MUSABAB
Journal of Islamic Law and Social Practice
Homepage: http://journal.shafiyyah.org/index.php/musabab Volume 1, Issue 1, 2025

Analysis of Judges' Considerations in Imposing Sanctions for Online Fraud: A Study of Positive and Islamic Criminal Law

Rahmi Ainaul Mardiah, Ahmatnijar, Nurhotia Harahap
Universitas Syekh Ali Hasan Ahmad Addary Padangsidimpuan, Indonesia

Article Information

Article history:
Received October 21, 2024
Revised January 30, 2025
Accepted February 28, 2025

Keywords

Online fraud;
Criminal law;
Tadlis;
Digital transaction security.

Correspondence

Rahmi Ainaul Mardiah

Universitas Syekh Ali Hasan Ahmad Addary Padangsidimpuan, Indonesia

E-mail: rahmiaina7@gmail.com

A B S T R A C T

This study aims to analyze judicial decisions in online fraud cases and evaluate the effectiveness of regulations used to prosecute cybercrime perpetrators. Using a normative juridical research method, this study focuses on legal analysis of the decision of the West Jakarta District Court Number: 1074/Pid.B/2020/PN.Jkt.Brt and a comparative study between Article 378 of the Indonesian Criminal Code (KUHP) and Article 28(1) of the Electronic Information and Transactions Law (UU ITE). The results indicate that the application of Article 378 KUHP in online fraud cases has weaknesses, as it does not fully reflect the complexity of digital crimes. In contrast, Article 28(1) of UU ITE is considered more relevant, as it specifically regulates the dissemination of false information that harms consumers. From an Islamic law perspective, online fraud can be categorized as *tadlis*, which may be subject to *ta'zir* sanctions at the judge's discretion. This study also finds that victim protection remains suboptimal, necessitating regulatory improvements and increased digital literacy among the public. The conclusion of this study emphasizes the need for reform in Indonesia's criminal law system to address online fraud cases by updating legal provisions to be more adaptive to technological developments. With stronger regulations and more effective law enforcement, online fraud cases can be minimized, fostering a safer digital transaction ecosystem for society.

1. Introduction

The advancement of information and communication technology has brought significant changes to various aspects of life, including the trade sector. One of the most notable impacts of this progress is the increasing popularity of online transactions, which offer convenience for people in obtaining goods and services. E-commerce platforms, social media, and instant messaging applications have become the primary means of digital commercial transactions. However, alongside this convenience, various legal issues have emerged, particularly those related to cybercrime, one of which is fraud in online transactions. This type of fraud frequently occurs due to weak oversight and low legal awareness among consumers, resulting in substantial economic losses. Additionally, legal uncertainty in handling such cases further complicates dispute resolution.

In legal terms, fraud is regulated under Article 378 of the Indonesian Criminal Code (KUHP), which states that anyone who, with the intent to unlawfully benefit themselves or others, deceives through fraudulent acts or false pretenses, may be subject to criminal sanctions. Furthermore, in the digital era, such crimes are also governed by Law No. 11 of 2008 concerning Electronic Information and Transactions (UU ITE), particularly Article 28(1), which regulates the dissemination of false information that harms consumers in electronic transactions. Although these regulations have been enacted, law enforcement against online fraud cases still faces numerous challenges, particularly in determining the most appropriate legal provisions to prosecute offenders. Differences in the interpretation of these laws often lead to inconsistencies in the legal system, resulting in varied sanctions for similar offenses.

One case that has drawn attention is the ruling of the West Jakarta District Court, Case Number: 1074/Pid.B/2020/PN.Jkt.Brt, in which the defendant, Dian Sarasah, was found guilty of online fraud by offering facial masks for sale but failing to deliver the purchased items. The court based its decision on Article 378 of the Criminal Code, sentencing the defendant to one year of imprisonment. However, this verdict has sparked debates regarding whether the imposed sanction truly reflects justice and whether Article 378 of the Criminal Code remains relevant in addressing digital-era crimes. Some legal experts argue that Article 28(1) of the UU ITE is more appropriate in such cases, as it specifically addresses the dissemination of misleading information that causes harm to victims.

Beyond the perspective of Indonesia's positive law, fraud cases can also be analyzed within the framework of Islamic criminal law. In Islam, fraud is known as *tadlis*, which refers to deception in transactions. Islamic criminal law does not specify fixed sanctions for fraud but entrusts the punishment to the discretion of the judge under the concept of *ta'zir*. In this context, it is relevant to examine how *ta'zir* in Islam compares to the sanctions imposed under positive law. In several cases, *ta'zir* provides broader flexibility for judges to consider the impact of the crime on victims and society, thereby allowing for penalties that align more closely with the principles of substantive justice.

Various studies have been conducted to examine the legal aspects of fraud in online commercial transactions. In general, these studies can be categorized into four main themes relevant to this research: the analysis of judicial decisions and legal considerations in online fraud cases, legal protection for consumers and fraud prevention efforts, the Islamic legal perspective on online fraud, and regulations and legal policies for combating cybercrime.

