Justice Law Review
Vol. 1, Nomor 1, 2025, pp. 37-56
e-ISSN: XXXX-XXXX; p-ISSN: XXXX-XXXX
DOI: https://doi.org/xxxx/xxxxx

Legal Protection for Victims of Fraud in Online Buying and Selling Transactions from the Perspective of Islamic Law

Siti Sumiwati Rannu[1*], Muh. Sutri Mansyah[2]

Universitas Muhammadiyah Buton
*Corresponding author's email: sitisumiwatirannu@email.com

Abstract

The rapid development of information technology, particularly in online buying and selling transactions, has increased the risk of fraud that harms consumers. This study aims to examine the form of legal protection for victims of fraud in online transactions from the perspective of Islamic law. The method used is a normative juridical approach, analyzing both Indonesia's positive law and sharia principles. The results show that legal protection can be carried out through penal (repressive) and non-penal (preventive) approaches. In Islamic law, fraudulent practices (gharar and tadlis) are prohibited acts, and perpetrators must be held morally and legally accountable. Islam emphasizes justice, honesty, and transparency in muamalah, including online transactions. In addition to national legal mechanisms such as the Criminal Code (KUHP) and the Electronic Information and Transactions Law (UU ITE), protection for victims can also be strengthened through educational approaches based on Islamic values to improve digital literacy and transaction ethics in society. The main obstacles in victim protection include weak oversight, low public legal awareness, and the suboptimal integration of Islamic principles into the practice of positive law. Therefore, synergy between national law and Islamic values is essential to create a fair and comprehensive protection system in the digital era.
Keywords: *legal protection, online fraud, Islamic law, electronic transactions.*

Submitted: May 01, 2025 | Accepted: June 03, 2025 | Published: June 30, 2025

Introduction

In recent years, Indonesia has experienced a significant acceleration in the development of its digital economy, marked by the rapid advancement of information and communication technologies, the widespread access to and use of the internet and digital devices by the public, and fundamental transformations in various sectors such as commerce, financial services, education, and public services. These developments have positioned Indonesia as one of the countries with the greatest potential in harnessing the digital economy, and it is predicted to become a major player in Southeast Asia in this field (Rosadi, 2018). This can be observed from the significant growth in the number of internet users. In 2016, there were 88.1 million internet users in Indonesia, and in 2017, that number increased by 51% to reach 132.7 million—nearly 50% of Indonesia's total population (Solim, Rumapea, Wijaya, Manurung, & Lionggodinata, 2019). Meanwhile, internet users in Indonesia have reached approximately 73.7% of the total population, according to a survey conducted by APJII (Indonesian Internet Service Providers Association) for the period 2019–2020 (Q2) (Gunawan, Aulia, Superno, Wijanarko, Uwiringiyimana, & Mahayana, 2023). Based on data from the Ministry of Communication and Information Technology (Kominfo) of the Republic of Indonesia in 2016, an analysis by Ernst and Young showed that the value of online trading in Indonesia has grown by 40% annually. Empirical conditions in Indonesia show that the number of internet users reached approximately 93.4 million people, of which 71 million used the internet as a means of obtaining information and communication, as well as for conducting online business. Economic growth and development are naturally also driven by advancements in technology and information, highlighting how individuals, in order to improve their economic standing, must continuously push themselves to increase their income and remain competitive (Bastari, Junaidi, & Ismiyanto, 2024).

One of the positive impacts of technological advancement is the significant change in the transaction patterns of Indonesian society, which previously involved conventional methods such as face-to-face meetings between sellers and buyers, the use of cash, and the need for physical locations like stores, but has now shifted to electronic transactions. This change offers greater opportunities for business actors to expand their enterprises with more efficient operational costs, more practical buying and selling processes, and a broader consumer reach. Currently, it is estimated that more than 25 million people in Indonesia are actively conducting transactions through e-commerce platforms (Syarief, Shahrullah, & Fitrianingrum, 2016).

The development of information technology has brought about a fundamental transformation in business transaction patterns, opening up various new opportunities that were previously unimaginable. This advancement not only facilitates communication and economic interaction across regions, but also creates an increasingly borderless global environment, thereby accelerating social change on a broad scale and at a very rapid pace. In this context, information technology plays a dual and complex role; on one hand, it serves as a driving force for the advancement of civilization, the improvement of quality of life, and the welfare of society. On the other hand, it also opens the door to various forms of misuse and criminal acts that violate the law, making it an ambivalent instrument in both social and legal structures (Primayoga, Saptono, & Njatrijani, 2019).

Buying and selling activities are increasingly expanding through the use of various virtual applications. Essentially, in Islam, buying and selling (transactions) fall under the category of *muamalah*, which is defined as the exchange of one item for another through a contract (*akad*). The basic legal ruling of *muamalah* is *mubah* (permissible) unless it contains prohibited elements or indications of fraud. As the development and advancement of the times especially in the field of technology and information can no longer be restrained, numerous issues have emerged, particularly in the area of sales contracts, which have nearly disappeared. Furthermore, the aspect of honesty between sellers and buyers must also be examined in light of how such conduct aligns with Islamic principles (Panggabean, 2022).

Electronic transactions are closely related to legal actions. This connection arises because it is easier for sellers to promote their goods dishonestly and in ways that do not reflect reality. According to Article 1 point 2 of Law No. 19 of 2016 concerning Electronic Information and Transactions (ITE Law), "An electronic transaction is a legal act carried out using computers, computer networks, and/or other electronic media" (Puspitasari & Sulistyo, 2024). The ITE Law is the first regulation in Indonesia to comprehensively govern electronic transaction activities and serves as an important milestone in the national legal system concerning the use of digital technology. The existence of this law provides legal certainty in the implementation of electronic activities, particularly those related to online communication and transactions, and is expected to protect public interests in an increasingly complex digital era. As explained by Kamran and Maskun (2021), the ITE Law not only functions as a legal umbrella for digital practices but also introduces reforms in the national legal framework to ensure a sense of security, justice, and legal certainty for every individual and business actor in utilizing electronic media for various transactional activities (Kamran & Maskun, 2021).

