Legal Autonomous Web-based Governance (LAW)
Vol. 1, No. 1, Juni 2026, pp. 109∼122
E-ISSN: XXXX-XXXX | P-ISSN: xxxx-xxxx

Juridical Analysis of Legal Protection Against E-Commerce Fraud in Indonesia

Ninda Lutfiani[1], Maulana Arif Komara[2], Sheila Aulia Anjani[3], Solahudin[4], Noah Rangi[5*], Alexander Chou Kiboy[6]
[1] Faculty of Science and Technology, Universitas Raharja, Indonesia
[2,3,4] Faculty of Economics and Business, Universitas Raharja, Indonesia
[5]Department of Economics and Business Pandawan Incorporation, new zealand
[6]Department of Law and Technology, Ijiis Incorporation, Singapore
[1]ninda@raharja.info, [2]maulana.arif@raharja.info, [3]sheila@raharja.info, [4]solahudin@raharja.info, [5]no.rangi3@pandawan.ac.nz, [6]houki@ijiis.asia
***Corresponding Author**

Article Info

Article history:

Submission March 12, 2026
Revised June 19, 2026
Accepted June 26, 2026
Published June 29, 2026

Keywords:

E-Commerce Fraud
Protection
Transactions
Legal
Digital

ABSTRACT

The rapid growth of e-commerce in Indonesia has enhanced the convenience and efficiency of digital transactions while simultaneously increasing the risk of fraud, thereby threatening consumer protection and trust in online commerce. This study aims to analyze the legal regulation of e-commerce fraud and evaluate the effectiveness of consumer protection mechanisms in Indonesia. **The research** employs a normative juridical method using statutory, conceptual, and case-based approaches through the analysis of laws and regulations, judicial decisions, legal doctrines, and relevant literature. **The findings indicate that e-commerce** fraud commonly occurs through fictitious sales, misleading product information, identity misuse, phishing attacks, and the unauthorized use of personal data. Although Indonesia has established a legal framework through the Indonesian Criminal Code (KUHP), the Law on Electronic Information and Transactions (ITE Law), consumer protection regulations, and digital governance policies, law enforcement continues to face challenges related to digital evidence, cybersecurity risks, cross-border transactions, and limited digital literacy. **The study also highlights the importance** of platform accountability, digital identity verification, and technology-based fraud prevention mechanisms in strengthening consumer protection. **This study** concludes that the effective prevention of e-commerce fraud requires not only robust legal enforcement but also stronger digital governance, enhanced institutional coordination, effective cybersecurity measures, and greater public awareness to support a secure and sustainable digital commerce ecosystem in Indonesia.

1. INTRODUCTION

The rapid development of information and communication technology has fundamentally transformed economic activities and commercial transactions worldwide. The expansion of internet accessibility, mobile technologies, and digital payment systems has accelerated the growth of e-commerce, enabling consumers and businesses to conduct transactions beyond geographical and temporal boundaries [1]. Indonesia has emerged as one of the largest digital economies in Southeast Asia, supported by a substantial increase in internet penetration, smartphone usage, and the widespread adoption of online marketplaces. The growth of digital commerce has generated significant economic opportunities, enhanced market accessibility, and promoted financial inclusion [2]. However, alongside these benefits, the expansion of e-commerce has also created new legal and regulatory challenges, particularly concerning fraudulent activities conducted through electronic transactions [3].

The increasing prevalence of e-commerce fraud has become a significant concern for regulators, law enforcement agencies, digital platforms, and consumers. Recent reports indicate that the rapid growth of Indonesia's digital economy has been accompanied by a substantial increase in online fraud cases, including fraudulent online sales, phishing attacks, identity theft, and payment-related scams. Online fraud may take various forms, including fictitious sales, identity deception, manipulation of product information, phishing attacks, unauthorized access to personal data, and fraudulent payment schemes [4]. Unlike conventional fraud, e-commerce fraud is characterized by the use of digital technologies, anonymous interactions, cross-jurisdictional transactions, and an extensive reliance on electronic evidence. These characteristics create substantial difficulties in identifying perpetrators, collecting admissible evidence, and enforcing legal accountability [5]. Consequently, fraudulent activities not only cause financial losses to consumers but also undermine public trust in digital commerce ecosystems and impede the sustainable development of the digital economy.

From a legal perspective, Indonesia has established several regulatory instruments to address fraudulent activities in electronic transactions [6]. The primary legal basis is found in Article 378 of the Indonesian Criminal Code (KUHP), which criminalizes fraudulent conduct intended to obtain unlawful benefits through deception or false representations. In addition, the Law on Electronic Information and Transactions (ITE Law) provides a specific legal framework governing electronic communications, digital transactions, and the recognition of electronic evidence [7]. More recently, developments in digital governance, cybersecurity regulation, electronic system administration, and personal data protection have expanded the regulatory landscape governing online commercial activities. Despite these developments, challenges remain regarding the effectiveness of law enforcement, the adequacy of consumer protection mechanisms, the responsibilities of digital platforms, and the ability of existing regulations to address increasingly sophisticated forms of cyber-enabled fraud [8].

Existing studies have extensively discussed consumer protection, cybercrime, and online fraud in Indonesia. However, most previous studies have focused primarily on either the criminal law dimension of fraud or the consumer protection aspect of electronic transactions [9]. Limited attention has been devoted to the interaction between criminal law, consumer protection law, digital governance frameworks, and platform responsibility in addressing e-commerce fraud. Furthermore, the rapid evolution of digital technologies, including artificial intelligence (AI)-based fraud schemes, digital identity systems, and cross-border electronic transactions, has created new legal challenges that have not been comprehensively addressed in existing scholarship [10]. This gap highlights the need for a more integrated juridical analysis capable of evaluating the adequacy of Indonesia's current regulatory framework within the broader context of contemporary digital governance.

