Jurnal Penelitian Hukum Ekonomi syariah

Data Forgery in Indonesian E-Commerce: Harmonizing Sharia Principles and Positive Law for Consumer Protection

Ika Atikah[1], Hadiat[2], Dian Febriyani [3]
[1,3] UIN Sultan Maulana Hasanuddin Banten, Indonesia
[2]STAI Al-Mas'udiyah Sukabumi, Indonesia
Email: [1]ika.atikah@uinbanten.ac.id, [2]hadiat.almas81@gmail.com,
[3]dian.febriyani@uinbanten.ac.id

Abstract

This article aims to analyze how the harmonization between Sharia principles and positive law can strengthen consumer protection against data forgery in Indonesian e-commerce transactions. The background of this study lies in the growing risks of identity manipulation, fictitious transactions, and consumer rights violations in the era of digital trade. Normatively, Sharia emphasizes honesty (*sidq*) and trustworthiness (*amanah*) as the foundation of contractual relations, while Indonesia's positive law provides a formal framework through the ITE Law, the Consumer Protection Law, and the Personal Data Protection Law. The research applies a normative juridical method by examining legislation, fatwas, and relevant literature. The findings show that although positive law offers legal instruments, its enforcement remains weak; meanwhile, Sharia economic law underscores ethical compliance as the basis of protection. The academic contribution of this study is to offer a conceptual framework that integrates Sharia ethics with positive legal regulations to reinforce legal certainty, build consumer trust, and promote the sustainability of Indonesia's digital economic growth.

Keywords: Data Forgery; E-commerce; Consumer Protection; Sharia Economic Law; Positive Law

Abstrak

Artikel ini bertujuan untuk menganalisis bagaimana harmonisasi antara prinsip Syariah dan hukum positif dapat memperkuat perlindungan konsumen terhadap pemalsuan data dalam transaksi e-commerce Indonesia. Latar belakang penelitian ini terletak pada meningkatnya risiko manipulasi identitas, transaksi fiktif, dan pelanggaran hak konsumen di era perdagangan digital. Secara normatif, Syariah menekankan kejujuran (sidq) dan kepercayaan (amanah) sebagai dasar hubungan kontraktual, sedangkan hukum positif Indonesia memberikan kerangka formal melalui UU ITE, UU Perlindungan Konsumen, dan UU Perlindungan Data Pribadi. Penelitian ini menerapkan metode yuridis normatif dengan meneliti peraturan perundang-undangan, fatwa, dan literatur yang relevan. Temuan menunjukkan bahwa meskipun hukum positif menawarkan instrumen hukum, penegakannya tetap lemah; Sementara itu, hukum ekonomi Syariah menggarisbawahi kepatuhan etika sebagai dasar perlindungan. Kontribusi akademik dari penelitian ini adalah untuk menawarkan kerangka konseptual yang mengintegrasikan etika Syariah dengan regulasi hukum yang positif untuk memperkuat kepastian hukum, membangun kepercayaan konsumen, dan mendorong keberlanjutan pertumbuhan ekonomi digital Indonesia.

***Kata Kunci**: Pemalsuan Data; E-Commerce; Perlindungan Konsumen; Hukum Ekonomi Syariah; Hukum Positif*

Introduction

The rapid advancement of information technology has transformed how people work and meet daily needs, as the integration of computers and telecommunications creates global networks used across business, banking, government, military, law, and personal activities. The internet, once limited to academic use, now enables a borderless world. However, this progress also opens opportunities for cybercrime. Cybercriminals are highly skilled individuals capable of exploiting complex digital systems. A notable example was the 1999 hacking of Indonesia's official government website, reported by Kompas. Similar incidents have occurred globally, including breaches of America Online and cyberattacks on the FBI that temporarily disrupted its online services. These cases illustrate the growing severity of cyber threats despite strengthened security measures.

The rapid development of information technology has transformed patterns of communication and social interaction, making the internet a central part of everyday life and enabling instant connectivity across distances. In Indonesia, this shift is reflected in the rising number of social media users, which reached approximately 191 million in 2022—an increase of 12.35% from the previous year (Dawitri & Amara, 2023). More recent data show that Indonesia recorded around 139 million social media user identities in 2024 and about 143 million in 2025, with total internet users reaching 212 million, indicating that digital connectivity continues to expand and increasingly shapes public behaviour at the national level (DataReportal, 2024; DataReportal, 2025). This means that more than half of the nation's population actively engages with social media platforms. While this digital expansion offers many benefits, it also presents challenges, including risks of privacy violations, cybercrime, and the gradual decline of ethical standards in online interactions.

However, international literature shows that the issue of fraud detection and prevention in e-commerce remains a major concern. Rodrigues et al. (2022) emphasize that while existing fraud detection methods continue to evolve, the greatest challenge lies in maintaining consumer trust while simultaneously strengthening regulatory frameworks. More recently, research has also highlighted the importance of integrating artificial intelligence in preventing digital fraud. Recent research has also highlighted the importance of integrating artificial intelligence in preventing digital fraud. Shahriar et al. (2022) demonstrate that explainable AI approaches not only improve the accuracy of fraud detection in e-commerce but also enhance consumer trust and protection, although legal and ethical frameworks still require further development.

Cybercrime operates across borders, making jurisdiction and enforcement difficult, especially in e-commerce where fraud is committed to gain financial or personal benefit while harming legitimate businesses. Such fraud typically exploits digital platforms to mislead victims by concealing essential information or presenting false claims, resulting in the loss of assets or legal rights. Increasing cases of deceptive practices—such as financial scams, false advertisements related to COVID-19 treatments, inflated prices of essential goods, and the sale of hazardous or counterfeit products—have drawn regulatory concern. In the United States, the FTC recorded more than 22,000 complaints early in the pandemic, with losses exceeding USD 22 million. Common techniques include phishing, malware, and identity theft, often executed by impersonating trusted institutions such as the WHO to obtain sensitive personal data (Kabir, 2022).

Most studies on cybercrime focus on legal and regulatory mechanisms aimed at preventing and punishing digital misconduct, while far less attention is given to ethical or religious perspectives such as Qur'anic principles (Gesyani et al., 2023). At the same time, Indonesia's digital economy has grown rapidly, marked by a surge in entrepreneurship and expanding online marketplaces. E-commerce now contributes around 36% of total transactions, with projections reaching US$81 billion by 2025. This growth is supported by an internet penetration rate of 77.02% in 2021–2022—equivalent to about 210 million active users—demonstrating vast potential for digital-based commercial activities (Santoso, 2022).