In Indonesia, the development of information technology has progressed rapidly and has had a significant impact on the economic sector. The use of information technology, particularly through the internet, has brought various broad benefits to society. One of the most tangible implications of this advancement is the emergence of electronic commerce (e-commerce), which has driven the popularity of online shops among the public. However, behind these benefits lies a negative side, one of which is the increasing number of fraud cases that exploit online trading platforms. Based on the provisions of Law No. 31 of 2014 as an amendment to Law No. 13 of 2006 concerning the Protection of Witnesses and Victims, Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), and Law No. 8 of 1999 on Consumer Protection, acts of fraud via the internet can be classified as criminal offenses. These actions may be subject to the provisions of Article 62 Paragraphs (1) and (2) of Law No. 8 of 1999 on Consumer Protection, Article 378 of the Indonesian Criminal Code (KUHP), as well as Article 28 Paragraph (1) and Article 45 Paragraph (2) of Law No. 11 of 2008 on ITE, as these acts meet the elements stipulated in those articles (Prakoso, Sujana, & Suryani, 2020).

Along with the rapid development of information technology within society, it is undeniable that online business platforms have become one of the primary sources of income for many individuals and business actors. The public has widely taken advantage of the convenience and efficiency offered by e-commerce to market products, reach consumers, and

carry out economic activities without geographical limitations. However, behind the great benefits offered by this technology lies a dark side that should not be overlooked. Technological advancement also opens up opportunities for irresponsible individuals who misuse online shop platforms as a means to commit crimes in the digital realm (Zulkifli, 2021). These perpetrators deliberately and systematically carry out fraud schemes to gain personal profit, exploiting security loopholes and users' lack of vigilance. Common crimes encountered in the online trading ecosystem include transaction fraud, identity falsification as either sellers or buyers, the delivery of fake or incorrect goods, and manipulation of product information. Such crimes frequently occur because perpetrators continuously innovate ways to exploit system vulnerabilities and take advantage of available technological advancements. The fact that technology is becoming increasingly sophisticated only strengthens their capacity to hide traces, expand their victim reach, and accelerate the criminal process, thus making consumer protection and the supervision of digital activities a major challenge in today's era of electronic commerce (Zulkifli, 2021).

Cybercrime can be understood as a form of criminal activity that takes place in digital space or cyberspace, and is generally defined as any illegal activity involving computers, computer networks, or digital systems—either as tools, targets, or locations where the criminal act occurs. This definition covers a broad spectrum of unlawful activities, as also explained in the Convention on Cybercrime, an international convention that serves as a reference for addressing cybercrime. The convention includes the criminalization of various acts, ranging from illegal access to computer systems, disruption of data and systems, computer-assisted fraud, to the online distribution of child pornography. The phenomenon of cybercrime continues to develop in a very dynamic and complex way, in line with the rapid advancement of information technology. Therefore, this type of crime is considered one of the most significant threats to global security and a strategic challenge that must be addressed seriously by the international community in the 21st century, both in terms of regulation, law enforcement, and adaptive and comprehensive cybersecurity policies (Maskun, et al., 2020).

Cybercrime is a form of modern criminality that has emerged alongside the rapid development of computer technology, particularly the internet, which has drastically transformed patterns of human interaction in various aspects of life. The presence of the internet and its cyberspace has created a virtual reality that offers convenience, efficiency, and tremendous potential in supporting human activities-ranging from communication and business transactions to education and governance. However, this advancement also brings negative consequences, as the digital space becomes a new arena for criminals to exploit vulnerabilities in information systems. Cybercrime can occur when computer networks are targeted-such as through hacking, data sabotage, and malware distribution-or when computers are used as tools to commit crimes, including online fraud, identity theft, and the distribution of illegal content. Given that information and data have become highly valuable assets with economic, political, and social dimensions, protecting such information is an urgent necessity in the context of both national security and individual protection. In this regard, the criminal law approach plays a vital role as a means of social control, providing deterrence and prevention against cybercrime through both penal (direct criminal action) and non-penal (prevention and rehabilitation)

measures. This approach is expected to offer effective legal protection for victims and safeguard the overall integrity of digital information systems (Sumenge, 2013).

From a criminological perspective, cybercrime in Islamic views is essentially a crime produced by society and is a common phenomenon. Therefore, to address this crime, a criminological study of the characteristics of the crime and its perpetrators is necessary. Richard Quiney argues that crime is caused by several complex factors, so understanding and tackling it requires an integrated approach between criminal law and other sciences. The study of crime involves keen investigation, even related to the structure of capitalist society. Such crimes are consequences of capitalist conflicts, including alienation, inequality, poverty, unemployment, moral decline, and economic crises in capitalist societies (Suharyadi, Sampara, & Ahmad, 2020).

Online trading activity, commonly referred to in modern terminology as electronic commerce or e-commerce, is a form of transformation in the business world that utilizes the advancement of digital technology especially the internet as the main medium for conducting the buying and selling of goods and services. E-commerce can be defined as a commercial transaction process carried out without physical presence between the seller and the buyer, where the entire process from offering, ordering, and payment to product delivery is conducted online. According to Chaerudin in Prakoso et al. (2020), this mechanism offers advantages in terms of time efficiency and effectiveness, as it allows business actors and consumers to transact anytime and anywhere, unrestricted by space and time. Amidst the rapid development of information technology, e-commerce activities are growing rapidly and have even become an integral part of modern lifestyle, particularly in urban areas, where the need for accessibility and speed of service is highly important. Nevertheless, behind its many benefits, online trading practices also carry a number of weaknesses and risks, especially due to the lack of direct interaction between the transacting parties. One common procedure in online transactions requires the buyer to first transfer funds including the product price, shipping fees, and taxes before the seller sends the purchased item. This pattern creates a gap that irresponsible parties can exploit through fraudulent or deceptive practices, especially considering the low barriers for individuals of all ages and backgrounds to create accounts on social media or e-commerce platforms. This phenomenon indicates the importance of strengthening digital literacy and consumer protection regulations in an increasingly inclusive yet vulnerable digital era (Prakoso, Sujana, & Suryani, 2020).

This study focuses on analyzing the forms of legal protection that can be provided to victims of fraud in online buying and selling transactions, viewed from the perspective of Islamic law. The main objective of this research is to gain a deeper understanding of how the legal system in Indonesia, both in terms of positive law and Sharia principles, regulates the protection of consumers who suffer losses due to fraudulent practices in e-commerce. Additionally, this study aims to examine the types of criminal sanctions that can be imposed on online fraud perpetrators and to evaluate the effectiveness of existing regulations in safeguarding the legal rights of victims. By integrating an Islamic legal approach, this research also seeks to explore how the values of justice, honesty, and responsibility taught in Islam can strengthen the protection of victims of fraud in the ever-evolving era of digital commerce.