This study is grounded in the theories of legal protection, legal certainty, and digital governance. Legal Protection Theory is employed to assess the extent to which existing regulations safeguard consumer rights and provide remedies for victims of online fraud [11]. Legal Certainty Theory is utilized to evaluate whether the current legal framework offers clear and predictable standards for law enforcement and dispute resolution. In addition, Digital Governance Theory is used to examine the evolving roles of the state, law enforcement institutions, e-commerce platforms, and digital intermediaries in preventing and responding to fraudulent activities within the digital environment [12]. Through these theoretical perspectives, this study seeks to provide a comprehensive understanding of the effectiveness of Indonesia's legal framework in addressing fraud within electronic commerce transactions [13]. Based on these considerations, this research aims to analyze the legal regulation of e-commerce fraud and consumer protection in Indonesia by examining the relationship between criminal law provisions, electronic transaction regulations, and emerging digital governance mechanisms [14].

The novelty of this study lies in its integrated approach, which combines criminal law analysis, consumer protection principles, platform accountability, and digital governance perspectives to evaluate contemporary challenges in combating e-commerce fraud [15]. Furthermore, the study explores how recent technological developments and evolving digital business models influence the effectiveness of law enforcement and consumer protection measures in Indonesia [16]. The findings of this research are expected to contribute to both theory and practice. Theoretically, the study enriches legal scholarship concerning cyber law, consumer protection, and digital governance by providing an integrated analytical framework for understanding e-commerce fraud [17]. Practically, the findings may serve as references for policymakers, law enforcement agencies, digital platform operators, and other stakeholders in strengthening regulatory frameworks, improving enforcement mechanisms, and enhancing consumer protection within Indonesia's digital economy ecosystem.

Figure 1. Research Contribution to Sustainable Development Goals (SDGs) Through Legal Protection in E-Commerce Transactions

Figure 1 illustrates how this study contributes to the achievement of several Sustainable Development Goals (SDGs). In particular, it supports SDG 8 (Decent Work and Economic Growth) by promoting a secure and trustworthy digital economy; SDG 9 (Industry, Innovation and Infrastructure) through the development of reliable digital transaction systems; SDG 12 (Responsible Consumption and Production) by strengthening consumer protection and encouraging responsible digital commerce practices; and SDG 16 (Peace, Justice and Strong Institutions) through the enhancement of legal certainty, regulatory effectiveness, and institutional capacity in combating digital fraud. Therefore, this study contributes to the broader goal of fostering a secure, inclusive, and sustainable digital commerce ecosystem in Indonesia.

2. LITERATURE REVIEW

2.1. Electronic Commerce and Digital Economy Ecosystems

Electronic commerce (e-commerce) refers to commercial transactions involving the exchange of goods, services, and information through electronic networks, particularly the Internet. Beyond serving as a medium for online transactions, e-commerce has become a fundamental component of the digital economy, influencing business activities, consumer behavior, and market accessibility [18]. The rapid expansion of e-commerce has created integrated digital ecosystems involving consumers, merchants, payment service providers, logistics companies, and online platforms, thereby generating significant economic benefits and enhancing transaction efficiency [19].

Despite these advantages, the growth of e-commerce has also introduced various legal and regulatory challenges, including cybersecurity threats, identity fraud, phishing attacks, data breaches, and deceptive commercial practices. The absence of direct physical interaction often creates information asymmetries that may be exploited by fraudulent actors [20]. Consequently, contemporary regulatory approaches increasingly emphasize platform accountability, consumer data protection, cybersecurity compliance, and digital governance. These developments indicate that effective e-commerce regulation requires an integrated framework that combines commercial law, consumer protection law, cybersecurity regulation, and platform governance.

2.2. Fraud in Electronic Transactions from a Criminal Law Perspective

Fraud is generally understood as a criminal act involving deception or misrepresentation intended to obtain unlawful benefits at the expense of another party [21]. In Indonesia, fraud is primarily regulated under Article 378 of the Indonesian Criminal Code (KUHP), which criminalizes deceptive conduct involving false representations, fictitious identities, or fraudulent schemes used to induce victims to transfer property or economic benefits [22].

The development of digital technologies has transformed the nature of fraudulent conduct. Unlike conventional fraud, e-commerce fraud involves digital identities, electronic payment systems, encrypted communications, and cross-border transactions, making investigations more complex due to difficulties in identifying perpetrators and collecting evidence [23]. Consequently, e-commerce fraud is increasingly recognized as a form of cyber-enabled crime that requires the integration of criminal law, cybercrime regulation, and digital forensic mechanisms [24]. Emerging technologies, including artificial intelligence and automated fraud systems, further challenge traditional concepts of criminal accountability and law enforcement.

2.3. Legal Regulation of Electronic Transactions and Digital Governance

The rapid growth of digital commerce has encouraged governments worldwide to develop legal frameworks regulating electronic transactions and digital activities. In Indonesia, the primary legal basis is the Law on Electronic Information and Transactions (ITE Law), which recognizes electronic communications, electronic documents, and digital evidence as legally valid instruments [25]. This framework provides the foundation for regulating commercial activities conducted through electronic systems and addressing unlawful conduct in digital environments. Contemporary regulatory approaches extend beyond traditional cyber law toward broader digital governance frameworks [26]. These frameworks emphasize the responsibilities of governments, digital platforms, and electronic system providers in ensuring accountability, transparency, security, and consumer protection. Comparative studies show that jurisdictions such as the European Union have strengthened platform accountability and intermediary responsibilities to prevent illegal activities and enhance consumer protection [27]. In Indonesia, the interaction among cyber law, platform governance, personal data protection, and consumer rights remains a critical area of legal regulation and analysis.

2.4. Consumer Protection and Platform Responsibility in Digital Transactions

Consumer protection is a fundamental component of digital commerce regulation. Consumers engaged in electronic transactions face greater risks than those in conventional commerce because they cannot directly verify product quality, seller identity, or transaction security [28]. This vulnerability increases exposure to deceptive practices, identity fraud, misleading advertisements, and the misuse of personal data. Consequently, effective consumer protection requires not only legal regulation but also institutional oversight, technological safeguards, and consumer awareness [29].

