person who intentionally and without right distributes, transmits or makes accessible electronic information and/or electronic documents that contain insulting and/or offensive content. or defamation, can be subject to sanctions in accordance with the provisions regulated in the ITE Law.

Sanctions for violating Article 28 of the ITE Law can be imprisonment for a certain period of time and/or a fine. It is important for the authorities to evaluate each case individually and identify which articles are most relevant and applicable in handling criminal acts of online buying and selling fraud. Article 28 Paragraph (1) of Law Number 11 of 2008 concerning Information and Electronic Transactions focuses more on the act of disseminating electronic information that contains insults or defamation. For online buying and selling fraud, the relevant article is Article 378 of the Criminal Code, as previously explained.

Article 378 of the Criminal Code and Article 28 paragraph (1) of the ITE Law regulate different things. The main difference between the two is in terms of the focus and scope of the offenses regulated. Article 378 of the Criminal Code is broader and covers fraud in general without being directly related to electronic media. Meanwhile, Article 28 Paragraph (1) of the ITE Law is more related to electronic content containing insulting and defamatory content that is distributed via electronic or online media.(Hutomo 2021).

Maqashid sharia is a concept in Islamic law that refers to the objectives or principles underlying Islamic law. This concept aims to achieve goodness and benefit for humanity and prevent harm in this life. *Maqashid sharia* acts as a guide for understanding, interpreting, and applying Islamic law by taking into account the final goals desired by the sharia(Deep 2017).

The functions and objectives of *Maqashid sharia* in the context of Islamic law are as follows: a) *Maqashid sharia* aims to achieve the benefit of mankind in their lives. It includes the physical, moral, spiritual, social, and economic good of individuals as well as society as a whole; b) *Maqashid sharia* functions as a guide to upholding justice in the Islamic legal system. The aim is to ensure fair treatment for all individuals, protect their rights, and prevent abuse of power; c) *Maqashid sharia* also aims to prevent harm and reduce losses in society. This includes protecting life, property, honor, religion, reason, and human offspring from all forms of loss and danger' d) *Maqashid sharia* helps understand and apply Islamic sharia contextually and relevant to the times. This allows for flexibility in dealing with social change, technology and new challenges that arise(Al-Hasani Islamic Boarding School 2020).

In the Qur'an, Surah Al Baqoroh verse 275 contains a prohibition and warning about usury, namely the system of borrowing money at interest which is prohibited in Islam. This verse emphasizes that people who are involved in usury will face bad consequences and are compared to someone who is possessed by the devil due to insanity. This verse also explains the difference between usury and halal buying and selling. Allah has permitted buying and selling which is done fairly and has prohibited usury. People who have accepted the prohibition regarding usury must stop this practice. If someone has stopped taking usury after gaining knowledge of the prohibition, then what he received previously will become his own and further matters will be in the hands of Allah. In the Hadith it is said "Whoever cheats, he is not among

us. People who commit treason and deception, their place is in hell" (HR. Ibnu Hibban 2: 326)(Nasaruddin 2021).

The man who steals and the woman who steals, have their hands cut off (as) retribution for what they have done and as a punishment from Allah. And Allah is All-Mighty, All-Wise. (Qs. Al-Maidah: 38)(Azizah 2021). The concept of Hajiyat in Islamic law is related to the principle of Maqashid sharia, which emphasizes fulfilling the benefit of humanity. Hajiyat covers essential and important needs for individual and community life, such as the need for food, clothing, shelter, education, health and protection. In the context of Islamic law, the Hajiyat principle can be used as a consideration in making legal decisions or fatwas(Azizah 2021).

Tahsiniyat refers to benefits or benefits related to an individual's morals or integrity. This term is often used in the context of Islamic ethics or moral values in Islam. Tahsiniyat means improving or increasing an individual's morality, behavior and moral quality. Tahsiniyat includes the moral demands and needs necessary to maintain individual dignity, integrity and honor in everyday life. Examples of Tahsiniyat in Islam include improving morals (morality), practicing honesty, generosity, justice, patience, and avoiding behavior that damages morality such as lying, cheating, or violence.(Azizah 2021).