According to Statista, the number of online shoppers in Indonesia was estimated to reach 65 million in 2022, a notable rise compared to 20 million in 2017. This significant growth reinforces Indonesia's position as one of the largest digital markets globally. Data from Digital 2025 indicate that Indonesia had 212 million internet users and 143 million social-media user identities by early 2025, underscoring the expanding ecosystem for e-commerce and digital business.

Electronic transactions now play a crucial role in global and Indonesian economic activity. Although e-commerce offers significant opportunities, it also faces persistent risks such as fraud, data forgery, and security breaches, all of which threaten consumer trust and market stability. Robust legal and regulatory frameworks are therefore essential, yet difficult to establish because cyber law is complex and technological developments evolve faster than regulation. New digital payment models and cloud-based systems further heighten the need for comprehensive safeguards. In this context, Indonesia must harmonize Sharia principles with positive law to effectively address data forgery in e-commerce. This article examines

existing legal protection mechanisms and incorporates international best practices, including those recommended by UNCTAD, to strengthen digital market governance.

From an Islamic perspective, E-commerce is regarded as analogous to conventional commerce, necessitating adherence to Islamic principles and the permissibility of its framework. Surah Al-Jumu'ah, verse 10 of the Qur'an, underscores the prevalent concerns of consumers, often leading to hesitancy in engaging with E-commerce, particularly due to trust-related apprehensions, thereby amplifying the risks associated with online transactions. Consequently, comprehending the rights of both consumers and producers concerning trust-related matters becomes imperative. These rights encompass various facets, including the right to privacy, protection of consumer data, assurances of transactional security, access to comprehensive product information, manufacturers' entitlement to consumer data, and prompt receipt of payment upon product delivery, among others. The significance of these rights is underscored in Surah Al-Muthaffifiin, verse 1, which highlights their pivotal role in ensuring equitable and righteous commercial transactions in the digital realm.

Understanding consumer behavior plays a vital role in addressing fraudulent practices. Fraudulent activities often develop gradually, making them difficult to detect and prevent. Several analytical approaches, such as the Dempster-Shafer theory and ontology-based models, are employed to determine the point at which customer actions can be classified as fraudulent. These methods typically examine statistical relationships between ongoing transactions and previously identified fraudulent cases. Common indicators include purchase frequency and volume, the use of multiple credit cards, and browsing behavior. Nevertheless, these techniques face limitations in keeping pace with the ever-changing strategies of fraudsters. As offenders continuously adapt their methods, identifying fraudulent patterns becomes more complex, and any misclassification may disrupt legitimate user experiences (Nations, 2015).

Consumer data leakage is one of the most critical challenges in e-commerce, as stolen information is often sold for personal gain, posing significant risks to both users and companies. Major global incidents highlight the severity of this issue. In 2014, eBay suffered a breach affecting 145 million accounts, while in 2013 Target lost over 40 million customers' credit and debit card details. The 2015 Ashley Madison hack exposed sensitive personal data from 37 million users, creating a worldwide scandal. Home Depot experienced a 2014 breach compromising 56 million payment cards, and in 2018 Facebook faced the Cambridge Analytica scandal, where millions of user profiles were misused for political purposes. These cases demonstrate that data breaches are persistent, widespread, and deeply damaging,

eroding public trust and underscoring the urgent need for stronger data protection in the digital marketplace (Priliasari, 2023).

The rise of hacking and system breaches has created significant legal and technological challenges in Indonesia, prompting the enactment of the ITE Law (Law No. 11/2008), later amended by Law No. 1/2024. Under this framework, unauthorized access to electronic systems is a criminal offense, regulated in Article 30 and sanctioned under Article 46. Although hacking motives vary, most involve accessing confidential data, threatening privacy, security, and the reliability of digital systems. The ITE Law thus provides the legal foundation to prevent, deter, and punish cyberattacks, reinforcing digital infrastructure protection and maintaining public trust in electronic transactions.

Data forgery is a serious criminal act involving the manipulation or falsification of essential information, particularly in digital or online documents. In e-commerce, this practice is often used to deceive users for personal gain, with perpetrators frequently disguising alterations as minor errors. The growth of online transactions and reliance on digital records has widened opportunities for such acts, enabling offenders to modify prices, quantities, or payment details, or even create fictitious accounts and transactions. The consequences extend beyond financial losses, affecting victims' reputations and weakening trust in digital transactions. Widespread data forgery undermines the credibility of digital commerce and threatens the integrity of online systems. Therefore, understanding the techniques used by forgers and implementing preventive measures is crucial to protecting consumers, businesses, and the long-term sustainability of e-commerce.

In contrast to global studies that primarily focus on the technical aspects of security and fraud detection (Rodrigues et al., 2022; Shahriar et al., 2022), this article contributes novelty by analyzing the harmonization of Sharia principles and positive law as a uniquely Indonesian framework for consumer protection, specifically in addressing data forgery practices in e-commerce transactions to strengthen consumer rights.

Methods

This study examines strategies to reduce the risks of data forgery in Indonesian e-commerce by integrating Sharia and positive law perspectives. A normative legal approach is employed, supported by an analytical framework that reviews legislation, regulatory instruments, and doctrinal interpretations relevant to consumer protection and fraud prevention (Diantha, 2016). The legal materials include Law No. 8 of 1999 on Consumer Protection, Law No. 11 of 2008 on Electronic Information and Transactions as amended by

Law No. 1 of 2024, Law No. 27 of 2022 on Personal Data Protection, and OJK Regulation No. 39/POJK.03/2019 on Anti-Fraud Strategies.

To incorporate the Sharia dimension, this study also examines key DSN-MUI fatwas—particularly Fatwa No. 146/DSN-MUI/XII/2021 on Online Shop, Fatwa No. 145/DSN-MUI/XII/2021 on Dropship, Fatwa No. 144/DSN-MUI/XII/2021 on Marketplace, and Fatwa No. 116/DSN-MUI/IX/2017 on Sharia Electronic Money—which articulate principles of *amanah*, *sidq*, and the prohibition of *tadlis* and *gharar* relevant to digital transactions and data integrity.