The growing influence of e-commerce platforms has expanded debates regarding platform responsibility in preventing fraudulent activities. Digital platforms are increasingly expected to implement seller verification mechanisms, transaction monitoring systems, fraud detection technologies, complaint resolution procedures, and consumer compensation frameworks [30]. Contemporary regulatory developments further emphasize the active role of online intermediaries in mitigating fraud and cybercrime risks. Therefore, the regulation of e-commerce fraud requires an integrated framework that combines criminal law, consumer protection law, cyber law, and digital governance perspectives to address the evolving challenges of digital commerce. Comparative international studies further demonstrate that effective regulation depends on the coordination of legal enforcement, platform governance, consumer protection mechanisms, and cybersecurity measures across multiple jurisdictions.

3. RESEARCH METHOD

This study employs a normative juridical research method to examine the legal regulation of e-commerce fraud and consumer protection in Indonesia. The approach focuses on analyzing legal norms, statutory regulations, judicial decisions, legal doctrines, and relevant scholarly literature [31]. Through normative analysis, the study evaluates the adequacy of Indonesia's legal framework in providing legal certainty, consumer protection, and effective law enforcement mechanisms for addressing fraudulent activities in electronic commerce transactions.

3.1. Research Type and Approach

This study adopts a normative juridical approach supported by statutory, conceptual, case-based, and comparative legal approaches [32]. The statutory approach is used to examine regulations governing electronic transactions, consumer protection, fraud-related offenses, and digital governance, including the Indonesian Criminal Code (KUHP), the Law on Electronic Information and Transactions (ITE Law), the Consumer Protection Law, the Personal Data Protection Law, and other relevant regulations [33]. The conceptual approach analyzes Legal Protection Theory, Legal Certainty Theory, Cyber Law Theory, and Digital Governance Theory as the principal analytical frameworks.

In addition, the case approach examines selected judicial decisions involving online fraud and electronic transactions to assess the practical implementation of legal provisions concerning electronic evidence, criminal liability, and consumer protection [34]. A comparative legal approach is also employed to review international developments in e-commerce regulation, platform accountability, and digital governance. By integrating these approaches, the study provides a comprehensive juridical analysis of e-commerce fraud regulation and consumer protection within the contemporary digital economy.

3.2. Research Data Sources

This study adopts a normative juridical approach supported by statutory, conceptual, case-based, and comparative legal approaches. The statutory approach examines regulations governing electronic transactions, consumer protection, fraud-related offenses, and digital governance, including the Indonesian Criminal Code (KUHP), the Law on Electronic Information and Transactions (ITE Law), the Consumer Protection Law, the Personal Data Protection Law, and other relevant regulations [35]. The conceptual approach analyzes Legal Protection Theory, Legal Certainty Theory, Cyber Law Theory, and Digital Governance Theory as the analytical framework for evaluating the effectiveness of existing regulations and identifying legal challenges arising from technological developments. The case approach examines selected judicial decisions involving online fraud and electronic transactions to assess the practical implementation of legal provisions, particularly with regard to electronic evidence, criminal liability, and consumer protection [36]. In addition, a comparative legal approach is employed to review international developments in e-commerce regulation, platform accountability, consumer protection, and digital governance. By integrating these approaches, this study provides a comprehensive juridical analysis of e-commerce fraud regulation and consumer protection within the contemporary digital economy [37]. The classification of legal materials used in this study is presented in Table 1.

Table 1. Classification of Legal Materials

Types of Legal Materials	Data Sources	Purpose of Use
Primary Legal Materials	Indonesian Criminal Code (KUHP), Law on Electronic Information and Transactions (ITE Law), Consumer Protection Law, Personal Data Protection Law, regulations on electronic systems and cybersecurity, and selected judicial decisions	To provide the primary legal basis for analyzing e-commerce fraud, consumer protection, platform accountability, and digital governance
Secondary Legal Materials	Peer-reviewed journal articles, academic books, research reports, conference proceedings, legal commentaries, and policy documents issued between 2022 and 2026	To provide legal interpretation, theoretical perspectives, comparative analysis, and critical evaluation of the regulatory framework
Tertiary Legal Materials	Legal dictionaries, legal encyclopedias, official legal guidelines, and other reference materials	To support conceptual clarification and enhance understanding of legal terminology

Table 1 The use of these legal materials enables a comprehensive juridical analysis of fraud in e-commerce transactions by integrating statutory provisions, judicial practice, contemporary legal scholarship, and emerging developments in digital governance and consumer protection.

3.3. Data Collection Techniques

The data collection process was conducted through a library research method, as this study primarily relies on legal materials and scholarly sources related to e-commerce fraud, consumer protection, cyber law, and digital governance [38]. This method facilitates the systematic collection and examination of statutory regulations, judicial decisions, academic literature, and policy documents relevant to the research objectives. The collection of legal materials involved several stages. First, relevant sources were identified through a review of statutory regulations, judicial decisions, academic publications, policy reports, and other authoritative materials concerning electronic commerce, fraud offenses, consumer protection, cybersecurity, platform regulation, and digital governance [39]. Particular attention was given to legal developments and scholarly publications issued between 2022 and 2026. Second, legal materials were collected from official government publications, legal databases, academic journals, university repositories, and other credible sources, including selected international references for comparative analysis [40]. Subsequently, the collected materials were classified according to their legal status, subject matter, and relevance to the research objectives. Finally, all legal materials were systematically documented and organized to ensure the traceability, consistency, and reliability of the data used in the legal analysis.

Table 2. Data Collection Procedures

Stage	**Activity**	**Purpose**
Literature Identification	Identifying relevant legal sources, scholarly publications, judicial decisions, and policy documents	To obtain authoritative and relevant legal materials concerning e-commerce fraud and consumer protection
Data Collection	Collecting statutory regulations, judicial decisions, academic literature, policy reports, and comparative legal materials	To gather comprehensive legal data required for the study
Data Classification	Categorizing legal materials based on legal status, subject matter, and analytical relevance	To facilitate systematic legal analysis
Documentation	Organizing and recording legal materials using a structured documentation system	To ensure the consistency, reliability, and traceability of research data

Table 2 Through these procedures, the study ensures that the collected legal materials adequately support a comprehensive juridical analysis of e-commerce fraud regulation, consumer protection mechanisms, platform accountability, and emerging digital governance challenges in Indonesia.