Several studies have explored the legal considerations judges use when imposing sanctions on online fraud perpetrators. For instance, research by Anggela et al. (2022) and Dirman & Cornelis (2024) discusses how judges apply Article 378 of the Indonesian Criminal Code (KUHP) and Article 28(1) of the Electronic Information and Transactions Law (UU ITE) to assess the legal elements of online fraud cases. Hanifiyah (2022) and Ilham (2023) further analyze how judicial considerations in various rulings differ in applying sanctions for cybercriminals. Meanwhile, Ilhamsyah (2023) and Rizwan (2019) compare the application of sanctions in positive criminal law and Islamic law, highlighting the flexibility of the *ta'zir* concept in Islamic law compared to conventional legal systems. These studies indicate that discrepancies in judicial approaches persist in handling online fraud cases, raising concerns about the effectiveness of current regulations in providing optimal legal protection for victims.

Additionally, legal protection for victims of online fraud and crime prevention efforts have been significant areas of focus in various studies. Dermawan et al. (2022) emphasize the importance of public education in raising awareness about online fraud schemes as part of prevention strategies. Research by Hamzah et al. (2019), along with Kakoe et al. (2020), underscores the importance of compensation as a legal mechanism to protect victims. Studies by Puspitasari & Sulistyo (2024) and Zulkifli (2021) reveal that current legal policies do not fully ensure effective protection for online fraud victims, highlighting the need for legal system reforms to enhance restitution and compensation mechanisms.

From an Islamic legal perspective, fraud in online commercial transactions can be categorized as *tadlis*, a deceptive practice that contradicts the principles of transparency and honesty in trade. Several studies, such as those by Al-Khālidī (2024) and Handayani & Zahara (2024), examine how *tadlis* in e-commerce can be assessed within the framework of DSN-MUI fatwas and shariah-based regulations. Research by Ilhamsyah (2023), Rizwan (2019), and Ronisah (2023) compares sanctions in Islamic law with those in positive law, demonstrating that *ta'zir* offers greater flexibility in determining punishments based on the social and economic impact of the crime. Additionally, Safitri (2016) and Sukmayanti (2021) emphasize that the principle of *hisbah* in Islam can be implemented in digital monitoring systems to prevent fraud in online transactions. These studies suggest that Islamic law provides more adaptive mechanisms for handling online fraud, which could be considered in developing a more substantively just legal framework.

In terms of regulations and legal policies for combating cybercrime, several studies highlight the need for legal reforms to address the increasing complexity of digital crime methods. Fauzi (2018) and Kamran & Maskun (2021) assess the effectiveness of Article 378 of the KUHP in dealing with online fraud cases, demonstrating that this regulation is not sufficiently responsive to digital technology advancements. Research by Kurniawan et al. (2020) and Saleh (2022) also highlights the need to revise existing regulations to align with the challenges of the digital era. Mann (2025) explores how cyber law provisions can be misused in online fraud cases, while Munik et al. (2023) and Pramesti & Rosnawati (2023) examine the factors influencing law enforcement effectiveness in prosecuting cybercriminals. Meanwhile, research by Sari et al. (2022) discusses online fraud from a criminological perspective, emphasizing how technology has altered crime patterns and legal accountability mechanisms for offenders.

Based on these previous studies, it is evident that research on online fraud in e-commerce transactions still faces several challenges in terms of regulations, victim protection, and law enforcement effectiveness. This study seeks to address these gaps by conducting a more in-depth analysis of judicial considerations in sentencing online fraud perpetrators from the perspectives of both positive criminal law and Islamic law. By comparing these two legal systems, this research aims to provide a more comprehensive understanding of the effectiveness of existing regulations and offer recommendations for legal reforms to enhance victim protection and reduce cybercrime rates in the future.

This study seeks to fill this gap by analyzing the judicial ruling in Case Number 1074/Pid.B/2020/PN.Jkt.Brt from two legal perspectives: Indonesia's positive criminal law and Islamic criminal law. By doing so, this research offers a more holistic approach to understanding judicial considerations in online fraud cases while evaluating the extent to which imposed sanctions align with the principles of justice in both legal systems. Additionally, this study aims to provide recommendations for more effective regulatory measures to combat online fraud, ensuring both deterrence for perpetrators and maximum protection for victims. By comparing these two legal frameworks, the study aspires to offer more effective and comprehensive solutions for addressing cybercrime in Indonesia.

Based on the background and previous research, this study is driven by the main question: Do judicial considerations in imposing sanctions on online fraud perpetrators in Case Number 1074/Pid.B/2020/PN.Jkt.Brt align with the principles of justice in both Indonesia's positive law and Islamic criminal law? Furthermore, this study explores whether Article 378 of the Criminal Code is the appropriate legal instrument for prosecuting digital crimes, or whether Article 28(1) of the UU ITE is more relevant for handling online fraud cases.

The primary objective of this study is to analyze and evaluate judicial considerations in imposing sanctions on online fraud perpetrators from the perspectives of both Indonesia's positive criminal law and Islamic criminal law. Specifically, this study aims to: (1) examine the legal basis used in the ruling of Case Number 1074/Pid.B/2020/PN.Jkt.Brt; (2) identify the strengths and weaknesses of applying Article 378 of the Criminal Code in handling online fraud cases; (3) compare sanctions under positive law and Islamic law, particularly in the context of *ta'zir*; and (4) provide legal policy recommendations for more effective measures in addressing online fraud cases in the future.

Through this analysis, it is hoped that the findings will contribute to the development of legal scholarship, particularly in refining regulations related to cybercrime and providing insights for law enforcement officials in applying sanctions that are fairer and more effective for perpetrators of online transaction fraud.