The Covid-19 (Corona Virus Disease 2019) pandemic emerged in all parts of the world in 2020, resulting in restrictions on all human activities. So, most people need their wants and needs every day online. Then, online buying and selling activities are often carried out. However, online fraud appears along with online buying and selling activities(2021 Protection Legal Aid Institute).

Throughout 2020 there were 707 cases [crime](#) based on the statement from the Solo Police. This number decreased by 10.05 percent compared to the cases revealed throughout 2019 with 786 cases. Police Commissioner Ade Safri Simanjuntak as Solo Police Chief, revealed that through 707 previous cases, the number of crime resolutions was 474 cases. This is homework [Solo Police](#) to always continue to optimize the implementation of investigations and investigations of cases experienced in 2020(Sholikah 2020). Case resolution is 67 percent, which is more than the target of 60% in each fiscal year. Regarding the crime time interval in 2020, every 1 hour 3 minutes 8 seconds experienced a crime in the Solo Police jurisdiction, every 56 minutes 48 seconds experienced in 2019(Sholikah 2020).

The chronology of cases related to online buying and selling fraud that occurred in Surakarta is where the incident began The victim admitted that the incident began at the beginning of this month. He saw a post from an account in the name of Arie Fitri selling a low-priced Honda CBR motorbike. At that time he made the sale for IDR 12.5 million. After he comments, then continue the chat via WA (WhatsApp)(Christian 2020).

On Saturday he sent a down payment of IDR 1.5 million. Two days later, the perpetrator asked for money back worth Rp. 3 million, he said, for filing purposes. Then, he said, on the 11th, his motorbike arrived at his house. In total, Toharoh had spent IDR 4.5 million, but after waiting until Tuesday evening, his dream motorbike didn't arrive. He actually felt suspicious. However, the perpetrator and his entire business always gave the victim confidence. Moreover, the victim received a National Police KTA (Membership Identification Card) along with Arie's photo, driver's license and KTP(Christian 2020). Because there is an identity, it is trusted. Then the suspect said that he was a member, so it was impossible to commit fraud. However, so far, then confirmed with Mbak Arie, in fact the identity sent was fake. When asked for confirmation, Brigadier Arie Fitri clarified that the photo he had used in carrying out online buying and selling fraud(Christian 2020).

Cases of online buying and selling fraud were experienced due to the presence of fake news which also led to misguidance by causing losses to customers in electronic transactions, further Article 45 in Law no. 11 of 2008 concerning Electronic Information and Transactions (UU ITE) Paragraph (1) Every person who intentionally and without right obtains, controls, changes or deletes Electronic Information and/or Electronic Documents belonging to another person, shall be punished with a maximum imprisonment of 6 (six) years or a maximum fine of IDR 1,000,000,000.00 (one billion rupiah). This matter is in accordance with the principle of *lex specialis derogat legi generali* which contains the meaning that specific legal

regulations can exclude general legal regulations, so, if you experience online buying and selling fraud, the article that can be implemented is Article 28 paragraph (1) Law Number 19 of 2016 concerning Electronic Information and Transactions. Article 45A paragraph (1) Law Number 19 of 2016 concerning Electronic Information and Transactions as long as the elements are met (Hutomo 2021).

Islamic law clearly explains fraud in purchase and sale transactions as stated in the Qur'an Surah An-Nahl verse 105 which reads:

وَالَّذِينَ يَدْعُونَ لِلشَّيْءِ الْكُذِّبِ

Meaning: "Indeed, those who invent lies are only those who do not believe in the verses of Allah, and they are liars."

The Prophet said:

مَنْ غَشَّنَا فَلَيْسَ مِنَّا

Meaning: "Whoever cheats, he is not among us. People who commit treason and manipulation, will go to hell." (HR Ibn Hibban).