3.4. Data Analysis Techniques

This study employs a qualitative juridical analysis through the systematic interpretation and evaluation of statutory regulations, judicial decisions, legal doctrines, academic literature, and policy documents related to e-commerce fraud and digital governance [41]. The analysis begins with the classification of legal materials according to their relevance to fraud offenses, electronic transactions, consumer protection, personal data protection, cybersecurity, and platform accountability. A statutory analysis is then conducted to examine the content, scope, and interrelationship of relevant legal provisions and to assess whether the existing legal framework provides adequate legal certainty, consumer protection, and effective enforcement mechanisms.

Furthermore, conceptual analysis is undertaken using Legal Protection Theory, Legal Certainty Theory, and Digital Governance Theory as the principal analytical frameworks [42]. The study also employs case-based analysis of judicial decisions involving online fraud and electronic transactions, as well as comparative analysis of international approaches to e-commerce regulation, consumer protection, platform responsibility, and digital governance [43]. The findings derived from these analyses are subsequently synthesized to evaluate the effectiveness of Indonesia's legal framework, identify regulatory gaps, and formulate recommendations for strengthening consumer protection, platform accountability, and law enforcement within the digital economy.

3.5. Research Method Flow

The research framework employed in this study is illustrated in Figure

Figure 2. Research Framework for the Juridical Analysis of E-Commerce Fraud and Consumer Protection in Indonesia

Figure 2 illustrates the systematic stages of the research process. The study begins with the identification of legal issues related to e-commerce fraud, consumer protection, and digital governance, followed by a literature review to establish the theoretical foundation based on Legal Protection Theory, Legal Certainty Theory, and Digital Governance Theory. Legal materials are subsequently collected from statutory regulations, judicial decisions, academic publications, policy documents, and comparative legal sources, and are then classified according to their relevance to fraud regulation, consumer protection, platform accountability, cybersecurity, and electronic transaction governance.

The analysis employs statutory, conceptual, case-based, and comparative legal approaches to evaluate the legal framework governing e-commerce fraud and digital transactions. The findings are synthesized to assess regulatory effectiveness, identify legal gaps, and evaluate platform responsibilities in addressing challenges related to digital identity verification, cybersecurity, AI-based fraud, and cross-border transactions [44]. Based on these findings, the study formulates conclusions and recommendations aimed at strengthening consumer protection, platform accountability, law enforcement effectiveness, and the sustainable development of Indonesia's digital commerce ecosystem.

4. RESULTS AND DISCUSSION

This section presents the findings of the study based on a normative juridical analysis of the legal regulation of e-commerce fraud and consumer protection in Indonesia. The discussion integrates statutory analysis, legal doctrines, judicial decisions, and contemporary perspectives on digital governance to evaluate the effectiveness of Indonesia's legal framework in addressing fraudulent activities in electronic commerce transactions [45]. Particular attention is given to the evolving characteristics of digital fraud, the adequacy of existing regulations, the role of digital platforms, and emerging legal challenges arising from technological developments. The results and discussion are organized into several thematic areas, including the legal regulation of e-commerce fraud, consumer protection mechanisms, platform accountability, law enforcement challenges, and emerging issues in digital governance [46]. Through this integrated analysis, the study evaluates the extent to which Indonesia's current legal framework is capable of addressing contemporary forms of fraud within the rapidly evolving digital commerce environment.

4.1. Forms and Characteristics of E-Commerce Fraud in Indonesia

The rapid expansion of e-commerce has significantly transformed commercial activities in Indonesia by creating broader market access and improving transaction efficiency. However, the growth of digital commerce has also been accompanied by the emergence of increasingly sophisticated forms of fraud [47]. Unlike conventional fraud, e-commerce fraud is characterized by the use of information technology, electronic communication systems, digital payment infrastructures, and virtual identities that enable perpetrators to operate without direct physical interaction with victims. Several forms of e-commerce fraud are frequently identified within Indonesia's digital marketplace ecosystem. One of the most common schemes involves fictitious sales, in which perpetrators advertise products through online marketplaces, social media platforms, or independent websites but fail to deliver the purchased goods after receiving payment [48]. Another prevalent practice involves misleading product representations, whereby sellers intentionally provide inaccurate descriptions regarding product quality, specifications, authenticity, or availability. Such practices violate consumer rights and undermine trust in digital commerce systems.

In addition, identity-based fraud has become increasingly prevalent. Perpetrators often use false identities, fictitious business profiles, stolen credentials, or compromised accounts to gain consumer trust and facilitate fraudulent transactions[49]. Cyber-enabled fraud schemes, such as phishing attacks, social engineering, account takeovers, and unauthorized access to financial information, have further increased the complexity of fraud prevention and law enforcement efforts [50]. These forms of fraud frequently extend beyond traditional criminal deception and involve broader issues related to cybersecurity, personal data protection, and digital identity management. From a legal perspective, the evolution of digital fraud demonstrates that technological innovation continuously creates new opportunities for criminal exploitation. Emerging technologies, including artificial intelligence, automated communication systems, and advanced data analytics, may further increase the sophistication of fraudulent activities. Consequently, e-commerce fraud should be understood not merely as a conventional offense committed through electronic media, but as a complex cyber-enabled crime that requires integrated legal, technological, and governance-based responses.

4.2. Legal Framework Governing E-Commerce Fraud and Consumer Protection

The regulation of e-commerce fraud in Indonesia is based on an integrated legal framework comprising criminal law, electronic transaction regulations, consumer protection laws, and digital governance policies. Article 378 of the Indonesian Criminal Code (KUHP) remains the primary legal basis for prosecuting fraudulent conduct, while additional regulations strengthen consumer protection and the governance of digital transactions. However, the rapid growth of digital commerce has introduced evidentiary and jurisdictional challenges that extend beyond the scope of traditional criminal law, highlighting the need for adaptive and coordinated legal enforcement mechanisms.