2. Method

This study employs a normative legal approach using the normative juridical research method (Christiani, 2016). Normative juridical research is a method that focuses on examining existing legal norms by analyzing primary and secondary legal materials (Sudrajat, 2022). The primary legal materials in this study include statutory regulations related to online fraud offenses, such as Article 378 of the Indonesian Criminal Code (KUHP) and Article 28(1) of the Electronic Information and Transactions Law (UU ITE), as well as the decision of the West Jakarta District Court Number: 1074/Pid.B/2020/PN.Jkt.Brt. Meanwhile, secondary legal materials consist of books, scholarly journals, and articles related to positive criminal law and Islamic law. This normative approach is relevant for understanding how legal regulations are applied in handling online fraud cases from both national law and Islamic law perspectives.

The data collection technique in this research is conducted through a literature study, which involves analyzing legal documents, academic literature, and relevant court decisions. The collected data is then analyzed using a descriptive-analytical method, where the research findings are systematically interpreted to derive a comprehensive conclusion. This approach enables the study to provide a deeper understanding of judicial considerations in online fraud cases and compare their application in positive law and Islamic law. Furthermore, the descriptive-analytical method helps identify the strengths and weaknesses of existing regulations and offers recommendations for improving legal policies related to cybercrime in Indonesia.

In addition to the normative approach, this study also conducts a comparative analysis between Indonesia's positive legal system and Islamic criminal law in addressing online fraud cases. By utilizing a comparative analysis technique, this research explores how different legal systems handle similar cases and evaluates the effectiveness of each approach. The results of this comparison are expected to provide insights for policymakers and law enforcement authorities in designing regulations that are more aligned with the needs of modern society. Thus, this study not only aims to understand the application of existing legal provisions but also seeks to offer solutions to the challenges faced in enforcing laws related to online fraud.

The normative juridical research method primarily examines legal norms by analyzing primary and secondary legal materials. Primary legal materials in this study include statutory regulations concerning online fraud, such as Article 378 of the Criminal Code and Article 28(1) of the UU ITE, as well as the West Jakarta District Court Decision Number: 1074/Pid.B/2020/PN.Jkt.Brt. Secondary legal materials comprise books, academic journals, and articles related to positive criminal law and Islamic law.

The data collection technique in this research is conducted through a literature study, involving the analysis of legal documents, academic literature, and relevant court rulings. The collected data is then analyzed using a descriptive-analytical method, allowing the research findings to be systematically interpreted to reach a comprehensive conclusion. This approach enables the study to offer a deeper insight into judicial considerations in online fraud cases while comparing their implementation in positive law and Islamic law.

3. Results and Discussion

3.1 Analysis of the Judge's Ruling in an Online Fraud Case

The decision of the West Jakarta District Court Number: 1074/Pid.B/2020/PN.Jkt.Brt declared that the defendant, Dian Sarasah, was legally and convincingly proven to have committed online fraud. The judge sentenced the defendant to one year in prison, considering various legal aspects, including the fulfillment of the elements outlined in Article 378 of the Indonesian Criminal Code (KUHP). The elements considered include fraudulent acts, unlawful financial gain, and the use of deception in transactions. During the trial, the defendant admitted that she did not deliver the goods that had been paid for by the victim, thereby fulfilling the elements of fraud as stipulated in the KUHP.

The judge's considerations in imposing sanctions on the defendant encompassed various legal and social aspects. One of the main factors was the impact on the victim, who suffered financial losses and lost trust in the online transaction system. Additionally, the judge considered that the defendant's criminal actions could harm the growing e-commerce industry in Indonesia. Mitigating factors in this ruling included the defendant's cooperative attitude during the trial, admission of guilt, and lack of prior criminal records. On the other hand, aggravating factors included the significant financial loss incurred and the negative impact on public trust in online transactions.

A comparison between the prosecutor's demands and the judge's ruling revealed differences in their perspectives on sentencing. The public prosecutor initially demanded that the defendant be sentenced to one year and six months in prison. However, the judge imposed a lighter sentence, taking into account the social and psychological aspects of the defendant. The judge determined that a one-year sentence was sufficient to serve as a deterrent while also sending a clear message to the public that online fraud remains a serious crime subject to strict legal sanctions.

Another factor considered by the judge was the level of culpability of the defendant in terms of intent and motive. During the trial, it was revealed that the defendant was not a repeat offender and committed the act due to economic difficulties. This served as an additional factor in reducing the sentence. However, the judge also emphasized that despite the defendant's difficult circumstances, her actions still constituted a crime that harmed the victim, and thus, a prison sentence was necessary to uphold justice.

From a criminal law perspective, this ruling has sparked debates regarding whether the application of Article 378 of the KUHP is effective in addressing digital fraud cases. This article was originally designed to handle conventional crimes, whereas online transactions have different characteristics, including the anonymity of perpetrators and the challenges in proving fraudulent intent. Therefore, some legal experts argue that Article 28(1) of the Electronic Information and Transactions Law (UU ITE) should have been used in this case, as it is more relevant to cybercrime methods.