Based on the description above, the author is interested in knowing about the role of judges in providing witness and victim protection in teleconference criminal justice. Therefore, the author is interested in conducting research which is realized in the form of a thesis entitled "ENFORCEMENT OF THE CRIMINAL ACT OF FRAUD IN ONLINE BUYING AND BUYING IN SURAKARTA"

RESEARCH METHODS

This thesis research was carried out using a juridical-empirical approach. The juridical-empirical approach is a method or approach in legal research that combines legal analysis (juridical approach) with empirical observations of facts and data related to legal phenomena. Juridical-empirical approach, researchers or legal experts will use traditional legal approaches, such as analyzing laws, court decisions, and other legal documents (juridical approach), but will also involve collecting empirical data through observation, interviews, surveys, or statistical analysis (empirical approach) related to law enforcement of criminal acts of fraud in online buying and selling in Surakarta (Wardiono 2004).

This research was conducted descriptively, a type of research that combines a descriptive approach with an empirical approach. A descriptive approach is used to describe or describe a phenomenon related to law enforcement of criminal acts of fraud in online buying and selling in Surakarta (Amirudin 2012).

Data source; a) Primary, is data that can be obtained directly through the first party. The research data was obtained from interviews at the Surakarta police station and victims of fraud, so that the results of the data collection can be ascertained from the implementation of the provisions of Article 378 of the Criminal Code and Article 28 paragraph (1) Law Number 19 of 2016 concerning Electronic Information and Transactions as well as obstacles in its implementation; b) Secondary Data, is data in the form of written descriptions of primary legal materials, including from the perspective of statutory regulations, research results, as well as legal experts. The 1945 Constitution of the Republic of Indonesia, the Criminal Code, Law Number 11 of 2008 concerning electronic information and transactions and Law Number 19 of 2016 concerning electronic information and transactions are the primary legal materials used in research. This. Secondary legal materials can be opinions of legal experts or doctrines obtained from literature, scientific articles, research results (Amirudin 2012).

The data collection methods for this research are as follows: a) Data Collection: First of all, empirical data must be collected according to a predetermined method; b) Data Categorization: After the data has been collected, the next step is to categorize or group the data according to relevant variables; c) Descriptive Analysis: to describe and summarize data narratively; d) Juridical Analysis: At this stage, the data collected and analyzed are descriptively analyzed using the relevant legal framework. This analysis helps to understand the legal implications of the empirical data found; e) Data Integration: This stage involves the integration of juridical and empirical data. The results of juridical and descriptive analysis are linked to look for relationships or patterns that may exist between legal factors and empirical factors; f)

Interpretation and Conclusion: The final stage in juridical-empirical data analysis involves interpreting the results of the analysis and concluding the research findings. The results can be used to inform policy, provide recommendations, or expand understanding of research subjects related to law enforcement of criminal acts of fraud in online buying and selling in Surakarta (Moleong 2007).

RESULTS AND DISCUSSION

Law Enforcement Against Fraud in Online Buying and Selling at the Surakarta Police

Article 1 number 17 of the ITE Law refers to the definition of "Online Buying and Selling Transactions" in Law Number 19 of 2016 concerning Electronic Information and Transactions (UU ITE) in Indonesia refers to the process of buying and selling goods or services carried out via electronic media, such as website, mobile application, or electronic trading platform. These transactions involve interactions between sellers and buyers conducted electronically, including ordering, payment, delivery, and the exchange of related information. The ITE Law also regulates requirements and protections related to online buying and selling transactions, such as consumer protection, validity of transactions, electronic payments, rights and obligations of sellers and buyers, protection of personal data, and so on. (Zaman 2001).

Legal protection for cybercrime victims in Indonesia is based on several laws that regulate crimes in cyberspace. The following are some relevant laws: Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE): The ITE Law is a law that regulates crimes in cyberspace, including crimes such as online fraud, insults via social media, and electronic data theft. The ITE Law provides legal protection for victims and regulates criminal sanctions for cybercrime perpetrators.