The Law on Electronic Information and Transactions (ITE Law) complements the Criminal Code by providing legal recognition of electronic information, electronic documents, and digital communications as admissible evidence in judicial proceedings. This legal recognition is particularly significant in e-commerce fraud cases because transaction histories, electronic communications, payment records, and digital logs frequently constitute the primary forms of evidence available to investigators and prosecutors. Consumer protection legislation further strengthens the legal framework by imposing obligations on business actors to provide accurate information, fair treatment, and adequate dispute resolution mechanisms. Within digital commerce environments, consumer protection principles become increasingly important because of the information asymmetry that exists between consumers and sellers. Furthermore, the enactment of the Personal Data Protection Law and various regulations governing electronic systems reflects Indonesia's evolving commitment to strengthening digital governance and protecting users within online commercial ecosystems. Despite the existence of these regulatory instruments, significant challenges remain regarding legal harmonization, regulatory consistency, and enforcement effectiveness. The coexistence of multiple regulatory regimes often creates interpretative difficulties and institutional overlaps that may reduce the effectiveness of law enforcement efforts. Therefore, the effectiveness of Indonesia's legal framework should be evaluated not only from the perspective of regulatory availability but also in terms of its practical implementation and capacity to address emerging technological challenges. To facilitate a clearer understanding of the legal framework governing e-commerce fraud in Indonesia, the principal regulations and their respective functions in addressing fraudulent activities within digital commerce are summarized in Table 3. The table demonstrates the multidimensional nature of legal protection in e-commerce transactions by integrating criminal law, electronic transaction regulation, consumer protection mechanisms, and digital governance instruments.

Table 3. Legal Framework Governing E-Commerce Fraud in Indonesia

Regulation	Main Scope	Relevance to E-Commerce Fraud
Article 378 of the Indonesian Criminal Code	Fraud Offense	Provides the legal basis for criminalizing deceptive conduct conducted through digital or conventional transactions
Electronic Information and Transactions Law	Electronic Transactions	Recognizes electronic information, documents, and digital communications as valid legal evidence in fraud cases
Consumer Protection Law	Consumer Rights	Protects consumers from misleading information, unfair business practices, and fraudulent transactions
Personal Data Protection Law	Personal Data Security	Prevents identity misuse, unauthorized data processing, and personal data theft in digital environments
Electronic System Regulations	Platform Governance	Establishes security, reliability, and accountability obligations for electronic system providers

Table 3 shows that the regulation of e-commerce fraud in Indonesia is based on an integrated legal framework rather than a single legal instrument. The Indonesian Criminal Code provides the basis for criminal liability, while the ITE Law strengthens the evidentiary framework for digital offenses. This framework is further supported by the Consumer Protection Law, the Personal Data Protection Law, and regulations on electronic systems and cybersecurity, which collectively enhance consumer protection, digital security, and platform accountability. Overall, this interconnected regulatory approach reflects Indonesia's effort to address increasingly sophisticated forms of fraud within the digital economy.

4.3. Juridical Analysis of Law Enforcement and Judicial Practice

Law enforcement against e-commerce fraud in Indonesia continues to face significant challenges despite the existence of an adequate normative legal framework. This situation demonstrates that legal effectiveness cannot be measured solely through regulatory completeness. Instead, the practical enforceability of legal norms depends on institutional readiness, technological capability, digital forensic expertise, and the capacity of law enforcement agencies to respond to increasingly sophisticated cyber-enabled fraud schemes. Consequently, a gap remains between normative legal protection and the actual protection experienced by consumers in digital transactions. The main obstacles include difficulties in identifying perpetrators, collecting and verifying electronic evidence, limited digital forensic capacity, jurisdictional issues in cross-border cases, and practical barriers faced by fraud victims in accessing legal remedies. Judicial practice shows that electronic communications, transaction records, and digital documents are increasingly accepted as evidence under the ITE Law, yet their effective use still depends on technical expertise, institutional capacity, and cooperation among law enforcement agencies, digital service providers, financial institutions, and international partners. Therefore, the effectiveness of legal protection against e-commerce fraud must be assessed not only from the availability of legal provisions, but also from the accessibility, responsiveness, and practical outcomes of law enforcement for consumers.

4.4. Platform Responsibility and Consumer Protection in Digital Commerce

The growing role of digital platforms in e-commerce has expanded legal expectations regarding platform responsibility for preventing fraud and protecting consumers. Platforms are no longer viewed merely as intermediaries, but also as active actors responsible for seller verification, transaction monitoring, fraud detection, complaint handling, dispute resolution, and user data protection. The increasing use of digital identity verification, electronic Know-Your-Customer (e-KYC) procedures, and automated monitoring systems reflects the importance of preventive governance in reducing fraud risks before consumer harm occurs. Therefore, effective consumer protection in digital commerce requires not only legal enforcement, but also collaborative governance involving digital platforms, regulators, law enforcement agencies, financial institutions, technological safeguards, and consumer digital literacy.

4.5. Emerging Legal Challenges in Digital Governance

Technological developments continue to generate legal challenges that may not be fully addressed by existing regulatory frameworks, particularly through the growing use of artificial intelligence (AI) in both legitimate commercial activities and fraudulent schemes, including AI-generated content, synthetic identities, automated phishing attacks, and sophisticated social engineering techniques. In addition, weaknesses in digital identity verification systems increase the risks of identity theft, account takeover attacks, and unauthorized financial transactions, while cross-border electronic transactions further complicate law enforcement through challenges related to jurisdiction, evidence collection, extradition, and international legal cooperation. These developments demonstrate that contemporary e-commerce fraud extends beyond traditional criminal conduct, as emerging technologies create new opportunities for both legitimate commercial activities and cyber-enabled fraud, thereby requiring adaptive digital governance responses to address the interconnected challenges of cybersecurity, consumer protection, and regulatory enforcement.