Methods

This study employs a normative juridical approach, which is a legal research method aimed at examining the correlation between existing laws and regulations, legal theories, and the implementation practices of positive law relevant to the issue under investigation (Indrawan & Permatasari, 2022). This approach includes both statutory and conceptual methods, with documentation techniques as the primary method of data collection, involving the citation, summarization, and review of various legal sources. Data analysis is conducted through normative reconstruction using deductive and inductive legal reasoning (Prakoso, Sujana, & Suryani, 2020). The data sources consist of primary legal materials (such as Law No. 11 of 2008 on Electronic Information and Transactions, Law No. 8 of 1999, and the Indonesian Penal Code), secondary sources (including academic literature, online articles, and scholarly publications), and tertiary sources (such as legal dictionaries and encyclopedias) (Sumenge, 2013). To complement and strengthen the Islamic legal perspective in the context of online buying and selling, this study also explores additional primary sources, such as books on Islamic commercial jurisprudence (fiqh muamalah) and relevant academic journals, in order to uncover Sharia principles related to honesty, transparency, and the protection of rights in electronic transactions (Panggabean, 2022).

Results and Discussion

A. Legal Regulation in Indonesia on Cybercrime Fraud

1. Regulation of Cybercrime Offenses

A criminal act is essentially a human behavior or action that is explicitly defined by law as an unlawful act, deemed disgraceful, and therefore subject to criminal penalties. This formulation includes several key elements, such as the presence of a human act, a violation of legal norms, and the presence of fault, which serves as the basis for criminal liability. Not every unlawful act can immediately be considered a crime unless it meets the element of fault that can be legally accounted for. In the criminal justice system, criminal liability can only be imposed on a perpetrator if it is proven that the person committed the act with full awareness and had intent or negligence indicating culpability. This culpability is a central element in the construction of criminal responsibility, as it determines whether someone deserves to be punished. A person is considered culpable if, at the time of committing the act, they understand that the action violates the law and is deemed morally and socially unjustifiable. The assessment of culpability is not only based on the perpetrator's personal viewpoint but also evaluated objectively through the normative views of society concerning prevailing legal values. Therefore, criminal acts are not merely viewed from a formal perspective as legal violations, but also from a substantive perspective encompassing moral and social responsibility. Thus, the element of fault and the societal view of such fault serve as crucial foundations in determining the presence or absence of criminal liability for the perpetrator (Dermawan, Amalia, & Handoko, 2022).

The rapid development of information technology, including the massive use of the internet, has posed complex challenges for the evolution of the legal system in

Indonesia. National law is required to adapt and respond dynamically to the various social changes that accompany technological advancement. However, in reality, the dynamics of social change in society do not always progress in parallel with the development of the law. In many cases, the law lags behind societal and cultural changes, resulting in regulatory gaps or delays in addressing emerging phenomena such as cybercrime. Cybercrime is a modern form of crime that arises from the use of information technology, particularly the internet, as the primary means of committing unlawful acts. The widespread use of internet services whether in communication, commerce, or information has created opportunities for irresponsible individuals to commit crimes in the digital space. As the number of users and demand for internet access continues to grow, cybercrime is also rapidly evolving, following the pace of technological advancement. This naturally causes significant harm to individuals, groups, and institutions that fall victim to such crimes. The legal system's unpreparedness in regulating and addressing this type of crime may amplify its negative impact. Prior to the enactment of the Law on Electronic Information and Transactions (ITE Law), law enforcement agencies still relied on provisions within the Indonesian Criminal Code (KUHP) to handle various cybercrime cases, even though the KUHP did not specifically regulate crimes involving digital technology (Sumenge, 2013).

Although cybercrime is virtual in nature, it is categorized as a real legal act and offense. Juridically, in the context of cyberspace, it is no longer appropriate to classify something using conventional legal qualifications as an object or action, because doing so would lead to numerous difficulties and allow many offenses to escape legal accountability. Cyber activities are virtual in form but have very real impacts, even though the evidence is electronic in nature. The perpetrators must also be qualified as individuals who have committed actual legal acts (Muhammad & Harefa, 2023).

Cybercrime is one of the modern forms of crime that is now recognized as a new dimension of contemporary criminal acts and has become a serious focus in legal enforcement discourse across many countries, including in international forums. This type of crime not only evolves alongside advancements in information technology, but also displays patterns and characteristics distinct from conventional crimes. Vodymyr Golubev even explicitly refers to cybercrime as *the new form of anti-social behavior* a deviant behavior that not only harms individuals personally but also disrupts the broader social order through the limitless digital world. In various literatures and scholarly studies, cybercrime is often described with different terms that reflect its complexity and broad scope. For instance, the term *cyber space or virtual space offence* is used to emphasize that the crime occurs in a virtual digital space rather than the physical world. Additionally, this type of crime is frequently categorized as a *high tech crime* because the perpetrators utilize sophisticated information technology to carry out their actions. In the context of globalization and international connectivity via the internet, cybercrime is also classified as *transnational crime*, meaning a cross-border crime that requires international cooperation to combat. Furthermore, some experts

categorize it as a new form of *white collar crime*, typically committed by educated individuals or groups with access to advanced technology for personal gain through unlawful means (Akub, 2018).

The regulation of cybercrime is based on the applicable legal sources currently in force, both within the Indonesian Penal Code (KUHP) and laws outside the Penal Code. The regulation of forms of cybercrime in the KUHP can be found in the following articles:

a. Article 362 of the KUHP on theft;
b. Article 369 of the KUHP on extortion and threats;
c. Article 372 of the KUHP on embezzlement;
d. Article 386 of the KUHP on fraudulent acts;
e. Article 506 of the KUHP on public order violations;
f. Article 382 bis of the KUHP;
g. Article 383 of the KUHP. 83 kata (Akub, 2018).

The following are several categories of cybercrime cases addressed in the Law on Electronic Information and Transactions (Articles 27 to 35) (Akub, 2018):

1) Article 27 – Illegal Contents
   - Disseminating immoral content (e.g., pornography).
   - Disseminating gambling content.
   - Committing defamation and insults electronically.
   - Committing extortion and threats via electronic media.
2) Article 28 – Misleading Information & SARA (Ethnicity, Religion, Race, and Intergroup Issues)
   - Disseminating false or misleading news that harms consumers in electronic transactions.
   - Spreading information that incites hatred or hostility based on ethnicity, religion, race, or intergroup relations (SARA).
3) Article 29 – Threat of Violence
   - Sending electronic information containing threats of violence or intimidation directly toward individuals.
4) Article 30 – Illegal Access
   - Illegally accessing someone else's computer or electronic system.
   - Accessing electronic systems to obtain information or documents without permission.
   - Hacking, breaching, or violating electronic security systems unlawfully.
5) Article 31 – Illegal Interception
   - Illegally intercepting information or electronic documents belonging to others.
   - Intercepting non-public electronic data transmissions, either altering or merely reading the data.
6) Article 32 – Data Leakage & Espionage
   - Altering, deleting, damaging, hiding, or transmitting electronic information belonging to others or the public without authorization.