Law Number 19 of 2016 concerning Amendments to the ITE Law: This law is an amendment to the previous ITE Law. One significant change is the addition of an article regarding the crime of spreading pornographic or slanderous content via electronic media. Law Number 21 of 2019 concerning Personal Data Security: This law regulates the protection of individuals' personal data, including regulation of personal data processing, collection, use and disclosure of personal data. This law provides legal protection for victims of personal data theft. (Iksan 2020).

Article 21 of Law Number 19 of 2016 concerning Information and Electronic Transactions (UU ITE) in Paragraph (1) states that Every Person intentionally and without right distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents which contains insulting and/or defamatory content; Paragraph (2) Every person intentionally and without right disseminates Electronic Information and/or Electronic Documents which contain insulting and/or defamatory content.

The results of interviews conducted by researchers with the Head of Criminal Investigation Unit of the Surakarta Police regarding law enforcement against fraud in online buying and selling include the following:

First, "The police will receive reports from victims of online fraud. The victim must report the case to the police and provide all relevant information, including evidence of transactions, conversations with the perpetrator, and other available evidence."

Second, "after receiving the report, the police will conduct a preliminary investigation to verify the validity of the claim and gather further information. This may involve interviewing the victim, examining transaction records, contacting relevant parties, or using technical resources to gather electronic evidence."

Third, "in the case of online fraud, tracking and identifying perpetrators can be challenging. However, by using technical tools such as digital footprint analysis, transaction monitoring, or collaboration with payment service providers, the police can try to trace the perpetrator and identify his identity."

Fourth, "The police will collect strong evidence to support fraud cases. This may include transaction evidence, communication records, digital traces, or the testimony of relevant witnesses. This evidence will be the basis for further legal proceedings."

Fifth, "after the perpetrator has been identified, the police can make an arrest with permission from

the investigator or prosecutor. Perpetrators will be faced with legal proceedings and prosecuted in accordance with the laws applicable in that jurisdiction.”

Sixth, "The police can work with payment service providers, online buying and selling platforms, or other related institutions to collect additional information, obtain cooperation in prosecutions, or improve security and prevent fraud in the future."

Obstacles in Enforcement Against Fraud in Online Buying and Selling at the Surakarta Police

The characteristics of cybercrime, or computer crime, include several aspects that differentiate it from conventional crime. The following are some general characteristics of cybercrime: a) use of technology: cybercrime involves the use of information technology and computers as a tool to commit crimes. This includes the use of the internet, computer networks, mobile devices, and malicious software (malware) to commit criminal acts; b) global reach: cybercrime is not limited to geographical boundaries; c) anonymity and difficult to trace: cybercrime perpetrators often use disguise techniques and tools to hide their identity. They can use technologies such as virtual privacy networks (VPN), proxies, or fake IP addresses to hide their digital footprints. This makes it difficult to track and identify criminals (Labib 2005).

As a result of interviews conducted by researchers with the Head of Criminal Investigation Unit of the Surakarta Police, there are several obstacles that may be faced in investigating cases of online buying and selling fraud, including the following:

First, security and anonymity: "online fraudsters often hide their identity by using fake accounts or other fraudulent techniques. This makes it difficult for the police to trace and identify the perpetrators."

Second, a difficult digital footprint: "online buying and selling fraud often involves money transfers via electronic payment systems, such as bank transfers, digital wallets, or cryptocurrencies. Tracking money digitally can be difficult and requires collaboration with payment service providers to obtain relevant transaction information."

Third, the number of cases is high: "cases of online buying and selling fraud are usually quite abundant, and the police often have limited resources. This may impact their ability to handle all cases quickly and efficiently."

Fourth, lack of evidence: "in some cases, sufficient evidence to prosecute perpetrators of online fraud is difficult to find. Perpetrators often use electronic concealment techniques or other methods to erase their digital footprints, making it difficult for police to gather solid evidence."