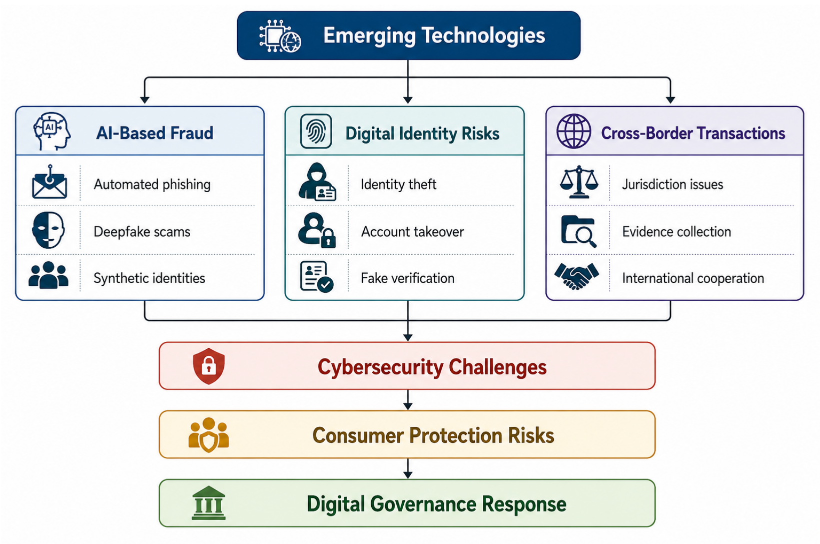

Figure 3. Emerging Legal Challenges in E-Commerce Fraud Governance

Figure 3 illustrates the interconnected legal challenges in digital commerce arising from artificial intelligence, digital identity systems, and cross-border electronic transactions. These developments create more sophisticated forms of fraud, increase cybersecurity risks, and complicate law enforcement, thereby threatening consumer protection and public trust. Although Indonesia has established a legal framework to address e-commerce fraud, the rapid evolution of digital technologies requires continuous regulatory adaptation and stronger digital governance. Therefore, enhancing platform accountability, cybersecurity governance, institutional capacity, digital identity verification, and consumer awareness is essential to strengthening fraud prevention and consumer protection in Indonesia's digital economy.

5. MANAGERIAL IMPLICATIONS

The findings of this study provide important managerial implications for e-commerce platforms, digital service providers, regulators, and other stakeholders within Indonesia's digital economy. As e-commerce fraud becomes increasingly sophisticated, effective prevention requires integrated governance strategies that combine legal compliance, technological innovation, cybersecurity measures, and consumer protection. E-commerce platforms should strengthen accountability through seller verification, electronic Know-Your-Customer (e-KYC) systems, identity authentication, transaction monitoring, AI-based fraud detection technologies, transparent complaint-handling procedures, dispute resolution mechanisms, refund policies, and consumer compensation frameworks. At the same time, policymakers and regulatory authorities must enhance collaboration with digital platforms, financial institutions, cybersecurity agencies, and law enforcement bodies, while continuously updating regulatory frameworks to address challenges related to artificial intelligence, cybersecurity threats, digital identity management, and cross-border electronic transactions. Through a collaborative governance approach that integrates technological safeguards, institutional coordination, regulatory adaptation, and consumer empowerment, stakeholders can strengthen consumer protection and support the sustainable growth of Indonesia's digital economy.

6. CONCLUSION

The findings of this study demonstrate that the rapid growth of e-commerce in Indonesia has generated significant economic opportunities while simultaneously increasing the risk and complexity of fraudulent activities in digital transactions. Various forms of e-commerce fraud, including fictitious sales, deceptive product representations, identity misuse, phishing attacks, and unauthorized access to personal data, continue to threaten consumer security and trust in digital commerce. Although Indonesia has established a comprehensive legal framework through the Indonesian Criminal Code (KUHP), the Law on Electronic Information and Transactions (ITE Law), consumer protection regulations, and other digital governance instruments, the effectiveness of law enforcement remains constrained by several challenges. These challenges include difficulties in identifying perpetrators, the complexity of electronic evidence, limited digital forensic capabilities, cross-border transactions, and varying levels of digital literacy among consumers.

This study contributes to legal scholarship by integrating criminal law, consumer protection law, and digital governance perspectives to evaluate the adequacy of Indonesia's legal framework in addressing e-commerce fraud. The findings indicate that effective consumer protection cannot rely solely on criminal sanctions but also requires stronger platform accountability, enhanced cybersecurity governance, robust digital identity verification mechanisms, and closer institutional coordination among regulators, law enforcement agencies, financial institutions, and e-commerce platforms. These findings provide important implications for policymakers, regulatory authorities, digital platforms, and other stakeholders in strengthening legal enforcement, digital governance mechanisms, and consumer protection within Indonesia's digital economy. From a practical perspective, the study highlights the importance of strengthening digital security systems, implementing artificial intelligence (AI)-based fraud detection technologies, improving dispute resolution mechanisms, and enhancing public awareness of digital transaction risks to create a safer, more secure, and trustworthy digital commerce environment.

Despite these contributions, this study is subject to certain limitations. The research adopts a normative juridical approach that focuses primarily on legal norms, statutory regulations, and legal doctrines without empirically examining law enforcement practices or consumer experiences. Accordingly, future research is recommended to employ empirical and interdisciplinary approaches that incorporate case studies, stakeholder perspectives, quantitative data, and comparative analyses of international regulatory frameworks. Such studies would provide a more comprehensive understanding of the effectiveness of legal and governance mechanisms in combating e-commerce fraud and contribute to the development of adaptive regulatory policies that support a secure, transparent, and sustainable digital economy in Indonesia.

7. DECLARATIONS

7.1. About Authors

Ninda Lutfiani (NL) https://orcid.org/0000-0001-7019-0020

Maulana Arif Komara (MK) https://orcid.org/0009-0005-8906-3132

Sheila Aulia Anjani (SA) https://orcid.org/0009-0007-9121-1151

Solahudin (SS) https://orcid.org/0009-0002-0801-5410

Noah Rangi (NR) https://orcid.org/0009-0004-6616-956X

Alexander Chou Kiboy (AK) https://orcid.org/0009-0009-3858-1852

7.2. Author Contributions

Conceptualization: NL; Methodology: MK; Software: SA; Validation: SS, NR and AK; Formal Analysis: NL and MK; Investigation: SA; Resources: SS; Data Curation: NR and AK; Writing Original Draft Preparation: NL and MK; Writing Review and Editing: SA, SS and NR; Visualization: AK; All authors, NL, MK, SA, SS, NR and AK, have read and agreed to the published version of the manuscript.