Data were collected through library research encompassing primary sources (laws, fatwas, official documents), secondary sources (books, journal articles, and regulatory commentaries), and tertiary sources (legal dictionaries and encyclopedias). The collected materials were analyzed qualitatively to interpret statutory norms, compare them with Sharia principles, and identify harmonization pathways for strengthening consumer protection and mitigating data-forgery risks in Indonesia's e-commerce sector.

Legal Framework for Consumer Protection

In consumer protection law, consumers are regarded as the primary legal subjects who must be protected. All institutions and organizations engaged in consumer protection exist as a representation of the consumers' own interests. Although the *Consumer Protection Act* also regulates consumers' obligations toward business actors, its main purpose remains focused on safeguarding consumers. A debate has arisen regarding who qualifies as a consumer entitled to legal protection. According to Akomolede and Oladele (Atikah, 2022), modern consumers not only purchase or use goods and services but also form part of the production chain. From this explanation, two main characteristics emerge: consumers as buyers and consumers as links in the production chain. One of the greatest challenges faced by law enforcement authorities is the rapid development of technology, which often gives rise to new legal issues.

Despite ongoing developments, the coordination between law enforcement authorities and the government does not immediately adjust regulations regarding price gouging. Moreover, sales personnel can independently adapt to rapidly advancing technology, efficiently acquiring skills demanded by the fast-paced digital environment. This situation increases the asymmetry and potential conflicts inherent in a rapidly evolving digital economy. Such challenges can be described as "disruptive," reflecting inaccuracies that persist within the economic and industrial systems (Mathios et al., 2020).

Consumer protection is grounded in the recognition that consumers generally hold weaker economic power than business actors, creating unequal bargaining positions that limit their ability to make informed and voluntary choices. The doctrine of bargaining power inequality and exploitation theory highlight how stronger parties—especially large firms—can impose unfavorable terms and exploit consumers' limited information and resources (Ariunjukna, 2018). This makes legal protection essential to prevent abuses, ensure fairness, and enable individuals to exercise their rights effectively. Although defining the subject of protection can be complex, consumer protection legislation typically views individuals who purchase goods for personal use as consumers, as reflected in various jurisdictions—for example, Tanzania excludes those who buy goods for resale or production (Atikah, 2020). Historically, consumer protection was not a primary public or governmental concern, but growing awareness of safety, trade, health, and industrial development eventually formed the basis for Indonesia's regulatory framework, culminating in the enactment of Law No. 8 of 1999 on Consumer Protection (Wibowo, 2020).

Legal protection is essential to ensure safe and fair economic activity, as the legal system's core function is to safeguard citizens. In Indonesia, Law No. 8 of 1999 reflects the state's commitment to protecting consumers and business actors in an era of free trade (Budianto & Wulandari, 2020). Consumer protection is needed to uphold constitutional development goals, prevent harm from technological advances, promote consumers' physical and mental well-being, and maintain consumers as a vital driver of national progress (Atikah, 2022). This framework strengthens market fairness and supports sustainable economic development.

Law No. 8 of 1999 provides the general framework for consumer protection in Indonesia by regulating the rights and obligations of both consumers and business actors. It guarantees key consumer rights, including safety from physical and psychological harm, access to accurate product information, freedom of choice without unfair pressure, and opportunities to inquire or file complaints. The law also ensures the right to a decent standard of living, consumer education, and a clean environment. Additionally, it protects consumers from unfair pricing practices, although it does not specifically regulate issues such as price gouging or impose detailed sanctions on business actors.

Besides consumer rights, business actors also possess rights and obligations under the Consumer Protection Law. Article 6 grants them the right to receive payment as agreed and to obtain legal protection in cases of unlawful actions, including the ability to defend themselves in disputes and seek remedies when appropriate. Article 7 outlines their obligations, requiring

business actors to act in good faith, provide accurate and complete product information, and deliver services responsibly and without discrimination. They must ensure product quality, allow consumers to test certain goods, offer proper guarantees, compensate for losses caused by their products, and fulfill payments for undelivered goods or services as stipulated in agreements.

Consumer protection law in Indonesia positions consumers as primary legal subjects whose rights must be safeguarded, while also outlining the responsibilities of business actors to ensure fair and safe economic interactions. The legislation, particularly Law Number 8 of 1999, provides a general framework that protects consumers from physical, psychological, and economic harm, while also promoting transparency, informed decision-making, and access to education. Although challenges persist such as rapid technological developments, market asymmetries, and emerging digital disputes the law establishes a foundation for balancing the interests of consumers and business actors. By securing consumer rights and ensuring that business actors operate in good faith, Indonesia's consumer protection system contributes to equitable economic growth, public welfare, and sustainable national development, highlighting the importance of legal safeguards in a dynamic and evolving market environment.

Data Forgery in E-Commerce: Harmonization of Sharia and Positive Law

From a Sharia perspective, consumers' personal data is considered an *amanah* (trust) that must be protected for its confidentiality (Nurzihad et al, 2023). Islam emphasizes honesty and prohibits all forms of fraud (*al-makr*) in business transactions (Isman et al, 2024). The Sharia even forbids *gharar* transactions (uncertain or ambiguous transactions), such as selling goods that the seller does not yet own, due to their potential to deceive consumers (Pradini, 2023). In modern e-commerce, situations where retailers offer goods owned by third parties (e.g., fulfillment from Amazon via a local store) can create misleading impressions for consumers. Therefore, regulations must ensure transparency of ownership in accordance with Sharia principles.

According to the *Fatwa DSN-MUI No. 146/DSN-MUI/XII/2021 on Online Shop* and the *Fatwa DSN-MUI No. 144/DSN-MUI/XII/2021 on Marketplace Based on Sharia Principles*, e-commerce transactions conducted through online shops and marketplace platforms must adhere to the principles of *shidq* (honesty), *amanah* (trustworthiness), and full transparency of information. Sellers are prohibited from engaging in *tadlis*, *gharar*, *ghisy*, or *najsy*, including manipulating product descriptions, falsifying item attributes, or concealing product defects.

These fatwas require that every offer includes complete and accurate information concerning product criteria, pricing, delivery fees, and the expected time of delivery, and that the contract is concluded within a valid digital *majelis akad*. Accordingly, the obligation to protect transactions includes preventing fraud, ensuring data openness, and clarifying the rights and obligations of all parties so that transactions remain lawful and equitable within the ethical framework of *"al-ghurm bi al-ghunm"* and the foundational principle that *amanah* is the core of Islamic commercial dealings.