Fifth, the difficulty of access to providers: the difficulty of access given to providers to find out the identity of the perpetrator means that the case of online buying and selling fraud that occurred in Surakarta did not progress or even end."

Article 378 of the Indonesian Criminal Code (KUHP) regulates the criminal act of fraud which consists of the following elements: a) Intent to benefit oneself or another person unlawfully; b) Deliberately defrauding someone; c) By using a false name or using someone else's name, or by carrying out other tricks; d) As a result of the deception, the person being deceived gives something, conveys something, or does something; e) Property loss occurs as a result of the fraudulent act. If all of these elements are met, the perpetrator of the fraud can be subject to imprisonment with a maximum sentence of four years or a maximum fine of nine hundred rupiah.

Online fraud, also known as cyber fraud, refers to actions that involve the misuse of technology and the internet to carry out fraudulent or counterfeit activities with the aim of illegitimate gain. It is a practice that involves the use of digital media and computer networks to obtain personal information, financial or sensitive data from individuals or other entities with the intent to defraud or harm them (Ali 2011).

According to the Head of Criminal Investigation Unit of the Surakarta Police, online buying and selling fraud explains that it often involves the use of fake accounts or fake identities. Perpetrators may use hidden IP addresses or other technical means to disguise their digital footprint. This makes it difficult for authorities to identify and track fraudsters (Maskun 2022).

Fraudsters often create fake websites that imitate the appearance of genuine online buying and selling sites. They use phishing or disguise techniques to appear convincing, making it difficult for victims

to differentiate between genuine and fake websites. Online buying and selling fraud often involves payments via digital wallets or other electronic payment systems. Perpetrators can use fake accounts or steal victims' payment information to carry out illegal transactions. This makes tracking and recovering funds more difficult because digital money transfers can be done quickly and anonymously (Maskun 2022).

Online fraudsters tend to use various techniques to hide their digital footprints. They can use virtual private networks (VPNs) or proxies to hide their IP addresses, or use encrypted messaging services to avoid monitoring by authorities. This complicates investigation and prosecution efforts (Dang 2020). As a strategic step to overcome these technical obstacles, it is important for the authorities to develop expertise in the field of computer crime and network security. Collaboration with payment service providers and online buying and selling platforms is also important to identify and stop fraudulent activities. Better public education and awareness about the threat of online fraud can also help reduce the number of fraud cases.

Online Buying and Selling from a Maqasid Syariah Perspective

In electronic buying and selling transactions, there are several types of legal relationships that can occur between the parties involved. The following are several types of legal relationships that are common in electronic buying and selling transactions: a) sales and purchase contracts: these contracts include agreements regarding prices, goods or services traded, payment, delivery, and other terms; b) service contract: in some online buying and selling transactions, there is a service contract formed between the seller or e-commerce platform and the buyer. These contracts are usually governed by terms and conditions that users must agree to before using the platform or making transactions; c) legal responsibility: in electronic buying and selling transactions, there are legal responsibilities that apply to both parties; d) consumer protection: in electronic buying and selling transactions, there is a legal relationship that involves consumer protection. The Consumer Protection Law may provide special rights to buyers, including the right to clear and accurate information, the right to obtain safe and quality goods or services, and the right to compensation or a refund in cases of nonconformity or fraud (Makarim 2004).

Islamic law clearly explains fraud in purchase and sale transactions as stated in the Qur'an Surah An-Nahl verse 105 which reads:

مَنْ أَكْثَرُ
 زُجْرًا
 وَالَّذِينَ
 كَذَبُوا
 فِي
 آيَاتِ
 اللَّهِ
 وَهُمْ
 كَاذِبُونَ

Meaning: "Indeed, those who invent lies are only those who do not believe in the verses of Allah, and they are liars."

The Prophet said:

مَنْ
 غَشَّنَا
 فَلَيْسَ
 مِنَّا

Meaning: "Whoever cheats, he is not among us. People who commit treason and manipulation, will go to hell." (HR Ibn Hibban).