7.3. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

7.4. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

7.5. Institutional Review Board Statement

Not applicable.

7.6. Informed Consent Statement

Not applicable.

7.7. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

[1] G. Saleh *et al.*, "Juridical analysis of the crime of online store fraud in indonesia," *Jurnal Hukum Dan Peradilan*, vol. 11, no. 1, pp. 151–175, 2022.

[2] S. Fatmah, M. Atnang *et al.*, "Digital transformation in entrepreneurship: Analysis of e-commerce utilization by msmes in indonesia to enhance competitiveness," *International Journal of Science Technology and Health*, vol. 3, no. 1, pp. 35–43, 2025.

[3] O. Ferli, N. A. Achsani, T. Andati, and Z. Asikin, "Sustainable business innovation in indonesian firms esg disclosure profitability and greenwashing," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 2, pp. 405–419, 2026.

[4] S. H. Jonaedi Efendi *et al.*, "Criminal law enforcement against e-commerce fraud: A case study at the east java regional police," *DE RECHT (Journal of Police and Law Enforcement)*, pp. 46–63, 2025.

[5] M. C. Ramadhan, D. K. Dewi, and Y. M. Saragih, "The legal protection in crime of e-commerce transactions," *Jurnal Akta*, vol. 10, no. 1, 2023.

[6] R. Sitio, S. Jahroh, H. Harianto, and S. Suprehatin, "Visualizing the adoption of circular economy practices in emerging apparel industry through rich picture," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 2, pp. 420–433, 2026.

[7] D. Siregar, "Transforming civil procedural law in the digital era: Evidence, contracts, and legal certainty," *JURNAL USM LAW REVIEW*, vol. 8, no. 3, pp. 2155–2177, 2025.

[8] D. Marsela, Y. Yudhistira, and B. Fawaid, "Legal protection of consumers in online business: a criminal law perspective in handling fraud and identity theft," *Research Horizon*, vol. 4, no. 3, pp. 99–106, 2024.

[9] C. Lukita, A. K. Chandra, R. Fahrudin, N. M. Agatha, and D. P. Suci, "Maturity level measurement model of msmes for sustainable economic growth," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 2, pp. 434–442, 2026.

[10] F. Z. Aqmal, S. Ashraf *et al.*, "Legal protection against gharar in sharia e-commerce: A consumer law analysis in support of the sdgs," *Profetika: Jurnal Studi Islam*, vol. 26, no. 02, pp. 615–630, 2025.

[11] G. Y. Andri, A. Dianti, A. P. Nandar, M. H. Fatahillah, and M. K. Kahfi, "The role of progressive law and legal culture in optimizing fintech services," in *Cirebon Annual Multidiciplinary International Conference (CAMIC)*, 2025, pp. 177–184.

[12] S. Saibaba, "Profiling critical thinking and ai attitudes in management education using a factor-cluster approach for the digital business era," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 2, pp. 493–507, 2026.

[13] E. Santoso *et al.*, "Opportunities and challenges: e-commerce in indonesia from a legal perspective," *Jurnal Penelitian Hukum De Jure*, vol. 22, no. 3, pp. 395–410, 2022.

[14] A. Munik, F. A. Syabana, E. E. ijayanto Wijayanto, A. Rasya, and S. Sufiarina, "Law enforcement and factors background to the crime of fraud in online selling transactions in indonesia," *IJOSPOL-International Journal of Social, Policy and Law*, vol. 4, no. 2, pp. 47–55, 2023.

[15] S. D. Retnandari, K. Khaeroman, A. T. Winarni, and W. Busse, "Digital innovation and technology driven evaluation of maritime safety systems performance in indonesia," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 2, pp. 551–564, 2026.

[16] D. B. D. Badruzaman, "Legal review of consumer protection in e-commerce transactions in indonesia," *Equality: Journal of Law and Justice*, vol. 2, no. 1, pp. 89–102, 2025.

[17] N. Anisahaq and K. Kuswardani, "Analysis of law enforcement related to the fraud of online shopping digital payment system," *Legal Brief*, vol. 11, no. 5, pp. 3095–3103, 2022.

[18] E. J. A. H. Nasution, H. Latief, and R. Rukmana, "Transforming zakat fatwas to strengthen technopreneurship and governance in islamic organizations," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 2, pp. 565–577, 2026.

[19] M. S. Mansyah *et al.*, "Legal protection for victims of fraud in online buying and selling transactions from the perspective of islamic law," *Justice Law Review*, vol. 1, no. 1, pp. 37–65, 2025.

[20] S. Widhaningroem and Y. Widowaty, "Juridical study on investigation of fraud crime cases in e-commerce in indonesia," *LAW & PASS: International Journal of Law, Public Administration and Social Studies*, vol. 1, no. 2, pp. 150–161, 2024.

[21] A. Ruangkanjanases, A. Khan, O. Sivarak, U. Rahardja, and S.-C. Chen, "Modeling the consumers' flow experience in e-commerce: The integration of ecm and tam with the antecedents of flow experience," *Sage Open*, vol. 14, no. 2, p. 21582440241258595, 2024.

[22] R. S. Sari, L. Ferdiles, and A. M. Rusdi, "Model of legal protection in e-commerce transactions to improve the community economy in indonesia," *Jurnal Hukum Indonesia*, vol. 3, no. 2, pp. 87–95, 2024.

[23] A. Z. A. Shami, M. Saleem, and J. Ashraf, "Cybercrime and digital evidence: Investigating the challenges and opportunities in prosecuting cybercrime and handling digital evidence," *Research Consortium Archive*, vol. 3, no. 2, pp. 401–411, 2025.

[24] R. Singh, *Cybercrime and Digital Forensics*. Educohack Press, 2026.

[25] U. Rahardja, N. Lutfiani, A. Rizky, Y. I. Tanjung, R. Evans *et al.*, "A framework for mining customer data in management information systems," *Journal of Computer Science and Technology Application*, vol. 3, no. 1, pp. 21–33, 2026.