The impact of this ruling on the victim also warrants attention. Although the defendant was sentenced to prison, the victim still suffered financial losses that may not be fully recovered. Thus, it is essential to consider additional sanctions such as restitution or compensation to help victims regain their losses. In several similar cases in other countries, judicial systems allow victims to receive compensation from perpetrators as part of the court's ruling.

From a legal policy standpoint, this ruling highlights the need for regulatory reforms in addressing cybercrime. With the increasing number of online fraud cases, the legal system requires updates to adapt to new technological challenges. This includes revisions to the KUHP and strengthening regulations within the UU ITE to provide better protection for victims and impose more effective sanctions on cybercriminals.

Overall, the ruling in the Dian Sarasah case illustrates the complexity of handling online fraud crimes. While the imposed sentence is considered fair within the context of conventional criminal law, there is still room for improvement in the broader legal system to accommodate technological advancements and new enforcement challenges. Therefore, further evaluation of existing regulations and potential legislative reforms is a crucial step that must be undertaken.

The judge sentenced the defendant to one year in prison, considering various legal aspects, including the fulfillment of the elements outlined in Article 378 of the KUHP. The elements considered include fraudulent acts, unlawful financial gain, and the use of deception in transactions. During the trial, the defendant admitted that she did not deliver the goods that had been paid for by the victim, thereby fulfilling the elements of fraud as stipulated in the KUHP.

The judge's considerations in imposing sanctions on the defendant encompassed various legal and social aspects. One of the main factors was the impact on the victim, who suffered financial losses and lost trust in the online transaction system. Additionally, the judge considered that the defendant's criminal actions could harm the growing e-commerce industry in Indonesia. Mitigating factors in this ruling included the defendant's cooperative attitude during the trial, admission of guilt, and lack of prior criminal records (Widhaningroem & Widowaty, 2024). On the other hand, aggravating factors included the significant financial loss incurred and the negative impact on public trust in online transactions.

A comparison between the prosecutor's demands and the judge's ruling revealed differences in their perspectives on sentencing. The public prosecutor initially demanded that the defendant be sentenced to one year and six months in prison. However, the judge imposed a lighter sentence, taking into account the social and psychological aspects of the defendant. The judge determined that a one-year sentence was sufficient to serve as a deterrent while also sending a clear message to the public that online fraud remains a serious crime subject to strict legal sanctions.

3.2 Evaluation of the Application of Article 378 of the Indonesian Criminal Code (KUHP) in Online Fraud Cases

Article 378 of the Indonesian Criminal Code (KUHP) is frequently used in handling fraud cases, including those involving online transactions. However, the effectiveness of this article in addressing cybercrime remains a subject of debate. One advantage of Article 378 KUHP is its broad scope, which can accommodate various forms of fraud. However, a significant weakness of this article is its inadequacy in addressing digital-based crimes, given that online fraud has distinct characteristics compared to conventional fraud.

In the context of modern law, the application of Article 378 KUHP to online fraud is considered less relevant as it does not specifically regulate the use of technology in criminal activities. For instance, cybercrimes often involve the dissemination of false information through digital media, which is not entirely covered by the provisions of the KUHP. Therefore, in several cases, the use of the Electronic Information and Transactions Law (UU ITE), particularly Article 28(1), is deemed more appropriate for handling digital fraud cases.

Another challenge in applying Article 378 KUHP in online fraud cases is the difficulty in proving criminal elements in electronic transactions. In many cases, cybercriminals use anonymity techniques that make it difficult for law enforcement authorities to identify them. Additionally, victims often struggle to file reports due to a lack of understanding of the available legal mechanisms. This highlights the need for a more comprehensive approach to handling online fraud, considering technological aspects and more sophisticated investigative methods.

From a juridical perspective, Article 378 KUHP is still based on a conventional criminal law model that does not specifically anticipate developments in information technology. In online fraud cases, perpetrators do not merely rely on verbal or written deception but also exploit digital payment systems, social media, and e-commerce platforms as tools to commit crimes. This indicates that the current criminal law needs to be updated to be more relevant in dealing with cybercrimes.

Furthermore, comparative studies with other countries have shown that their legal systems have adopted specific provisions on cybercrime that are more aligned with technological advancements. Several nations have incorporated digital elements as part of criminal offenses in their legislation, enabling law enforcement authorities to more effectively investigate online fraud cases (Putri & Hadrian, 2022). This serves as an important reference for Indonesia in designing regulations that are more adaptive to modern developments.

As a long-term solution, there needs to be an integration between the KUHP and the UU ITE in addressing online fraud crimes. The KUHP can remain the foundation for regulating the general elements of fraud offenses, while the UU ITE can serve as an additional instrument that accommodates the specific characteristics of digital crimes. This approach would enhance law enforcement effectiveness against cybercrimes, provide better protection for victims, and create a stronger deterrent effect for offenders.

3.3 Alternative Application of Article 28(1) of the UU ITE in Online Fraud Cases

Article 28(1) of the UU ITE provides an alternative legal framework for addressing online fraud as it is more relevant to technological developments. This article regulates the dissemination of false information that can harm consumers in electronic transactions. With this provision, cybercriminals who use the internet as their primary means of committing fraud can be subjected to more specific and severe sanctions compared to Article 378 KUHP.