The *Fatwa DSN-MUI No. 116/DSN-MUI/IX/2017 on Sharia Electronic Money* affirms that electronic money is permitted as a means of payment as long as it upholds Sharia principles, which include the prohibition of *riba*, *gharar*, *maysir*, *tadlis*, *risywah*, and any transaction involving unlawful goods or services. The fatwa stipulates that electronic money issued under *wadī'ah* or *qardh* contracts must be managed securely, transparently, and with full accountability. Issuers must protect the entrusted funds, refrain from misuse without the user's consent, and ensure that the full nominal value is returned upon request. Foundational scriptural commands—such as the duty to deliver trusts in QS. al-Nisā': 58 and the obligation to uphold contracts in QS. al-Mā'idah: 1—provide the ethical basis that electronic money must operate with integrity and contractual clarity, ensuring that digital transactions reflect justice (*'adālah*) and responsible conduct (*mas'uliyyah*) consistent with Islamic law.

The *Fatwa DSN-MUI No. 145/DSN-MUI/XII/2021 on Dropship Based on Sharia Principles* clarifies that dropshipping is permissible provided it follows a valid contractual structure—such as *salam*, *wakālah*, or *ju'ālah*—depending on the relationship between the dropshipper, supplier, and buyer. This fatwa strictly prohibits manipulation of product information and requires sellers to present item descriptions accurately, either based on actual knowledge or on verified guarantees of availability. Any form of data forgery—misleading photos, falsified specifications, or fabricated claims—constitutes *tadlis*, which is explicitly forbidden in Islamic commercial ethics. Because many dropshipping arrangements do not involve physical possession (*qabdh*) of goods by the dropshipper, honesty and transparency are essential to prevent the contract from falling into *bai' al-ma'dūm* (selling what is not yet possessed) or excessive *gharar*. These guidelines reinforce the necessity for digital business practices to remain free from data manipulation and firmly within Sharia-compliant boundaries.

The protection of personal data in e-commerce is essential because highly sensitive information—such as national identification numbers, family records, and other identity documents—is vulnerable to misuse and potential economic or social harm. While regulations

require strict confidentiality, businesses simultaneously rely on consumer data to understand behavioral patterns and enhance service efficiency, especially with the growing influence of Big Data in digital commerce (Ayunda, 2022). From a Sharia perspective, the obligation to safeguard personal data is reinforced by *Fatwa DSN-MUI No. 146/DSN-MUI/XII/2021 on Online Shop*, which prohibits *tadlis*, deception, and any form of misinformation, emphasizing that transactions must be conducted with *amanah* (trustworthiness) and transparent disclosure of relevant information. Similarly, *Fatwa DSN-MUI No. 116/DSN-MUI/IX/2017 on Sharia Electronic Money* requires issuers to manage consumer data and entrusted funds securely and responsibly, prohibiting unauthorized use or exploitation. These principles affirm that protecting personal data is not only a legal obligation but also a moral imperative to uphold honesty, justice (*'adālah*), and trust in digital economic activities in accordance with Sharia.

Fraud refers to intentional acts of deception aimed at securing unlawful or unjust benefits, whether through misrepresentation, manipulation, concealment of crucial facts, or other forms of deceit designed to dispossess others of their rights or property. Legal definitions, such as those found in *Black's Law Dictionary*, characterize fraud as deliberate distortion of truth intended to induce another person—who relies on the false information—to surrender something of value or relinquish a legal right (Ahmed, 2021). Within the Sharia framework, fraudulent behavior directly violates the ethical foundations established in *Fatwa DSN-MUI No. 146/DSN-MUI/XII/2021 on Online Shop*, which explicitly prohibits *tadlis*, deception, and misleading representations in digital transactions. Likewise, *Fatwa DSN-MUI No. 116/DSN-MUI/IX/2017 on Sharia Electronic Money* mandates truthful disclosure, responsible conduct, and the safeguarding of entrusted rights, thereby rejecting any form of manipulation or concealment that harms others. These fatwa principles reaffirm that fraud is not only a legal offense but also a moral transgression that undermines *amanah*, violates justice (*'adālah*), and disrupts the integrity of commercial relations in the digital marketplace.

External fraud refers to deceptive acts committed by individuals outside an organization and may lead to civil or criminal consequences. In civil cases, victims can recover financial losses and pursue punitive damages to discourage similar misconduct. Criminal fraud, however, is prosecuted by the state because it threatens public order, and sanctions may include imprisonment. In taxation, fraud may appear as civil evasion or deliberate criminal tax evasion, and distinguishing between the two depends largely on intent and the circumstances surrounding the act (Ahmed, 2021).

In classical *fiqh*, forgery is known as *tazyiif*, meaning the alteration or creation of something so that it appears genuine despite contradicting reality. Within *fiqh jinayah*, this

practice is categorized as *al-makr*, referring to deception used to gain unlawful benefit. Islamic law considers such acts sinful and socially damaging because they undermine trust, violate honesty, and can cause harm to both individuals and communities (Abubakar & Abdullah, 2020; Kamali, 2019; Hasan, 2021). Acts such as falsifying signatures, documents, or records fall squarely within this prohibition.

Related to this is the concept of *tadmīn*, which refers to presenting false information in a form perceived as authentic. Islamic jurisprudence regards *tadmīn* as *haram*, stressing the moral, ethical, and social harms caused by falsification. Unlike positive law, which emphasizes legal procedures and sanctions, Islamic law focuses on moral accountability, the protection of social trust, and the ethical foundations of transactions (Ismail, 2019).

Forgery manifests in various forms, ranging from counterfeit currency and falsified academic certificates to altered identity documents or digital impersonation. Criminals may insert false data into blank but genuine documents, modify legitimate documents belonging to others, or create highly sophisticated forgeries used even in espionage operations. Misusing borrowed identity documents or purchasing fabricated documents from defunct states further demonstrates the wide scope and danger of forgery, particularly as these items often include fake supporting credentials to appear convincing (Cabric, 2015).

From the perspective of international law, fraud and forgery are classified as computer-related crimes. Under the Council of Europe Cybercrime Convention, computer-related forgery involves unauthorized alteration, deletion, or insertion of data to produce falsified information intended to mislead. Computer-related fraud includes digital impersonation, often achieved through spoofed emails or deceptive domain names, to obtain sensitive data or financial benefits. These practices exploit weaknesses in digital communication systems, posing serious cybersecurity threats and eroding user confidence in online services (Nations, 2013).