7) Article 33 – System Interference
   - Taking actions that disrupt electronic systems or cause the system to malfunction.

8) Article 34 – Misuse of Devices
   - Creating, selling, distributing, importing, providing, or possessing hardware/software or access codes used for cybercrime.
9) Article 35 – Data Manipulation
   - Manipulating electronic data by altering, deleting, creating, or damaging it to make it appear authentic.

Not only does the Indonesian Criminal Code (KUHP) contain provisions regarding fraud, but there are also other regulations that, in principle, govern cybercrime, namely Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law). This law has been reviewed in relation to factors associated with electronic information and transactions, as well as prohibited actions related to the "cyber world," along with their legal consequences. The ITE Law itself does not explicitly define the meaning of fraud, but fraud in online transactions can be referred to in articles of the ITE Law, such as Article 28 paragraph (1), especially when the elements of a criminal offense are fulfilled. Although Article 28 paragraph (1) of the ITE Law does not specifically regulate the crime of fraud in detail, it is related to the harm experienced by consumers, as stated by Prakoso, Sujana, & Suryani (2020):
"*Without proper authority, disseminating false and misleading news that causes harm to consumers in conducting electronic transactions*."

2. Cybercrime in the Perspective of Islamic Law

Cybercrime is a form of modern crime committed by illegally utilizing computer facilities or networks, either by altering data or not, and includes crimes that use electronic media such as the internet as the primary means, thus categorized as cybercrime. These crimes are generally directed at computer systems or networks and encompass various new forms of violations based on digital technology. From the perspective of Islamic law (*jinayah*), such actions may be subject to *ta'zīr* punishment, which refers to sanctions not specifically prescribed in the Qur'an or Hadith, unlike *ḥudūd*, *qiṣāṣ*, or *kaffārah*. Linguistically, *ta'zīr* means prevention, and terminologically, it is an educational punishment (*ta'dīb*) meant to instill fear (*tankīf*) in order to deter repeated sinful acts. *Ta'zīr* penalties are imposed based on the judge's discretion during the judicial process, and the forms of punishment may include imprisonment, exile, flogging, or even the death penalty, depending on the severity of the harm caused by the cybercrime perpetrator (Suharayadi, Sampar, & Ahmad, 2020).

In Shar'i (Islamic legal) terms, *ta'zīr* refers to a sanction imposed for acts of disobedience (*ma'ṣiyah*) that are not explicitly categorized as crimes in the Qur'an and Hadith, unlike *ḥadd*, *qiṣāṣ*, or *kaffārah*. The types of *ta'zīr* punishments may include:

1) the death penalty;
2) flogging not exceeding ten lashes;
3) exile, boycotting, or imprisonment;
4) crucifixion;
5) compensation (ghurāmah) or confiscation of property;
6) warning or advice;
7) partial deprivation of property rights (ḥurmān);
8) public censure (taubīkh);
9) public exposure (tashhīr). (Naufal & Jannah, 2012)

The forms of *ta'zīr* punishment are limited to those previously mentioned. The caliph, or his representative—the *qāḍī* (judge)—is granted by the Sharia the authority to choose among these forms of punishment and determine their severity; he is not permitted to impose sanctions beyond these forms. In general, *ta'zīr* cases are classified into:

1) violations of personal honor;
2) violations of dignity;
3) acts that corrupt the intellect;
4) violations involving property;
5) breaches of public security;
6) subversive activities;
7) violations related to religion. (Naufal & Jannah, 2012)

Electronic and online media have become alternatives for conducting business transactions, such as e-commerce. Commercial activities carried out through electronic services particularly via the internet, including promotion systems, transaction systems, and payment systems carry significant risks of criminal acts. Without proper caution, fraud can easily occur, and the perpetrators may remain unidentified due to the nature of the business, which lacks face-to-face interaction between parties. Therefore, criminal acts are highly likely to be committed through these electronic media. Such irresponsible behavior by certain individuals can cause substantial harm to the parties involved in the transaction (Suharayadi, Sampar, & Ahmad, 2020).

In Islamic criminal law, cybercrimes such as fraud, immorality, gambling, and extortion/threats are subject to sanctions aligned with sharia principles. Fraud is regarded as a hypocritical act that is deeply reprehensible, even more dangerous than disbelief, as stated in the Qur'an and Hadith. As such, perpetrators may receive punishments equivalent to robbery, including the death penalty or amputation, depending on the severity of the harm caused. Acts of immorality committed in cyberspace are classified as ta'zīr offenses, where the nature of the offense and the corresponding punishment are determined by the authorities, as these are not explicitly regulated in the Qur'an and Hadith. Meanwhile, gambling, equated with the prohibition of alcohol in Al-Ma'idah verse 90, is subject to ḥadd punishment, such as 40 or 80 lashes, depending on the scholarly opinion. Countries like Indonesia have even adopted caning punishments in certain regions as a form of law enforcement deemed just and humane.

As for extortion or threats, these are considered acts akin to robbery, and the perpetrators may face severe penalties such as execution, crucifixion, or amputation. However, in practice, the severity of the punishment may be reduced through judicial processes, including punishments such as flogging, imprisonment, fines, or supervision, as long as the applicable legal requirements are fulfilled (Suharayadi, Sampar, & Ahmad, 2020).

3. Legal Regulation in Indonesia Regarding the Crime of Fraud

The ease with which individuals can use various types of false or incorrect identities to carry out electronic transactions in multiple locations and times without being physically present poses a major challenge for law enforcement in identifying and determining who the actual perpetrator is and where they are located. This creates complexity in the investigation and prosecution process, especially in terms of collecting and verifying valid evidence. Therefore, the existence and admissibility of electronic evidence in Indonesia's criminal justice system has become a crucial topic to be studied and developed, especially after the enactment of Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), which specifically regulates the legal aspects of electronic transactions and digital information. In addition, the rapid development of information technology, including the widespread use of the internet, presents its own challenges to the development of law in Indonesia, which is required to be adaptive and responsive to the ongoing social changes brought about by such technological progress. However, in practice, social change in society and legal change do not always progress simultaneously. In some cases, legal development lags far behind the changes occurring in the social and cultural elements of society, making the law less responsive to new phenomena such as cybercrime. Conversely, under certain conditions, legal change can even precede the existing social developments (Agustini, 2022). Therefore, continuous efforts are needed to harmonize social dynamics with legal development in order to provide optimal protection and justice in this digital era.