[26] E. M. Ali, F. Dirgantara, and D. Darmawan, "Legal protection of consumers in online transactions: A case study of online fraud in indonesia," *International Journal of Service Science, Management, Engineering, and Technology*, vol. 6, no. 3, pp. 27–38, 2024.

[27] D. Andayani, R. S. Ubed, S. Pranata, I. N. Hikam, and A. A. Kamal, "Digital business transformation through shopee's integrated strategy in global e-commerce," *ADI Bisnis Digital Interdisiplin Jurnal*, vol. 6, no. 2, pp. 167–178, 2025.

[28] E. Saragih, M. A. Sahlepi, and M. A. Siregar, "Implementation of the law against fraud crimes in e-commerce-based electronic transactions," in *Proceedings of International Conference on Islamic Community Studies*, 2025, pp. 360–370.

[29] A. Sugiyato, C. S. Bangun, F. Fauzi, M. Mulyati, and O. A. Al-Kamari, "Evaluating the effectiveness of ai in developing digital marketing content for certification service firms," *ADI Bisnis Digital Interdisiplin Jurnal*, vol. 6, no. 2, pp. 144–155, 2025.

[30] A. H. Rambe, I. Kumalasari *et al.*, "Juridical analysis of legal protection for consumers in e-commerce transactions in indonesia," *IJECK (International Journal Of Economy, Computer, Law, Management And Communication)*, vol. 2, no. 2, pp. 34–42, 2024.

[31] U. Rahardja, M. L. Daeli, S. A. Anjani, L. Pasha, A. Asri, and H. Zainarthu, "Enhancing trust and efficiency in e-commerce transactions through blockchain ai synergy," *ADI Journal on Recent Innovation*, vol. 7, no. 1, pp. 25–37, 2025.

[32] R. Hanifiyah, "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)," B.S. thesis, Fakultas Syariah dan Hukum Universitas Islam Negeri Syarif Hidayatullah Jakarta, 2022.

[33] F. P. Oganda, P. A. Sunarya, M. Hardini, S. V. Sihotang, R. S. Ikhsan, and M. Abbas, "Digital transformation as a strategy for building adaptive pesantren management systems," *ADI Bisnis Digital Interdisiplin Jurnal*, vol. 6, no. 2, pp. 120–132, 2025.

[34] I. D. Kurniawan, P. Suwadi, and J. G. S. Soehartono, "An analysis of economic criminal actions of e-money theft case in e-commerce in indonesia," in *1st INTERNATIONAL CONFERENCE ON LAW, BUSINESS, AND GOOD GOVERNANCE 2024*, 2024, p. 1134.

[35] U. Rahardja, M. T. D. S. Putri, N. Septiani, F. Amelia, A. Avandi, and R. Evans, "Human centered legal governance for autonomous ai in digital societies," *Legal Autonomous Web-based Governance (LAW)*, vol. 1, no. 1, pp. 29–41, 2026.

[36] S. D. Andini and R. Nilasari, "Juridical analysis of legal protection against disadvantaged sellers in e-commerce transactions on the tokopedia online shopping site," *Proceedings Series on Social Sciences & Humanities*, vol. 14, pp. 284–289, 2023.

[37] S. Widada, S. T. S. Alfian *et al.*, "Utilizing blockchain for electronic wellbeing records," *Blockchain Frontier Technology*, vol. 1, no. 2, pp. 11–22, 2022.

[38] I. R. Jannah, H. T. Syanturi, and A. Zunaidi, "Legal protection of consumers in transactions e-commerce in indonesia," *IJIEF: Indonesian Journal of Islamic Economics and Finance*, vol. 8, no. 2, pp. 72–80, 2025.

[39] S. Wibowo, I. A. Widjaya, J. Zanubiya, R. Evans, U. Rahardja *et al.*, "Orange technology for humanistic innovation in higher education," *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, vol. 4, no. 2, pp. 105–115, 2026.

[40] I. Purnamasari, "Consumer legal protection in indonesia's e-commerce transactions and efforts to improve security," in *Proceedings of Annual Conference on Scientific Writing*, vol. 2, 2025.

[41] S. Setiawan, M. Susan, and I. Istiharini, "Navigating e-commerce loyalty: The role of e-brand experience and mediating factors in indonesian millennial consumers," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 6, no. 3, pp. 357–368, 2024.

[42] A. Felix and G. D. Rembulan, "Analysis of key factors for improved customer experience, engagement, and loyalty in the e-commerce industry in indonesia," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 2sp, pp. 196–208, 2023.

[43] R. A. Mardiah, A. Ahmatnijar, and N. Harahap, "Analysis of judges' considerations in imposing sanctions for online fraud: A study of positive and islamic criminal law," *Musabab: Journal of Islamic Law and Social Practice*, vol. 1, no. 1, pp. 92–106, 2025.

[44] A. Gunawan, T. Yuniarsih, A. Sobandi, and S. A. Muhidin, "Digital leadership towards performance through mediation of organizational commitment to e-commerce in indonesia," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 1Sp, pp. 68–76, 2023.

[45] L. E. Susanti, "Digital payment legal terminology in online transactions," *10 Juni*, 2025.

[46] P. Celestin *et al.*, "How e-commerce law is evolving to address consumer protection and digital marketplace regulations," *Brainae Journal of Business, Sciences and Technology*, 2024.

[47] F. P. Wathan, "Legal effectiveness in providing consumer protection for online sales and purchase at ecommerce," *Journal Research of Social Science, Economics, and Management*, vol. 2, no. 11, pp. 2707–2718, 2023.

[48] A. Matyash, "Challenges and prospects of legal regulation of advertising on online platforms," *Legal Horizons*, vol. 21, no. 2, pp. 9–17, 2024.

[49] V. Komandla, "Enhancing security and fraud prevention in fintech: Comprehensive strategies for secure online account opening," *Global Research Review in Business and Economics*, vol. 10, no. 5, pp. 102–112, 2024.

[50] OECD, *Addressing Legal and Regulatory Barriers to Quality Infrastructure Investment in India, Indonesia and the Philippines*. OECD Publishing, 2025. [Online]. Available: https://doi.org/10.1787/fb81e1be-en