Islamic principles strictly prohibit all forms of fraud, promoting honesty and fairness in commercial activities as part of safeguarding consumer rights. This ethical foundation aligns with modern legal frameworks aimed at preventing deception in e-commerce. However, some digital business practices conflict with Sharia, such as selling goods not yet in one's possession—a form of *gharar*. For example, retailers who market Amazon-sourced goods as their own mislead consumers about ownership and responsibility, requiring regulatory oversight and clearer disclosure standards (Almaki, 2021).

Consumers in digital markets face persistent challenges such as data privacy risks, identity theft, phishing schemes, deceptive advertising, hidden charges, and inconsistent

refund policies. Delivery delays and misleading product descriptions further undermine market reliability. Enhancing secure digital authentication, improving dispute resolution mechanisms, and strengthening digital literacy are essential steps toward reinforcing trust and protecting consumers in online transactions (Shaik, 2020).

A fundamental difference exists between *fiqh* and positive law in addressing data forgery. *Fiqh* treats it as a moral and social violation that disrupts justice and violates ethical norms, emphasizing accountability before Allah SWT. Positive law, however, treats forgery as a criminal act requiring formal legal procedures to maintain public order and impose sanctions proportionate to the offense (Alkamees, 2017; Solove & Hartzog, 2021). Both approaches ultimately seek to prevent harm but through different philosophical foundations.

The rapid expansion of e-commerce platforms has increased exposure to cybercrimes, including identity theft, data breaches, and insider misuse. Weak cybersecurity infrastructure leaves digital platforms vulnerable to external attacks or unauthorized internal access, leading to financial loss and reputational damage. Continuous improvement of security technologies, employee monitoring, and robust data protection policies are thus essential to reduce risks and sustain consumer confidence (Lubis, 2022).

Risk in project or system management refers to uncertain events that may influence outcomes positively or negatively. Effective risk identification requires structured analysis, expert input, and the documentation of potential threats in risk registers. By anticipating vulnerabilities early, organizations can design mitigation strategies and improve decision-making throughout the project lifecycle (Ahmed, 2017).

Legal protection plays a crucial role in maintaining order, ensuring fairness, and safeguarding human rights. Within this framework, consumer protection law functions to prevent unethical business practices, enhance transparency, and protect vulnerable consumers. Institutions and consumer organizations contribute by promoting education, dispute mediation, and oversight mechanisms, thereby strengthening market fairness and building long-term public trust (Atikah, 2022; Atikah, 2020).

Although fraud in online transactions is strictly prohibited, enforcement remains difficult due to the complex nature of cybercrime. Several factors contribute to this problem: (1) limited jurisdiction and unclear offender identities, since online transactions take place in virtual spaces, making perpetrators difficult to trace; (2) challenges in evidence collection, as online fraud is governed simultaneously by the Criminal Code (*lex generalis*) and the ITE Law (*lex specialis*), requiring extensive digital proof; (3) suboptimal use of technological tools by law enforcement, despite the availability of advanced investigative infrastructure; and

(4) low public awareness, where many users lack knowledge of safe online practices, making them vulnerable to scams such as Binomo and Fahrenheit, which lure victims with unrealistic profit claims (Fadhila, 2021). These obstacles require comprehensive solutions through stronger law-enforcement capabilities, improved digital literacy, and reinforced legal frameworks to more effectively combat cybercrime and protect consumers.

Common forms of e-commerce fraud include: (1) discrepancies between goods ordered and those delivered, (2) the use of fictitious companies or false identities, and (3) deceptive promotions or discount schemes. These practices involve providing false or misleading information that causes material or immaterial losses. In cases of dispute, Article 45A(1) of the ITE Law provides the legal basis, imposing penalties of up to six years' imprisonment and/or fines of up to one billion rupiah. Legal enforcement begins with a preliminary investigation under the ITE Law, followed by further investigation as regulated by the Criminal Procedure Code.

Criminal acts involving data forgery in information technology can take several forms under conventional laws, including fraud, cheating, theft, and data falsification for personal gain, but when committed through computer systems, they appear in more specific digital variants: (1) False Oath or False Statement, where individuals intentionally provide misleading information under oath—formally or informally—to deceive others; (2) Counterfeiting State Coins, Banknotes, and Stamps, involving the production or alteration of currency or official stamps to imitate authenticity or increase perceived value; and (3) Forgery of Letters, which includes fabricating documents or altering existing ones to falsify their origin, often through unauthorized changes to signatures or written content (M. Yusuf et al., 2022). These evolving digital forms of forgery highlight the increasing need for stronger legal safeguards and technological vigilance in protecting electronic information systems.

These criminal activities are governed by various legal frameworks, including Law Number 19 of 2016 concerning Information and Electronic Transactions (ITE). Article 35 of this law addresses acts of data forgery conducted through electronic systems, encompassing the creation, alteration, or destruction of electronic information or documents to falsely represent them as authentic. Such offences entail the intent to deceive or manipulate data for personal gain or to mislead others into accepting forged information as genuine, with implications for agreements, debts, or evidentiary purposes. These actions may be subject to legal sanctions outlined in Article 263 of the Criminal Code (KUHP), which prohibits the use or dissemination of falsified documents as if they were authentic.

A review of Articles 67–70 of the Personal Data Protection (PDP) Law No. 27/2022 shows that falsifying an identity or fabricating a name using personal data belonging to another person—when done for personal or third-party benefit and causing harm—is punishable by up to 5 years of imprisonment and/or a fine of up to IDR 5 billion. Deliberately creating or altering personal data to gain advantage and harming others carries a heavier penalty of up to 6 years' imprisonment and/or a fine of up to IDR 6 billion. Individuals involved in falsifying names or identities may therefore face multiple criminal charges. Beyond primary sanctions, offenders may also be required to surrender profits or assets and pay compensation. When the offense is committed by a corporation, penalties may extend to management or beneficial owners, with corporate fines reaching up to ten times the maximum amount, alongside additional sanctions such as asset confiscation, business suspension, permit revocation, or even dissolution.