The Electronic Information and Transactions Law (ITE Law) specifically regulates several criminal offenses related to cybercrime, such as illegal access as outlined in Article 30 and interference with computer systems in Article 32. In addition, Article 36 of the ITE Law introduces further criminal provisions, stating that any act as regulated in Articles 27 to 34, if committed intentionally, without right, or unlawfully, and causes harm to others, may also be subject to criminal sanctions. However, in practice, if investigators are required to first prove the elements of the criminal act in order to conclude a form of computer-related fraud, this could pose challenges to the effectiveness of law enforcement. Meanwhile, fraud in general is regulated under Article 378 of the Indonesian Penal Code (KUHP), which stipulates that anyone who unlawfully, with the intent to benefit themselves or others, uses a false name, false status, deceit, or a series of lies to persuade someone to surrender goods, give credit, or cancel a debt, can be sentenced to up to four years in prison. However, this provision is more applicable to

conventional fraud in the physical world. In contrast, fraud via the internet falls under a more specific scope as regulated by the ITE Law, particularly relating to the dissemination of false and misleading information through electronic media. In this regard, Article 28 paragraph (1) of the ITE Law states: “Any person who intentionally and without right disseminates false and misleading information that causes harm to consumers in electronic transactions” may be considered a form of digital fraud, though situated within the realm of cyber law (Sumenge, 2013).

The Electronic Information and Transactions Law (ITE Law) not only regulates forms of cybercrime but also imposes severe criminal sanctions on perpetrators of such offenses, as stipulated in Articles 45 through 52. These articles outline prison sentences ranging from six (6) to twelve (12) years, accompanied by substantial fines starting from IDR 600,000,000 (six hundred million rupiah) up to IDR 12,000,000,000 (twelve billion rupiah). These penalties reflect the seriousness of the state in addressing cybercrimes that may cause extensive harm to the public, both materially and morally. Moreover, the ITE Law emphasizes not only the substantive aspects of criminal offenses but also explicitly regulates the formal aspects of law enforcement processes, particularly concerning investigations. Article 42 of the ITE Law stipulates that investigations into criminal offenses under this law must be conducted based on the provisions of Law No. 8 of 1981 on the Criminal Procedure Code (KUHAP), unless otherwise specifically regulated by the ITE Law itself. Thus, the investigative process for violations of the ITE Law must continue to refer to the general principles in KUHAP, except in cases where the ITE Law provides specific provisions, indicating that this law does not stand alone but is part of an integrated national criminal law system (Wahyudi, 2013).

B. Legal Protection for Victims of Online Transactions in the Perspective of Islamic Law

In Islamic teachings, buying and selling fall under the scope of fiqh muamalah and hold an important position as a fundamental part of socio-economic interactions. Islam considers trade as a lawful and legitimate activity, as emphasized in Surah Al-Baqarah verse 275, which states that Allah has permitted trade and prohibited usury (riba). The verse also affirms that those who abandon riba will attain success, while those who persist in it will face the torment of Hell. A similar message is conveyed in Surah An-Nisa verse 2, which forbids people from consuming one another's wealth unjustly, except through mutual trade based on consent from both parties. In a hadith narrated by Ahmad, the Prophet Muhammad (peace be upon him) was asked about the best kind of work, and he responded that the best work is that which a person performs with their own hands and every trade that is free from fraud and betrayal. These teachings reflect Islam’s strong emphasis on justice, honesty, and mutual consent in commercial transactions (Panggabean, 2020).

According to Sinaga as cited in Panggabean (2020), there are several forms of buying and selling that, while technically valid, are prohibited in Islamic law, including the following:

a. Purchasing an item that is still under negotiation by another buyer (khiyar);
b. Intercepting goods on their way to the market and purchasing them en route;
c. Hoarding goods in order to sell them later at a higher price;

d. Engaging in transactions that involve elements of fraud, such as manipulation of quantity, weight, use of counterfeit money, falsification of product authenticity, and similar practices;
e. Setting excessively high prices for goods.

If one or more of the criteria mentioned above are present, then the transaction is deemed unlawful (*haram*). However, if it is free from all five elements, the online sale is considered valid and permissible (*halal*). A closer examination reveals that Islamic law imposes strict requirements on buying and selling practices, which creates a potential for comfort and security for all parties engaging in Islamic-based transactions. This, indeed, reflects the very purpose of Islamic law: to establish a life grounded in honesty and justice (Panggabean, 2020).

Fraud is a deceptive act that is identified as a trait of hypocrisy, as explained in both Hadith and verses of the Qur'an. While there is no explicit textual evidence (*nash*) regulating fraud in the context of cybercrime, digital fraud is still addressed within the Islamic legal framework. Therefore, fraudulent acts conducted through information technology are subject to *ta'zīr* punishment, whereby the judge determines the appropriate penalty based on the severity of the offense. Extortion and threats involve forcibly seizing property without a legitimate transaction and, in practice, resemble robbery or mugging in the physical world. Likewise, violations of decency in the digital space-such as online sexual harassment-constitute new forms of crimes that continue to evolve. These types of offenses typically do not meet the specific criteria for *ḥudūd* punishments under Islamic criminal law, and thus are dealt with through *ta'zīr* punishments, adjusted by legislators and judges according to the circumstances of each case (Zulfahmi, Aulia, Muklis, & Pulungan, 2025).

The response to cybercrime in Islamic law is carried out through the application of *ta'zīr*, which allows for punishments to be tailored to the level of violation, along with the adoption of *restorative justice* principles aimed at restoring the rights of victims. Moreover, the concept of collective responsibility and community-based supervision aligns with the Islamic command to enjoin good and forbid evil (*amar ma'rūf nahī munkar*), while collaboration between the government and faith-based institutions supports effective regulation and digital security systems. Sanctions imposed on perpetrators not only encompass legal dimensions but also include moral and spiritual elements, through the enforcement of sincere repentance (*taubat nasūḥa*) and religious guidance (Zulfahmi, Aulia, Muklis, & Pulungan, 2025).