Islamic law explains that buying and selling fraud is included in the category of prohibited acts. Islam encourages its followers to carry out trade with honesty, fairness and strong trust in buying and selling transactions. The principle of justice is very important in every buying and selling transaction in Islam. Justice demands that all parties involved in a transaction fulfill their rights and obligations honestly and fairly (Syarifuddin 2014). Fraudulent buying and selling violates this principle of justice. Honesty is a value that is highly upheld in Islam. Buying and selling fraud perpetrators violate this principle by deliberately providing false information or covering up important facts in transactions, which can harm other parties (Syarifuddin 2014).

Ghararis an element of uncertainty in a transaction that can cause losses to one of the parties. Transactions that contain excessive *gharar* elements, such as the sale of goods whose condition is unclear or uncertainty in price, can be considered a form of buying and selling fraud (Syarifuddin 2014). *Usury* refers to the prohibition in Islam against trading in certain goods that have the characteristics of *riba* (interest). If there are fraudulent practices involving *ribawi* transactions, such as changing prices or avoiding payments that should be made, it is also considered to violate Islamic law (Syarifuddin 2014).

Islam explains that buying and selling fraud is considered a sin and an act that harms other people.

Parties involved in buying and selling fraud are encouraged to correct their mistakes, restore lost rights, and repent to Allah. On the legal side, Muslim communities are expected to follow the legal provisions applicable in their country and report cases of buying and selling fraud to the authorities for follow-up in accordance with applicable legal regulations.

CONCLUSION

Indonesian positive law, consumer protection from criminal acts of fraud in online buying and selling is regulated by several relevant laws and articles. Several laws that provide consumer protection include Law no. 8 of 1999 concerning Consumer Protection, Law Number 19 of 2016 concerning Electronic Information and Transactions (UU ITE), and the Criminal Code (KUHP). In the context of the Criminal Code, related articles include Article 378 concerning fraud, Article 372 concerning embezzlement, and Article 263 concerning forgery. Acts of fraud, embezzlement or forgery in online buying and selling may be subject to criminal sanctions in accordance with applicable legal provisions. In addition, Law Number 8 of 1999 concerning Consumer Protection provides general protection for consumer rights, including in online buying and selling transactions. The ITE Law also regulates criminal acts in electronic transactions, which include fraud in the online context.

As a strategic step to overcome these technical obstacles, it is important for the authorities to develop expertise in the field of computer crime and network security. Collaboration with payment service providers and online buying and selling platforms is also important to identify and stop fraudulent activities. Better public education and awareness about the threat of online fraud can also help reduce the number of fraud cases.

Islamic law explains clearly regarding fraud in purchase and sale transactions as in the Qur'an Surah An-Nahl verse 105 which reads: "Indeed, those who invent lies are only those who do not believe in the verses of Allah, and they are liars. ." The Prophet said: "Whoever cheats, he is not among us. People who commit treason and manipulation, will go to hell." (HR Ibn Hibban).