Case studies involving the use of the UU ITE indicate that in several rulings, offenders who committed fraud using similar methods received harsher penalties under this law. This demonstrates that the use of the UU ITE in online fraud cases can create a stronger deterrent effect compared to the KUHP. Additionally, the UU ITE has enforcement mechanisms that are better suited to the nature of cybercrimes, such as digital tracking and access blocking of accounts or websites used in criminal activities.

Furthermore, the UU ITE provides a more detailed legal framework for regulating digital crimes, giving law enforcement authorities clearer guidelines in handling online fraud cases. One of the key advantages of the UU ITE is its flexibility in dealing with cybercrimes that continue to evolve alongside technological advancements. With more specific regulations, legal authorities can more effectively identify, investigate, and prosecute cybercriminals.

Moreover, the application of Article 28(1) of the UU ITE also allows for the use of digital forensic technology in investigations. With more advanced tools such as IP address tracking, digital footprints, and data security systems, law enforcement agencies can obtain stronger evidence to prosecute cybercriminals. This mechanism is crucial in distinguishing between online fraud cases and other types of crimes, ensuring that penalties are appropriately applied based on the severity of the offense.

Beyond law enforcement, the use of the UU ITE in addressing online fraud cases also has a significant impact on consumer protection. With stricter regulations against the dissemination of false and misleading information, consumers can be better protected from the risks of fraud in electronic transactions. This also encourages e-commerce platforms and digital service providers to take a more active role in monitoring transactions on their platforms to prevent cybercrimes.

Overall, the application of Article 28(1) of the UU ITE in online fraud cases offers numerous benefits, both in terms of law enforcement and consumer protection. With harsher penalties and more modern investigative mechanisms, online fraud cases can be more effectively minimized. However, challenges remain in its implementation, particularly in enhancing the capacity of law enforcement agencies and improving coordination between the government, digital service providers, and the public in preventing and addressing cybercrimes.

3.4 Islamic Legal Perspective on Online Fraud in Commercial Transactions

In Islamic law, fraud in commercial transactions is known as *tadlis*, which refers to deception and misrepresentation, both of which are strictly prohibited. Islam upholds the principles of honesty and transparency in trade, making any form of fraud a violation of shariah. In the context of Islamic law, fraud is subject to *ta'zir*, a discretionary punishment determined by the judge based on the severity of the crime committed by the offender (Al-Khālidī, 2024). *Tadlis* is not limited to concealing product defects but extends to any manipulation of information that misleads buyers, including in modern digital transactions. In the context of e-commerce, *tadlis* can take the form of manipulated customer reviews, the concealment of key product details, or the dissemination of false information to attract potential buyers.

The principle of *ta'zir* in Islamic law provides flexibility in determining sanctions, allowing punishments to be tailored to the harm caused by the offense. In certain cases, fraud in commercial transactions may be punished with fines, compensation for the victim, or corporal punishment, depending on the severity of the crime. Judges in the *ta'zir* system have broad authority to consider various factors, such as the offender's intent, the impact on the victim, and the need to prevent future offenses. For instance, in cases of online fraud that result in substantial financial losses for consumers, judges may impose harsher penalties to deter the perpetrator from repeating their actions.

From an Islamic perspective, the concept of *hisbah* also plays a crucial role in preventing fraudulent practices in commerce. *Hisbah* refers to a supervisory mechanism within Islamic society that ensures transactions adhere to principles of justice and transparency. Historically, *hisbah* institutions were responsible for market oversight, ensuring that traders did not engage in fraudulent practices and enforcing sanctions against those who violated ethical trade standards. In the context of online fraud, this concept can be implemented through stricter regulations for e-commerce platforms and increased consumer awareness regarding their rights in digital transactions (Handayani & Zahara, 2024). For example, e-commerce platforms could be required to implement seller verification systems to reduce the risk of fraud.

Islamic law also places significant emphasis on the rights of victims in fraud cases. In addition to penalizing offenders, the *diyat* (compensation) system can be applied to ensure that victims receive appropriate restitution. This approach prioritizes victim recovery, distinguishing it from positive legal systems, which often focus solely on criminal penalties without guaranteeing the return of victims' lost assets (Ilhamsyah, 2023). In several shariah-based jurisdictions, fraud victims have the right to file compensation claims against perpetrators, ensuring that justice is not only punitive but also restorative.

With the rapid growth of the digital economy, the application of Islamic law to online fraud is becoming increasingly relevant. Some countries with shariah-based legal systems have begun adopting regulations that integrate the principles of *tadlis* and *ta'zir* in addressing cybercrime. For example, certain jurisdictions impose progressive fines and transactional bans on individuals repeatedly found guilty of fraud, in line with the principles of *hisbah*. Consequently, *hisbah* can also be incorporated into modern regulatory frameworks to enhance consumer protection against digital fraud, including simplified reporting mechanisms for victims.

Additionally, some countries have implemented *hisbah* -based approaches in their electronic trade monitoring systems. Such regulations could be adopted in Indonesia through collaboration between the government and digital platforms, ensuring that all transactions meet strict transparency standards. By implementing such mechanisms, consumers can feel more secure when conducting online transactions, while sellers found guilty of *tadlis* may face administrative sanctions or temporary bans from engaging in online commerce.

Thus, the Islamic legal approach to online fraud is more corrective and preventive compared to positive law, which tends to focus on punitive measures. The application of *tadlis*, *ta'zir*, and *hisbah* in modern regulations can serve as an effective solution for preventing and addressing digital fraud in the globalized era. As digital transactions continue to evolve, incorporating Islamic legal principles into contemporary regulations can help ensure that online trade remains guided by justice, transparency, and optimal consumer protection.