C. Regulations as the Basis for Law Enforcement Authorities in Combating Fraud in Online Buying and Selling

Online buying and selling, often referred to as e-commerce, has become a daily necessity for urban communities. According to Alimin, online buying and selling is defined as a dynamic set of technologies, applications, and business processes that connect companies, consumers, and specific communities through electronic transactions and the trade of goods, services, and information conducted electronically (Atikah, 2019). The

process of online transactions through e-commerce platforms involves many different parties, including the e-commerce platform provider, buyers, sellers, and delivery services. These parties are interconnected in the online transaction process, and if any of these parties fail to fully meet their responsibilities, the transaction may be halted or fail to take place (Simbolon & Rosando, 2023).

From a legal perspective, e-commerce is a commercial transaction activity that includes several forms such as: negotiated contracts, auctions, advertising, marketing, online payment and settlement, online delivery of goods and services, internet subscription services, commissions (commissions that regulate between several websites), shopping sites, and tenders. It can be concluded that e-commerce opens up many business opportunities, ranging from the procurement of goods and services, agency, leasing, investment, finance, banking, to the field of transportation business (Mawarni, 2016).

One of the legal foundations used by law enforcement authorities in handling fraud in online buying and selling is stipulated in Law Number 8 of 1999 concerning Consumer Protection, which in Article 1 paragraph (1) states that consumer protection is all efforts aimed at ensuring legal certainty in protecting consumers' rights. This legal protection is provided so that the public can enjoy their rights without being harmed by other parties, covering the entire process from obtaining to using goods or services, including addressing the impacts arising from such transactions (Habeahan & Tamba, 2021).

In the effort to realize the principles of the rule of law in society and the state, the role and function of law enforcement officers as a free, independent, and responsible profession is essential, alongside the judiciary and other law enforcement institutions. In carrying out their duties, law enforcement officers must comply with fundamental norms in legal enforcement, namely: humanity, justice, propriety, and honesty. In addition to these principles, law enforcement officers must also adhere to the professional code of ethics as appropriate (Sinaga, 2020).

Abdulkadir Muhammad, as cited in Rahmanto (2019), stated that "*law enforcement can be defined as an effort to implement the law properly, to supervise its implementation in order to prevent violations, and if violations occur, to restore the violated law so that it can be upheld again.*"

The handling of online fraud crimes needs to be carried out through two main approaches, namely preventive and repressive approaches, as stated by Bambang Waluyo in Rahmad (2019). The preventive approach aims to prevent criminal acts early, by taking proactive steps before the crime actually occurs. These measures may include public education through outreach programs, legal awareness campaigns, and the dissemination of relevant information via various media platforms, both print, electronic, and digital. Media here functions not only as an information channel but also as a strategic learning tool to enhance public legal literacy, especially regarding laws in the field of Information and Electronic Transactions (ITE), so that the public is not easily deceived by online fraud. In addition, strong synergy and coordination are needed between law enforcement agencies and related institutions in formulating a legal framework that is responsive to the dynamics of cybercrime. On the other hand, the repressive approach is reactive, carried out after a

criminal act has occurred. In this context, law enforcement is responsible for following up on every report or complaint from the public regarding online fraud by conducting investigations, inquiries, and prosecution of the perpetrators. This firm action must be accompanied by the imposition of legal sanctions in accordance with the provisions of the applicable laws, as a form of protection for victims and to create a deterrent effect for the offenders. Thus, in addition to enforcing the law fairly, the repressive approach also aims to create a sense of security in society and restore public trust in the existing legal system (Rahmad, 2019).

The use of criminal law as a means of preventing and combating cybercrime is highly relevant, considering the dangers and losses that may arise from the increasing risks associated with the development of information technology. Criminal law is called upon to remedy the harm suffered by society, as such crimes can disrupt the socio-economic activities of the public. As part of efforts to combat online fraud and to protect public interests, criminal law is essential in addressing cybercrime issues—even before such crimes occur. Barda Nawawi explains that in order to prevent a criminal offense, the main target is to address the conducive factors that lead to the crime. These factors are centered around social issues or conditions that directly or indirectly may cause or promote criminal behavior. Thus, from the perspective of criminal policy, preventive efforts occupy a key position and strategy within the overall framework of criminal policy (Amelia, 2023).

Basically, each party involved in electronic transactions has their own rights and obligations. The seller (merchant) is the party who offers products through the internet; therefore, a seller is obliged to provide accurate and honest information about the products being offered to the buyer or consumer. The seller/business actor has the right to receive payment from the buyer/consumer for the goods sold, and also has the right to obtain protection against actions by buyers/consumers who act in bad faith in carrying out transactions through electronic commerce (Putra, 2014).

Various parties, including the government, the police, and online marketplace providers/managers, have made efforts to prevent and address fraudulent acts that may occur on online shopping platforms. In terms of regulation, Indonesia has established a comprehensive legal framework through the Electronic Information and Transactions Law (ITE Law), the Consumer Protection Law (CPL), the Trade Law, and Government Regulation No. 82 of 2012 concerning the Implementation of Electronic Systems and Transactions (Solim, Rumapea, Wijaya, Manurung, & Lionggodinata, 2019). Online buying and selling transactions or e-commerce are regulated under Law No. 11 of 2008 in conjunction with Law No. 19 of 2016 concerning Electronic Information and Transactions, as well as in Government Regulation No. 82 of 2012 on the Implementation of Electronic Systems and Transactions (Nugroho & Yuniarlin, 2020).

Efforts to protect victims of online fraud conducted by the Surabaya Metropolitan Police (Polrestabes Surabaya) include two forms of legal protection: preventive and repressive. Preventive efforts are carried out through education about fraud schemes on social media, dissemination of information regarding the ITE Law and the Criminal Code

(KUHP), as well as the provision of tools to track online fraud perpetrators, although there are still limitations in terms of IT human resources. Meanwhile, repressive protection is implemented through legal action after the crime has occurred, including providing access for reporting both online and offline, and the application of legal provisions such as Article 378 of the Criminal Code and Article 28 paragraph (1) of the ITE Law. Although each article has a different scope, both can be used complementarily in handling online fraud cases, especially if the criminal elements can be legally proven (Zulkifli, 2021).