REFERENCES

1. Ali, Mahrus. 2011. *Dasar-Dasar Hukum Pidana*. Jakarta: Sinar Grafika.
2. Amirudin. 2012. *Pengantar Metode Penelitian Hukum*. Jakarta: PT. Grafindo Persada.
3. Azizah, Siti. 2021. "Mengenal Lebih Dalam Maqashid Syariah: Pengertian Dan 5 Tujuannya." *BSI*. <https://www.bsimaslahat.org/blog/2022/04/04/mengenal-lebih-dalam-maqashid-syariah-pengertian-dan-5-tujuannya/>.
4. Christian, Antonius. 2020. "Niat Beli Motor Murah, Emak-Emak Tertipu Akun Bodong Catut Polwan Solo." *Jawa Pos Radar Solo*. <https://radarsolo.jawapos.com/daerah/solo/12/02/2020/niat-beli-motor-murah-emak-emak-tertipu-akun-bodong-catut-polwan-solo-2/>.
5. Dang, Yearim. 2020. *Why? Cyber Crime-Kejahatan Dunia Maya*. Jakarta: Elex Media Komputindo.
6. Hutomo, Dimas. 2021. "Cara Menentukan Pasal Untuk Menjerat Pelaku Penipuan Online." *Universitas Katolik Parahyangan*. <https://lbhpengayoman.unpar.ac.id/sanksi-pidana-bagi-pelaku-penipuan-jual-beli-online/>.
7. Iksan, Rizal Pambudi & Muchamad. 2020. "Tinjauan Yuridis Perlindungan Hukum Bagi Korban Cyber." In *Universitas Aisyiyah Surakarta*, Surakarta: Universitas Aisyiyah Surakarta: The 12th University Research Colloquium.
8. Jauhar, Ahmad Al-Mursi Husain. 2017. *Maqashid Syariah*. Jakarta: Amzah.
9. Labib, Abdul Wahid & M. 2005. *Kejahatan Mayantara (Cybercrime)*. Bandung: Refika Aditama.
10. Lembaga Bantuan Hukum Pengayoman. 2021. "Sanksi Pidana Bagi Pelaku Penipuan Jual Beli Online." *Universitas Katolik Parahyangan*. <https://lbhpengayoman.unpar.ac.id/sanksi-pidana-bagi-pelaku-penipuan-jual-beli-online/>.

11. Makarim, Edmon. 2004. *Kompilasi Hukum Telematika*. Jakarta: Raja Grafindo Persada.
12. Maskun. 2022. *Kejahatan Siber (Cyber Crime): Suatu Pengantar*. Jakarta: Prenada Media.
13. Moleong, Lexy J. 2007. *Metode Penelitian Kualitatif*. Bandung: Tarsito.
14. Nasaruddin. 2021. "Hukum Jual Beli COD Cash of Delivery, Apakah COD Diperbolehkan Dalam Islam?" *Tribun Pontianak*. <https://pontianak.tribunnews.com/2021/10/16/hukum-jual-beli-cod-cash-of-delivery-apakah-cod-diperbolehkan-dalam-islam?page=all>.
15. Ponpes Al-Hasani. 2020. "Mengenal Maqashid Syariah, Pengertian Dan Bentuk-Bentuknya." *Ponpes Al-Hasani*. <https://ponpes.alhasanah.sch.id/pengetahuan/mengenal-maqashid-syariah-pengertian-dan-bentuk-bentuknya/>.
16. Prasetyo, Rizki Dwi. 2014. "Pertanggungjawaban Pidana Pelaku Tindak Pidana Penipuan Online Dalam Hukum Pidana Positif Di Indonesia." Universitas Brawijaya.
17. Primasari, Satria Nur Fauzi & Lushiana. 2018. "Indak Pidana Penipuan Dalam Transaksi Di Situs Jual Beli Online (E-Commerce)." *Recidive* 7(3): 251.
18. Sholikhah, Binti. 2020. "Polresta Solo Ungkap 707 Kasus kejahatan Selama 2020." *Republika*. <https://news.republika.co.id/berita//qm6h6r370/polresta-solo-ungkap-707-kasus-kejahatan-selama-2020?>
19. Solim, Jevlin, et.all. 2019. "Upaya Penanggulangan Tindak Pidana Penipuan Situs Jual Beli Online Di Indonesia." *Jurnal Hukum Samudera Keadilan* 1(1): 103–4.
20. Syarifuddin, Amir. 2014. *Garis-Garis Besar Ushul Fiqh*. Jakarta: Kencana.
21. Wardiono, Khudzaifah Dimiyati & Kelik. 2004. *Metode Penelitian Hukum*. Surakarta: Universitas Muhammadiyah Surakarta.
22. Zaman, Badrul. 2001. *Kompilasi Hukum Perikatan*. Jakarta: Citra Aditya Bakti.