3.5 Implications of the Court Ruling on Law Enforcement in Indonesia

This ruling has significant implications for cybercrime regulations in Indonesia. One of the primary recommendations of this study is the need for regulatory revisions regarding online fraud to ensure that perpetrators receive more proportional sanctions. Additionally, this study provides insights for academics and policymakers in formulating more effective legal policies to combat cybercrime. With the increasing number of online fraud cases in Indonesia, a stricter legal approach is required, including enhanced criminal provisions and stricter oversight of electronic transactions.

Another key recommendation is improving cooperation between law enforcement agencies, relevant authorities, and the private sector in tackling online fraud cases. The government must establish closer coordination with internet service providers and e-commerce platforms to ensure that their systems have stronger monitoring mechanisms for detecting and preventing fraudulent activities. Strengthening cybercrime investigation capabilities is crucial to enhancing law enforcement effectiveness. Law enforcement officers must be equipped with expertise in digital forensics, big data analysis, and monitoring suspicious online transactions.

Moreover, increasing public digital literacy is a critical step in preventing similar crimes in the future. Society needs better education on how to identify online fraud schemes, understand their rights as consumers, and learn the legal steps they can take if they become fraud victims. Public awareness campaigns through social media, seminars, and collaborations with educational institutions can be effective strategies to improve public understanding of cybercrime risks.

Furthermore, in an effort to establish a more responsive legal system, regulatory strengthening is needed to impose administrative sanctions on digital platforms that fail to protect their users from fraud. Other countries have implemented regulatory models that require e-commerce companies and social media platforms to take greater responsibility in handling fraud reports, and Indonesia can adopt similar policies. Thus, in addition to directly prosecuting offenders, this approach will also foster a safer digital ecosystem for all stakeholders.

The government's role in strengthening regulations and oversight of cybercrime is crucial. Policies must be established that require digital companies to be more transparent in disclosing their security practices while also enhancing international cooperation in tackling cross-border cybercrimes. Many online fraud cases involve perpetrators operating from foreign countries, making coordination with international law enforcement agencies an essential aspect that cannot be overlooked.

Additionally, the role of independent institutions in monitoring the implementation of digital regulations needs to be reinforced. Such institutions can act as mediators between the public, the government, and digital service providers in handling cybercrime cases. They can also provide recommendations for more effective policies in addressing online fraud.

From a technical standpoint, strengthening digital security infrastructure must also be a priority. The development of more advanced cybersecurity systems, the application of artificial intelligence to detect suspicious transactions, and the enhancement of encryption systems in digital communications can help reduce the number of online fraud cases. The implementation of blockchain technology in payment systems and smart contracts can also serve as a solution to increase transparency and security in online transactions.

Equally important, the criminal justice system must adapt to technological advancements. The investigation and evidence-gathering processes in online fraud cases often face challenges due to the lack of recognized digital evidence in court. Therefore, digital forensics regulations must be strengthened to ensure that electronic evidence is admissible in legal proceedings more effectively. Additionally, judges and prosecutors should receive specialized training in handling cybercrime cases to better understand the complexities of cases involving digital technology.

The impact of this ruling also highlights the importance of consumer protection in online transactions. Many consumers still lack awareness of their rights in digital transactions, making them vulnerable to cybercrime. Thus, strengthening consumer protection agencies and enforcing consumer rights in digital transactions should be integral parts of Indonesia's cybercrime prevention strategy.

In the long term, regulatory frameworks need to be more flexible and adaptive to technological changes. A risk-based approach in regulatory design could be an effective model, allowing the government to periodically update policies related to cybercrime in accordance with technological advancements and emerging crime patterns. By doing so, the implemented policies will not only be reactive but also proactive in addressing the increasingly complex challenges of digital crime.

With more adaptive legal policies in response to technological advancements, cybercrime is expected to be significantly minimized. Implementing a multidimensional strategy that includes stricter legal approaches, public education, and cross-sector collaboration will help establish a more resilient system in facing the challenges of the digital era. More dynamic and responsive regulations are essential to ensure that the legal framework continues to evolve in alignment with the ever-changing landscape of cybercrime.

4. Conclusion

Based on the findings of this study, it can be concluded that online fraud is a form of cybercrime that continues to grow in line with the rapid advancement of digital technology. The decision of the West Jakarta District Court Number: 1074/Pid.B/2020/PN.Jkt.Brt serves as a concrete example of how the Indonesian legal system handles online fraud cases using Article 378 of the Indonesian Criminal Code (KUHP). However, the application of this article remains a subject of debate, particularly regarding its effectiveness in prosecuting cybercriminals who operate differently from conventional offenders.

This study also highlights that the judge's considerations in sentencing the defendant in this case took into account various legal and social factors. Although the judge sentenced the defendant to one year in prison, some perspectives argue that this sanction may not be sufficient to deter similar crimes in the future. From the perspective of positive criminal law, there is a need to reassess whether Article 378 KUHP is still relevant for handling technology-based fraud cases or whether Article 28(1) of the Electronic Information and Transactions Law (UU ITE) would be more appropriate for prosecuting cybercriminals who use electronic media as their primary tool in committing fraud.