In providing legal protection for consumers in e-commerce transactions, Arief & Elisatris G divide it into four main aspects: business actors, consumers, products, and transactions. Business actors hold a stronger position because they provide the products, and therefore must include clear identification, business address, and official permits. Consumers, on the other hand, must be guaranteed that their personal data will not be misused. The products offered must be accompanied by complete, easily understood, and accurate information. Meanwhile, in the transaction process, business actors must clearly state the terms of the transaction, including price, tax, shipping cost, delivery system, and guarantees for returns or refunds, as well as provide a transparent dispute resolution mechanism. All of these provisions should be regulated in an agreement or contract between the consumer and the business actor to ensure legal certainty (Susanti, 2017).

Conclusion

Legal protection for victims of fraud in online buying and selling transactions is crucial amid the rising prevalence of digital crimes. From both Indonesian legal and Islamic perspectives, this protection can be implemented through penal (repressive) and non-penal (preventive) approaches. Penal measures grant victims the right to report fraud to law enforcement officials so that perpetrators can be sanctioned according to the applicable criminal provisions in the Indonesian Criminal Code (KUHP) and the Electronic Information and Transactions Law (UU ITE), as well as reviewed under *ta'zīr* sanctions in Islamic law. The non-penal approach focuses on raising public awareness through legal education and digital literacy to make people more cautious and less susceptible to deception in online trading activities. Although regulations exist, their implementation still faces obstacles such as limited supporting facilities, low public legal awareness, and weak responses from law enforcement officers. From an Islamic viewpoint, protection of victims is also part of social justice, making it the state's duty to uphold justice and prevent recurrence of similar crimes. Therefore, collaboration between the government, law enforcement, and the community is essential to create a fair, secure, and Sharia-compliant online transaction system.

References

Agustini, S. (2022). Pengaturan hukum di Indonesia terhadap tindak pidana penipuan cyberlaw. *Ensiklopedia Education Review*, 4(3), 303–308. https://jurnal.ensiklopediaku.org/ojs-2.4.8-3/index.php/education/article/view/1587

Akub, M. S. (2018). Pengaturan tindak pidana mayantara (cyber crime) dalam sistem hukum Indonesia. *Al-Ishlah: Jurnal Ilmiah Hukum*, 21(2), 85–93. https://jurnal.fh.umi.ac.id/index.php/ishlah/article/download/19/17

Amelia, A. (2023). Kajian hukum terhadap tindak pidana penipuan secara online. *Jurnal Inovasi Global*, 1(1), 14–25. https://jig.rivierapublishing.id/index.php/rv/article/download/3/5

Atikah, I. (2019). Pengaturan hukum transaksi jual beli online (e-commerce) di era teknologi. *Muamalatuna*, 10(2), 1–27. https://www.researchgate.net/profile/Ika-Atikah-2/publication/345406258_PENGATURAN_HUKUM_TRANSAKSI_JUAL_BELI_ONLINE_E-COMMERCE_DI_ERA_TEKNOLOGI/links/63036d44e3c7de4c34765288/PENGATURAN-HUKUM-TRANSAKSI-JUAL-BELI-ONLINE-E-COMMERCE-DI-ERA-TEKNOLOGI.pdf

Bastari, R. G., Junaidi, A., & Ismiyanto, I. (2024). Perlindungan hukum terhadap tindak pidana penipuan dalam situs jual beli online di Indonesia. *Ranah Research: Journal of Multidisciplinary Research and Development*, 7(1), 287–294. https://www.jurnal.ranahresearch.com/index.php/R2J/article/download/1226/1075

Dermawan, A., Amalia, A., & Handoko, W. H. (2022). Pencegahan tindak pidana penipuan jual beli barang online. *Jurnal Bangun Abdimas*, 1(1), 13–20. http://ejurnal.bangunharapanbangsa.com/index.php/abdimas/article/download/5/4

Fitrianingrum, A., Shahrullah, R. S., & Syarief, E. (2016). Legal approaches to online arbitration: Opportunities and challenges in Indonesia. *Mimbar Hukum-Fakultas Hukum Universitas Gadjah Mada*, 28(2), 314–321. https://journal.ugm.ac.id/jmh/article/download/16724/11025

Gunawan, R., Aulia, S., Supeno, H., Wijanarko, A., Uwiringiyimana, J. P., & Mahayana, D. (2021). Adiksi media sosial dan gadget bagi pengguna internet di Indonesia. *Techno-Socio Ekonomika*, 14(1), 1–14. https://jurnal.usbypkp.ac.id/index.php/techno-socio-ekonomika/article/download/544/309

Habeahan, B., & Tamba, A. R. (2021). Perlindungan hukum pembeli dalam perjanjian jual beli melalui sistem elektronik. *Nommensen Journal of Legal Opinion*, 47–54. https://ejournal.uhn.ac.id/index.php/opinion/article/download/208/335

Indrawan, M., & Permatasari, P. (2022). Perlindungan hukum korban penipuan transaksi jual beli online melalui ganti rugi. *Jurnal Kewarganegaraan*, 6(3), 6487–6494. https://journal.upy.ac.id/index.php/pkn/article/download/4157/2630

Kamran, M., & Maskun, M. (2021). Penipuan dalam jual beli online: Perspektif hukum telematika. *Balobe Law Journal*, 1(1), 41–56. https://fhukum.unpatti.ac.id/jurnal/balobe/article/viewFile/501/267

Maskun, S. H., dkk. (2020). *Korelasi kejahatan siber dan kejahatan agresi dalam perkembangan hukum internasional* (Cetakan pertama). CV. Nas Media Pustaka.https://repository.unhas.ac.id/id/eprint/4229/1/Buku%20Wajib.pdf

Mawarni, R. (2016). Perlindungan hukum bagi para pihak dalam transaksi e-commerce melalui Facebook. *PROGRESIF: Jurnal Hukum*, 10(1). https://www.journal.ubb.ac.id/progresif/article/download/180/162

Mezak, M. H. (2006). Jenis, metode dan pendekatan dalam penelitian hukum. *Ltiw Review. Fakultas Hukum Universiius Pelita Harapan*, 5(3). https://www.academia.edu/download/33676150/lw-05-03-2006-jenis_metode_dan_pendekatan.pdf

Muhammad, F. E., & Harefa, B. (2023). Pengaturan tindak pidana bagi pelaku penipuan phishing berbasis web. *Jurnal USM Law Review*, 6(1), 226–241. https://pdfs.semanticscholar.org/ca75/9e2ecca40cb873f97f8c3368b6d344c8ff54.pdf