In contrast to the UK, the regulations governing personal data protection law are outlined in the Data Protection Act 1998. This act succeeded the Data Protection Act of 1984. Additionally, the UK established an enforcement agency tasked with overseeing the use of personal data, known as the Data Protection Commissioner. The provisions outlined in the Data Protection Act of 1998 were established to prevent data processing that may be detrimental to the interests of individuals. This includes ensuring that the data obtained is not retained for an excessive duration and is only utilized for as long as necessary. The regulations about the protection of personal data are stringent, with strict sanctions imposed if personal data is transferred to another location unless the recipients of such data can ensure comparable levels of data protection (Ayunda, 2022).

Ensuring personal data security in e-commerce is essential for maintaining consumer trust. When users feel their data is well protected, they are more willing to engage with a platform. Conversely, data breaches erode confidence and expose consumers to privacy risks, especially as digital technologies increasingly capture sensitive biometric information. Privacy reflects an individual's autonomy and dignity, making strong data-security measures crucial. Therefore, e-commerce companies must prioritize robust protection systems to safeguard consumer rights and sustain trust in digital transactions.

Fraud detection is crucial for securing e-commerce transactions, protecting consumers, and reducing financial losses. Techniques such as transaction monitoring, IP geolocation, and device fingerprinting are commonly used, while machine learning has become especially effective in identifying suspicious patterns and enhancing overall security (M. Golyeri et al., 2023). In the digital-signature context, forgery refers to attempts to generate a signature

without the signer's private key, undermining the principle of nonrepudiation. Digital signature systems rely on key-generation, signing, and verification algorithms, which together ensure the authenticity and integrity of messages (Bleumer, 2023).

According to Yurita and Farizha, reducing social commerce fraud requires understanding users' own insights into safe online behavior. Their study identified four key mitigation strategies: conducting preliminary research on sellers, relying on referrals and reviews to verify authenticity, checking seller background and communication responsiveness, and ensuring clear terms and conditions regarding products, payments, and delivery. A smaller portion of respondents advised avoiding social media purchases entirely and opting for safer platforms like Lazada or physical stores instead (Yurita & Rudy, 2020).

Industry professionals recognize that fraud will not disappear on its own and must be addressed proactively. Effective fraud risk management begins with identifying vulnerabilities through systematic risk assessments, allowing organizations to design targeted controls and internal checks to reduce potential misconduct. This proactive approach also strengthens regulatory compliance, especially as legal requirements grow more stringent. By implementing a comprehensive fraud risk management strategy, organizations can prevent violations, minimize penalties, and maintain stronger accountability across their operations.

Anti-fraud strategies under POJK 03/2019 are executed through a four-pillar fraud control system. The first is prevention, which reduces fraud risks by fostering ethical awareness, disseminating Anti-Fraud Statements, training employees, educating consumers, and identifying vulnerabilities through mechanisms such as pre-employment screening and continuous character monitoring. The second is detection, which ensures early identification through whistleblowing channels, confidential reporting, follow-up procedures, and surprise audits that strengthen accountability. The third pillar**,** investigation, reporting, and sanctions, requires competent and independent investigators with skills in forensic accounting and digital forensics, supported by structured internal reporting to management and the OJK, along with consistent sanctions that deter violations. The fourth pillar is monitoring**,** evaluation, and follow-up**,** involving ongoing oversight of fraud incidents, analysis of root causes, and corrective actions that reinforce internal controls and maintain the effectiveness of the overall fraud control framework.

These four anti-fraud pillars illustrate that OJK's regulatory framework adopts a proactive and comprehensive model that emphasizes prevention, transparency, and continuous governance enhancement rather than relying solely on punitive responses. This approach aligns closely with Sharia principles—such as *amanah*, *shidq*, and the prohibition of *tadlis*—

as articulated in Fatwa DSN-MUI No. 146/DSN-MUI/XII/2021 on Online Shop and Fatwa DSN-MUI No. 116/DSN-MUI/IX/2017 on Sharia Electronic Money, both of which demand honesty, accountability, and the protection of consumer rights. By integrating culture-building, early detection, rigorous investigation, and systematic evaluation, the regulatory framework not only strengthens institutional resilience against fraud but also demonstrates a clear harmonization between positive law and Sharia ethics in safeguarding consumers and promoting trustworthy digital financial practices.

Security strategies are a vital component of fraud prevention because they protect users' personal data from cyber threats. Strong measures—such as multi-factor authentication, encryption, and access controls—help maintain data confidentiality and reduce cybercrime risks. Tokopedia's use of OTP-based login shows how effective identity verification can strengthen account security and user trust (Pratama et al., 2022; Adisya P.K. et al., 2023). Yet, data protection requires shared responsibility: platforms must provide robust technical safeguards, while users must practice safe digital behavior. Weakness on either side increases exposure to cyberattacks. Thus, coordinated action between platforms and users is essential to mitigating security risks and ensuring safer digital transactions.

Another common threat involves the illegal modification of online documents, where cybercriminals present fabricated changes as minor errors to deceive users. In some cases, attackers circulate counterfeit bank-site links, causing victims who perform transactions through these pages to unknowingly disclose sensitive credentials such as account numbers and PINs (Sari et al., 2024). This method further demonstrates how sophisticated manipulation of digital interfaces can compromise personal data and undermine user trust.

Although Sharia emphasizes ethical and moral obligations, it shares with positive law the fundamental goal of safeguarding trust and justice in digital interactions. The Islamic notion of *aurah* as protected privacy aligns with the PDP Law's requirement of data confidentiality, while the *Maqasid al-Shariah* framework reinforces compatibility between Sharia values, societal norms, and international standards (Isman et al., 2024). This convergence is evident in their shared aims: the prohibition of fraud—where Islam forbids deception and positive law criminalizes data forgery; the protection of consumer data—viewed as an *amanah* in Islam and legally safeguarded in the PDP Law; and the pursuit of social justice—reflected in Maqasid's emphasis on fairness and public welfare in regulating digital transactions. Together, these principles demonstrate that Sharia and positive law can mutually reinforce a more ethical, trustworthy, and secure digital ecosystem.

Through this harmonization, Sharia and positive law function as complementary systems: Sharia—reflected in DSN-MUI Fatwa No. 146/2021 on Online Shop and Fatwa No. 116/2017 on Sharia Electronic Money—offers ethical guidance rooted in *amanah*, honesty, and the prohibition of *gharar* and *tadlis*, while positive law provides enforceable mechanisms and sanctions to protect consumers. Together, they strengthen trust and accountability in e-commerce. Integrating both perspectives creates an ethical–legal framework that safeguards consumer data and, through the *Maqasid al-Shariah* approach, enhances justice and resilience against data forgery and digital fraud.