From the perspective of Islamic law, online fraud can be categorized as *tadlis*, which refers to deceptive practices that contradict the principles of honesty and transparency in trade. Islamic law offers a more flexible approach through the concept of *ta'zir*, where judges have the authority to impose penalties based on the impact of the crime on victims and society. Additionally, the concept of *hisbah* in Islam emphasizes the importance of supervision in transactions to prevent fraud and ensure fairness for all parties involved in trade.

Furthermore, the implications of this ruling for Indonesia's law enforcement system indicate the urgent need for regulatory reforms in addressing cybercrime. As online fraud schemes become increasingly complex, existing regulations require adjustments to be more responsive to the challenges posed by digital technology. One potential solution is strengthening collaboration between the government, e-commerce platforms, and law enforcement agencies to create a safer digital ecosystem for consumers.

Additionally, improving digital literacy among the public is a crucial factor in preventing cybercrime. People need to be better educated on how to recognize online fraud schemes and the legal steps they can take if they become victims. Educational campaigns involving various stakeholders, including the government, academics, and digital service providers, can serve as an effective strategy to reduce the rate of cybercrime in Indonesia.

Overall, this study underscores that Indonesia's criminal justice system still faces significant challenges in effectively handling cybercrime. The application of more relevant legal provisions and improvements in law enforcement mechanisms are essential steps that must be taken promptly. Moreover, insights from Islamic law can also contribute to creating a legal system that is more just and victim-oriented. With more comprehensive legal reforms, it is hoped that online fraud cases can be significantly reduced, and public trust in digital transactions can continue to grow.

References

Al-Khālidī, F. K. Ḥmoud. (2024). From Taghrīr to Trust: A Comparative Study of Misrepresentation Challenges in Online Sales Contracts Within Islamic Law and the Jordanian Legal Framework. In J. Fraedrich, M. Pirtskalava, T. Khoshtaria, H. Terzi, M. Bayirli, & B. Al Serhan (Eds.), *Contemporary Business Research in the Islamic World* (pp. 297–322). Springer Nature. https://doi.org/10.1007/978-981-97-5400-7_17

Anggela, T. R., Ikhsan, R. M., & Nurillah, I. (2022). *Dasar Pertimbangan Hukum Hakim Kasus Penipuan Online Dalam Perspektif Undang-Undang Informasi Dan Transaksi Elektronik (ITE (Putusan Nomor 6/Pid.sus/2021/Pn.bdg Dan Putusan Nomor 712/Pid.sus/2020/Pn.jkt.brt)* [Undergraduate Thesis, Sriwijaya University]. https://repository.unsri.ac.id/63411/

Christiani, T. A. (2016). Normative and Empirical Research Methods: Their Usefulness and Relevance in the Study of Law as an Object. *Procedia - Social and Behavioral Sciences*, *219*, 201–207. https://doi.org/10.1016/j.sbspro.2016.05.006

Dermawan, A., Amalia, A., & Handoko, W. H. (2022). Pencegahan Tindak Pidana Penipuan Jual Beli Barang Online. *Jurnal Bangun Abdimas*, *1*(1), 13–20. https://doi.org/10.56854/ba.v1i1.5

Dirman, M., & Cornelis, V. I. (2024). Juridical Review of the Decision on the Crime of Online Fraud against Job Vacancies. *Journal of Law and Social Politic*, *2*(2), 166–176. https://doi.org/10.46799/jlsp.v2i2.28

Fauzi, S. N. (2018). Tindak Pidana Penipuan Dalam Transaksi Di Situs Jual Beli Online (e-Commerce). *Recidive : Jurnal Hukum Pidana Dan Penanggulangan Kejahatan*, *7*(3), 250–261. https://doi.org/10.20961/recidive.v7i3.40603

Hamzah, R., Berlian, C., & Yuniarti, R. (2019). Legal Protection for Consumers Against Fraud on E-Commerce: A Comparative law Analysis. *International Journal of Innovation, Creativity and Change (IJICC)*, *10*(5), 43–54. https://repository.uir.ac.id/22816/

Handayani, S., & Zahara, F. (2024). Legal Consequences of Product Quality Tadlis in E-Commerce Shopee Perspective of DSN MUI Fatwa Number 146 of 2021 on Online Shop Based on Sharia Principles. *Journal Equity of Law and Governance*, *4*(2), 294–299. https://doi.org/10.55637/elg.4.2.10009.294-299

Hanifiyah, R. (2022). *Law Enforcement of Online Business Fraud Crimes According to Positive Law and Islamic Law (Study on Court Decision Number 975/PID. Sus/2018/PN Mks)* [Undergraduate Thesis, Fakultas Syariah dan Hukum Universitas Islam Negeri Syarif

Hidayatullah Jakarta]. https://repository.uinjkt.ac.id/dspace/handle/123456789/64904

Ilham, A. (2023). *Pertimbangan Hakim Dalam Menjatuhkan Pidana Terhadap Pelaku Tindak Pidana Penipuan (Analisis Putusan Nomor 583/Pid.B/2022/Pn Mlg)* [Undergraduate Thesis, Universitas Islam Malang]. http://repository.unisma.ac.id/handle/123456789/7798