Naufal, M. M., & Jannah, H. S. (2012). Penegakan Hukum Cyber Crime Ditinjau Dari Hukum Positif Dan Hukum Islam. *Al-Mawarid Journal of Islamic Law*, *12*(1), 42565. https://www.academia.edu/download/56615294/42565-ID-penegakan-hukum-cyber-crime-ditinjau-dari-hukum-positif-dan-hukum-islam.pdf

Nugroho, R. A., & Yuniarlin, P. (2021). Pelaksanaan jual beli secara online berdasarkan perspektif hukum perdata. *Media of Law and Sharia*, 2(2), 190–206. https://journal.umy.ac.id/index.php/mlsj/article/download/11488/6280

Panggabean, S. A., & Tanjung, A. (2022). Jual Beli Online dalam Perspektif Hukum Islam dan Hukum Negara. *Jesya (Jurnal Ekonomi dan Ekonomi Syariah)*, *5*(2), 1504-1511. https://stiealwashliyahsibolga.ac.id/jurnal/index.php/jesya/article/download/758/412

Prakoso, B. A. D., Sujana, I. N., & Suryani, L. P. (2020). Perlindungan hukum terhadap korban penipuan jual beli online. *Jurnal Konstruksi Hukum*, 1(2), 266–270. https://ejournal.warmadewa.ac.id/index.php/jukonhum/article/download/2591/1850

Primayoga, A. M., Saptono, H., & Njatrijani, R. (2019). Perlindungan hukum terhadap konsumen yang menerima barang tidak sesuai pesanan dalam transaksi jual beli online. *Diponegoro Law Journal*, 8(3), 1732–1743. https://ejournal3.undip.ac.id/index.php/dlr/article/download/24558/23375

Putra, S. (2014). Perlindungan hukum terhadap konsumen dalam transaksi jual-beli melalui e-commerce. *Jurnal Ilmu Hukum Riau*, 4(2), 91–64. https://www.neliti.com/publications/9164/perlindungan-hukum-terhadap-konsumen-

dalam-transaksi-jual-beli-melalui-e-commerc

Puspitasari, R. J., & Sulistyo, A. Q. P. (2024). Perlindungan hukum bagi korban penipuan online shop dengan merujuk pada Undang-Undang Nomor 19 Tahun 2016. *Eksaminasi: Jurnal Hukum*, 3(2), 53–60. https://jurnal.umpwr.ac.id/index.php/eksaminasi/article/download/2088/1213

Rahmad, N. (2019). Kajian hukum terhadap tindak pidana penipuan secara online. *Jurnal Hukum Ekonomi Syariah*, 3(2), 103–117. https://core.ac.uk/download/pdf/275932358.pdf

Rahmanto, T. Y., Kav, J. H. R. S., & Kuningan, J. S. (2019). Penegakan hukum terhadap tindak pidana penipuan berbasis transaksi elektronik. *Jurnal Penelitian Hukum De Jure*, 19(1), 31. https://www.academia.edu/download/86005712/pdf_1.pdf

Rosadi, S. D. (2018). Protecting privacy on personal data in digital economic era: Legal framework in Indonesia. *Brawijaya Law Journal*, 5(1), 143–157. https://www.academia.edu/download/86857253/pdf.pdf

Simbolon, F. A., & Rosando, A. F. (2023). Bentuk perlindungan hukum bagi pelaku usaha online dalam retur barang sistem cash on delivery (COD). *Innovative: Journal Of Social Science Research*, 3(6), 10509–10526. https://j-innovative.org/index.php/Innovative/article/download/6541/5506

Sinaga, N. A. (2020). Kode etik sebagai pedoman pelaksanaan profesi hukum yang baik. *Jurnal Ilmiah Hukum Dirgantara*, 10(2). https://journal.universitassuryadarma.ac.id/index.php/jihd/article/viewFile/460/676

Solim, J., Rumapea, M. S., Wijaya, A., Manurung, B. M., & Lionggodinata, W. (2019). Upaya penanggulangan tindak pidana penipuan situs jual beli online di Indonesia. *Jurnal Hukum Samudra Keadilan*, 14(1), 96–109. https://ejurnalunsam.id/index.php/jhsk/article/download/1157/1054

Suharyadi, S., Sampara, S., & Ahmad, K. (2020). Kejahatan Dunia Maya (Cyber Crime) Dalam Prespektif Hukum Islam. *Journal of Lex Generalis (JLG)*, *1*(5), 761-773. https://pasca-umi.ac.id/index.php/jlg/article/download/199/228

Sumenge, M. (2013). Penipuan menggunakan media internet berupa jual-beli online. *Lex Crimen*, 2(4). https://ejournal.unsrat.ac.id/index.php/lexcrimen/article/download/3093/2637

Susanti, I. (2017). Tinjauan yuridis terhadap perlindungan konsumen belanja online berdasarkan UU No. 8 Tahun 1999 tentang perlindungan konsumen juncto UU No. 11 Tahun 2008 tentang informasi dan transaksi elektronik. *Sigma-Mu*, 9(1), 19–32. https://jurnal.polban.ac.id/sigmamu/article/view/966/801

Wahyudi, D. (2013). Perlindungan hukum terhadap korban kejahatan cyber crime di Indonesia. *Jurnal Ilmu Hukum Jambi*, 4(1), 43–295.

https://www.neliti.com/publications/43295/perlindungan-hukum-terhadap-korban-kejahatan-cyber-crime-di-indonesia

Zulfahmi, Aulia, P., Muklis, M., & Pulungan, R. (2025). Perbandingan Perspektif Hukum Pencegahan Kejahatan Dunia Maya Dalam Hukum Positif Dan Hukum Pidana Islam. *Jurnal El-Thawalib*, *6*(2). https://www.researchgate.net/profile/Zulfahmi-Zulfahmi-8/publication/390525042_Perbandingan_Perspektif_Hukum_Pencegahan_Kejahatan_Dunia_Maya_dalam_Hukum_Positif_dan_Hukum_Pidana_Islam/links/67f19ab795231d5ba5b559db/Perbandingan-Perspektif-Hukum-Pencegahan-Kejahatan-Dunia-Maya-dalam-Hukum-Positif-dan-Hukum-Pidana-Islam.pdf

Zulkifli, N. F. R. (2021). Perlindungan hukum terhadap korban penipuan jual beli online pada masa pandemi Covid-19 di Polrestabes Surabaya. *Jurnal Syntax Transformation*, 2(5), 638–649. http://jurnal.syntaxtransformation.co.id/index.php/jst/article/download/276/416