Conclusion

This study finds that data forgery in Indonesian e-commerce threatens consumer protection by weakening financial security and digital trust. While positive law through the ITE Law, Consumer Protection Law, and PDP Law provides mechanisms to punish identity falsification, enforcement remains limited due to jurisdictional and evidentiary challenges. Sharia economic law—supported by DSN-MUI Fatwa No. 146/2021 on Online Shop and Fatwa No. 116/2017 on Sharia Electronic Money—emphasizes *sidq*, *amanah*, and the prohibition of *tadlis* and *gharar*, offering strong ethical safeguards. Harmonizing these two systems strengthens legal certainty and ethical conduct, resulting in a more just, trustworthy, and sustainable digital market capable of preventing data forgery and online fraud.

This study contributes an integrative framework that connects Sharia principles with Indonesia's regulatory system for digital consumer protection. Its limitation lies in relying solely on normative analysis without empirical assessment of user awareness, enforcement practices, or platform security. Future research should include empirical studies, cross-jurisdictional comparisons, and evaluations of fintech and e-commerce data protection practices to enhance the framework's practical relevance and support more responsive policy reforms in Indonesia's digital economy.

Bibliography

Abubakar, A. Y., & Abdullah, A. (2020). Forgery and its implications under Islamic law: A jurisprudential analysis. *Journal of Islamic Law Review, 16*(2), 45–63. https://doi.org/10.2139/ssrn.3745762

Adisya, P. K., et al. (2023). Analisis keamanan data pribadi pada pengguna e-commerce: Ancaman, risiko, strategi keamanan (literature review). *Jurnal Ilmu Manajemen Terapan, 4*(5). https://doi.org/10.31933/jimt.v4i5

Ahmed, R. (2017). Risk mitigation strategies in innovative projects. *Intech.* https://doi.org/10.5772/intechopen.69004

Ahmed, S. Z. (2021). An evaluation of the anti-fraud regime in Saudi Arabia from the Islamic Shariah perspective. *Universal Journal of Business and Management, 1*(1), 94–120. https://doi.org/10.31586/ujbm.2021.122

Alkhamees, A. (2017). The application of Islamic law in commercial and civil disputes in Saudi Arabia: The role of Shari'ah and its impact on modern legal frameworks. *Arab Law Quarterly, 31*(3), 305–325. https://doi.org/10.1163/15730255-12314005

Almalki, A. (2021). Legal protection for the consumer in e-commerce according to Saudi law (A descriptive, analytical, and comparative study with the laws of the United States of America). *Beijing Law Review, 12*(4), 1058–1081. https://doi.org/10.4236/blr.2021.124058

Atikah, I. (2020). Perlindungan hak-hak konsumen dalam Hukum Negara. Media Madani Publishing.

Atikah, I. (2020). Consumer protection and fintech companies in Indonesia: Innovations and challenges of the Financial Services Authority. *Jurnal Hukum dan Peradilan, 9*(1), 132–153. http://dx.doi.org/10.25216/jhp.9.1.2020.132-153

Atikah, I. (2022). Consumer rights protection against price gouging during the Covid-19 pandemic in Indonesia. *UUM Journal of Legal Studies, 13*(2), 109–128. https://doi.org/10.32890/uumjls2022.13.2.5

Ayunda, R. (2022). Personal data protection to e-commerce consumer: What are the legal challenges and certainties? *Law Reform, 18*(2), 144–163. https://doi.org/10.14710/lr.v18i2.43307

Cabric, M. (2015). External risks. In *Corporate security management*. Elsevier. https://www.sciencedirect.com/topics/medicine-and-dentistry/forgery#definition

DataReportal. (2024). *Digital 2024: Indonesia Report*. https://datareportal.com/reports/digital-2024-indonesia

DataReportal. (2025). *Digital 2025: Indonesia Report*. https://datareportal.com/reports/digital-2025-indonesia

Dawitri, N., & Amara, M. (2023). *Indonesia's Low Digital Civility Index -Two Sides of Indonesia*. https://doi.org/10.13140/RG.2.2.17889.58721

Dewan Syariah Nasional–Majelis Ulama Indonesia. (2017). *Fatwa DSN-MUI No. 116/DSN-MUI/IX/2017 tentang Uang Elektronik Syariah*. DSN-MUI.

Dewan Syariah Nasional–Majelis Ulama Indonesia. (2021). *Fatwa DSN-MUI No. 144/DSN-MUI/XII/2021 tentang Marketplace Berdasarkan Prinsip Syariah*. DSN-MUI.

Dewan Syariah Nasional–Majelis Ulama Indonesia. (2021). *Fatwa DSN-MUI No. 145/DSN-MUI/XII/2021 tentang Dropship Berdasarkan Prinsip Syariah*. DSN-MUI.

Dewan Syariah Nasional–Majelis Ulama Indonesia. (2021). *Fatwa DSN-MUI No. 146/DSN-MUI/XII/2021 tentang Online Shop Berdasarkan Prinsip Syariah*. DSN-MUI.

Diantha, I. M. P. (2016). *Metodologi penelitian hukum normatif dalam justifikasi teori hukum*. Jakarta: Kencana.

Fadhila, A. P. (2021). Tinjauan kriminologi dalam tindakan penipuan e-commerce berdasar peraturan perundang-undangan pada masa pandemi Covid-19 di Indonesia. *Jurnal Suara Hukum, 3*(2). https://journal.unesa.ac.id/index.php/suarahukum/article/view/12361

Gesyani, H., Ritonga, A. W., Arab, I., & Ningsih, I. (2023). Budaya Pendidikan Al-Qur'an Bagi Anak Usia Dini di Era Teknologi. *Awladuna: Jurnal Pendidikan Islam Anak Usia Dini*, *1*(2), 16–27. https://doi.org/10.61159/awladuna.v1i2.116

Golyeri, M., Çelik, S., Bozyiğit, F., & Kılınç, D. (2023). Fraud detection on e-commerce transactions using machine learning techniques. *Artificial Intelligence Theory and Applications, 3*(1), 45–50. https://dergipark.org.tr/en/download/article-file/3046212