Ilhamsyah, R. (2023). *Sanksi pidana Bagi Pelaku Penipuan Jual Beli Online Menurut KUHP, UU ITE & Hukum Islam* [Undergraduate Thesis, Fakultas Syariah dan Hukum UIN Syarif Hidayatullah Jakarta]. https://repository.uinjkt.ac.id/dspace/handle/123456789/73839

Kakoe, S., Ruba'i, M., & Madjid, A. (2020). Perlindungan Hukum Korban Penipuan Transaksi Jual Beli Online Melalui Ganti Rugi Sebagai Pidana Tambahan. *Jurnal Legalitas*, *13*(02), 118–131. https://doi.org/10.33756/jelta.v13i02.7612

Kamran, M., & Maskun, M. (2021). Penipuan Dalam Jual Beli Online: Perspektif Hukum Telematika. *Balobe Law Journal*, *1*(1), 41. https://doi.org/10.47268/balobe.v1i1.501

Kurniawan, O., Zurnetti, A., & Suharizal. (2020). Penyelesaian Sengketa Wanprestasi Dalam Perjanjian Jual Beli Online (E-Commerce) Yang Mengarah Pada Tindak Pidana Penipuan. *Jurnal Syntax Transformation*, *1*(07), 353–358. https://doi.org/10.46799/jst.v1i7.111

Mann, T. (2025). *Activists on Trial: The Weaponisation of Online Defamation Provisions in Indonesia* (SSRN Scholarly Paper 5121948). Social Science Research Network. https://papers.ssrn.com/abstract=5121948

Munik, A., Syabana, F. A., Wijayanto, E. E. ijayanto, Rasya, A., & Sufiarina, S. (2023). Law Enforcement And Factors Background To The Crime Of Fraud In Online Selling Transactions In Indonesia. *International Journal of Social, Policy and Law*, *4*(2), 47–55. https://doi.org/10.8888/ijospl.v4i2.128

Pramesti, Y. A., & Rosnawati, E. (2023). Tindak Pidana Penipuan dalam Media Jual Beli Online. *Web of Scientist International Scientific Research Journal*, *2*(4), 1–15. https://doi.org/10.47134/webofscientist.v2i4.8

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://doi.org/10.37729/eksaminasi.v3i2.2088

Putri, A. H., & Hadrian, E. (2022). Perlindungan Hukum Bagi Korban Penipuan Jual Beli Online. *Krtha Bhayangkara*, *16*(1). https://doi.org/10.31599/krtha.v16i1.1198

Rizwan, H. (2019). *Sanksi pidana bagi pelaku penipuan dalam jual beli online perspektif hukum pidana positif dan hukum pidana Islam (analisis Putusan Pengadilan Nomor: 185/Pid.Sus/2014/PN Msb)* [bachelorThesis, Fakultas Syariah dan Hukum Universitas Islam Negeri (UIN) Syarif Hidayatullah Jakarta]. https://repository.uinjkt.ac.id/dspace/handle/123456789/46903

Ronisah. (2023). *Sanksi Pidana Terhadap Penyalahgunaan E-Commerce Dalam Metode Pembayaran Cash On Delivery (Cod) Menurut Hukum Pidana Positif Dan Hukum Pidana Islam (Studi Putusan Nomor: 303/Pid.B/2022/PN. Tjk)* [Undergraduate Thesis, Fakultas Syariah dan Hukum UIN Syarif Hidayatullah Jakarta]. https://repository.uinjkt.ac.id/dspace/handle/123456789/74779

Safitri, D. R. (2016). *Tinjauan Fiqh Jinayah Tentang Sanksi Pidana Terhadap Pelaku Penipuan Jual Beli Online Melalui Instagram* [Undergraduate Thesis, UIN Raden Fatah Palembang]. http://eprints.radenfatah.ac.id/322/

Saleh, G. (2022). Juridical Analysis of the Crime of Online Store Fraud in Indonesia. *Jurnal Hukum Dan Peradilan*, *11*(1), 151–175. https://doi.org/10.25216/jhp.11.1.2022.151-175

Sari, E. P., Febrianti, D. A., & Fauziah, R. H. (2022). Fenomena Penipuan Transaksi Jual Beli Online Melalui Media Baru Berdasarkan Kajian Space Transition Theory. *Deviance Jurnal Kriminologi*, *6*(2), 153–168. https://doi.org/10.36080/djk.1882

Sudrajat, T. (2022). The Combination of Normative Juridical Methods and Literature in Educational Administration Research. *Proceedings of International Conference on Social Science, Political Science, and Humanities (ICoSPOLHUM)*, *3*, 00026–00026. https://doi.org/10.29103/icospolhum.v3i.160

Sukmayanti, H. (2021). *Sanksi tindak pidana penipuan jual beli online dalam putusan nomor: 906/Pid.B/2011/PN.Jkt.Tim Perspektif Hukum Pidana Islam* [Undergraduate Thesis, UIN Sunan Gunung Djati Bandung]. https://digilib.uinsgd.ac.id/43756/

Widhaningroem, S., & Widowaty, Y. (2024). Juridical Study on Investigation of Fraud Crime Cases in E-Commerce in Indonesia. *LAW&PASS: International Journal of Law, Public Administration and Social Studies*, *1*(2), 150–161. https://doi.org/10.5281/zenodo.11653601

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*(05), 638–649. https://doi.org/10.46799/jst.v2i5.276