Hasan, K., Abdullah, & Ahyar. (2024). Islamic Communication Ethics: Concepts and Applications In The Digital Era. *Jurnal Al-Fikrah*, *8523*, 97–111.
https://doi.org/https://doi.org/10.54621/jiaf.v13i1.734

Hasan, Z. (2021). Fraud and forgery in Islamic commercial transactions: A fiqh-based perspective. *Arab Law Quarterly, 35*(1), 27–50. https://doi.org/10.1163/15730255-BJA10015

Isman, Zaim, M.A., Eldeen, A.B. (2024). Maqashid Sharia and Harmonizing Law in Indonesia: Impact for SDGs Global Context. In: Hamdan, R.K., Buallay, A. (eds) Artificial Intelligence (AI) and Customer Social Responsibility (CSR). Studies in Systems, Decision and Control, vol 517. Springer, Cham. https://doi.org/10.1007/978-3-031-50939-1_60

Kabir, M. A. (2022). A legal analysis on resolving recently growing online business frauds in Bangladesh. *Law Reform, 18*(2), 264–281. https://doi.org/10.14710/lr.v18i2.46636

Kamali, M. H. (2019). *Crime and punishment in Islamic law: A fresh interpretation.* Cambridge: Cambridge University Press.

Law. (1999). *Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen / Law Number 8 of 1999 on Consumer Protection*.

Law. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik / Law Number 11 of 2008 on Electronic Information and Transactions*.

Law. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi / Law Number 27 of 2022 on Personal Data Protection*.

Law. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik / Law Number 1 of 2024 Amending Law Number 11 of 2008 on Electronic Information and Transactions*.

Lubis, F. (2022). Cybercrime e-commerce business transactions. *SASI, 28*(4), 589–598. https://doi.org/10.47268/sasi.v28i4.1068

Mathios, A., Micklitz, H.-W., Reisch, L. A., Thøgersen, J., & Twigg-Flesner, C. (2020). Journal of Consumer Policy's 40th anniversary conference: A forward looking consumer policy research agenda. Journal of Consumer Policy, 43(1), 1–9. https://doi.org/10.1007/s10603-019-09446-9

Nurzihad, M.I., Ichsan, M., Fitriyanti, F. (2023). Personal Data Protection in Indonesian E-commerce Platforms: The *Maqasid Sharia* Perspective. In: Yang, XS., Sherratt, R.S., Dey, N., Joshi, A. (eds) Proceedings of Eighth International Congress on Information and Communication Technology. ICICT 2023. Lecture Notes in Networks and Systems, vol 693. Springer, Singapore. https://doi.org/10.1007/978-981-99-3243-6_88

Otoritas Jasa Keuangan. (2019). *Peraturan Otoritas Jasa Keuangan Nomor 39/POJK.03/2019 tentang Penerapan Strategi Anti-Fraud bagi Bank Umum*. Otoritas Jasa Keuangan.

Pradini, A. Y. (2023). Pelarangan Riba Dalam Akad dan Problematikanya. In *Dasar-Dasar Hukum Perikatan Islam* (p. 225). Mahra Pustaka.

Priliasari, E. (2023). Perlindungan data pribadi konsumen dalam transaksi e-commerce. *Jurnal Rechtsvinding, 12*(2), 261–279. https://rechtsvinding.bphn.go.id/ejournal/index.php/jrv/article/view/1285

Rodrigues, V. F., et al. (2022). Fraud detection and prevention in e-commerce: A systematic literature review. *Electronic Commerce Research and Applications, 56.* https://doi.org/10.1016/j.elerap.2022.101207

Santoso, E. (2022). Opportunities and challenges: E-commerce in Indonesia from a legal perspective. *Jurnal Penelitian Hukum De Jure, 22*(3), 395–410. http://dx.doi.org/10.30641/dejure.2022.V22.395-410

Sari, H.P.,Mulyani, D. I., Nilamasari, M.A., Sitorus D.D.F., & Harimurti, Y. W. (2024). Efektivitas Hukum Perlindungan Data Pribadi Terhadap Kejahatan Siber di Indonesia.

Shahriar, S., Zhou, Y., Rahman, M. M., & Hossain, M. S. (2022). Explainable artificial intelligence for fraud detection in e-commerce: A systematic review. *Information Processing & Management, 59(6),* 103067. https://doi.org/10.1016/j.ipm.2022.103067

Shaik, D., & Poojasree, V. (2020). Consumer protection in e-commerce: A legal and compliance framework in the digital market. In *Proceedings of the 1st International Conference on Law and Human Rights 2020 (ICLHR 2020).* Atlantis Press. https://doi.org/10.2991/assehr.k.210506.004

Solove, D. J., & Hartzog, W. (2021). The scope and limits of data protection law. *Washington Law Review, 96*(3), 803–851.

United Nations. (2015). *Cyberlaws and regulations for enhancing e-commerce: Case studies and lessons learned.* Trade and Development Board, Investment, Enterprise and Development Commission Expert Meeting on Cyberlaws and Regulations for Enhancing E-Commerce, Including Case Studies and Lessons Learned, Geneva, 25-27 March 2015.

United Nations Office on Drugs and Crime. (2013). *Module 2: General types of cybercrime.* https://www.unodc.org/e4j/zh/cybercrime/module-2/key-issues/computer-related-offences.html

Wan Ismail, W. A. F., et al. (2019). Understanding of Syariah practitioners in Malaysia on document forgery. *Humanities & Social Sciences Reviews, 7*(6), 349–355. https://doi.org/10.18510/hssr.2019.7660

Wibowo, D. E. (2020). How consumers in Indonesia are protected fairly? Indonesian Journal of Advocacy and Legal Services, 2(1), 57–70. https://doi.org/10.15294/ijals.v2i1.36546

Yurita, Y. A. T., & Rudy, F. H. (2020). The current state of social commerce fraud in Malaysia and the mitigation strategies. *International Journal of Advanced Trends in Computer Science and Engineering, 9*(2). https://www.warse.org/IJATCSE/static/pdf/file/ijatcse105922020.pdf

Yusuf, M., et al. (2022). Tindak pidana kejahatan pemalsuan data (data forgery) dalam bentuk kejahatan siber (cybercrime). *Jurnal Pendidikan dan Konseling, 4*(6), 6635–6640. https://journal.universitaspahlawan.ac.id/index.php/jpdk/article/view/9365.