Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. June 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

LEGAL LIABILITY OF DIGITAL PLATFORMS FOR THE PRACTICE OF FAKE REVIEWS AND FAKE BUYERS

Aulia Tri Hapsari[1a*], Ferry Irawan Febriansyah[2b], and Yogi Prasetyo[3c]

[123] Faculty of Law, Law Study Program , University of Muhammadiyah Ponorogo

E-mail: Auliahapsari42@gmail.com
E-mail: ferryirawanfhumpo@umpo.ac.id
E-mail: Yogiprasetyomadiun@gmail.com

(*) Corresponding Author
Auliahapsari42@gmail.com

ARTICLE HISTORY
Received : 20-01-2026
Revised : 07-02-2026
Accepted : 15-05-2026

KEYWORDS
Fake reviews;
E-Commerce;
Consumer Protection;
Platform Responsibilities;

ABSTRACT
Fake reviews and fake buyers on e-commerce platforms are practices that have the potential to mislead consumers and undermine trust in the digital commerce system. The manipulation of the review system not only affects consumer decisions, but also creates injustice for good-faith business actors. This study aims to analyze the legal arrangements related to fake reviews and fake buyers from the perspective of consumer protection, focusing on the responsibilities of e-commerce platform operators in Indonesia. The research method used is normative legal research with a regulatory approach and a contextual approach, through a study of Law Number 8 of 1999 concerning Consumer Protection and Law Number 11 of 2008 concerning Information and Electronic Transactions. The results of the study show that positive law has not explicitly regulated the practice of fake reviews and fake buyers, so the responsibility of platforms is still limited as a provider of electronic means. Therefore, it is necessary to strengthen regulations to clarify the obligations of platforms in preventing digital fraud practices and protecting consumers.

INTRODUCTION

The rapid development of e-commerce has significantly changed the global economic landscape, creating great opportunities for businesses and consumers to conduct cross-border transactions efficiently and practically. Digital platforms such as Tokopedia, Shopee, and Lazada are becoming an integral part of the lifestyle of modern society, where purchasing decisions are increasingly influenced by consumer reviews and ratings. However, behind this convenience, there is a manipulative phenomenon in the form of fake review practices and fake buyers that have the potential to reduce public trust in the digital system. This practice is done through the creation of fake reviews engineered to improve the reputation of a particular product or store, sometimes even using fictitious buyer accounts to create the impression of pseudo-popularity. This phenomenon not only misleads consumers in making decisions,

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. June 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

but also harms business actors who compete healthily in a digital ecosystem that should be transparent and honest(Kennedy, 2024).

Legal problems related to fake reviews and fake buyers have become increasingly complex because there is no explicit regulation in the national legal system that expressly regulates the practice. Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE) and its amendments have indeed provided a basis for protection against the spread of false or misleading information in the digital space, but it has not specifically regulated the form of economic manipulation that occurs through the false review mechanism(article, 2025). This void in norms creates legal uncertainty in determining the limits of responsibility between business actors, consumers, and digital platform operators. Furthermore, this practice can be categorized as a form of cyber fraud because it contains elements of technology-based fraud that cause economic losses for consumers and other business people(Liu, 2025).

Previous academic studies have shown that research on cybercrime in the field of electronic commerce still focuses on common issues such as transaction fraud, personal data theft, and consumer privacy violations. Meanwhile, studies that specifically highlight the legal responsibility of digital platforms for the existence of fake reviews and fake buyers are still limited(Paul & Nikolaev, 2021). This research gap is important to fill, considering that digital platforms have a central role as transaction facilitators as well as data controllers that allow these manipulative practices to occur(Wu et al., 2020). In this context, this study is directed to analyze how the legal regulation of fake review and fake buyer practices can be qualified as a form of cyber fraud, as well as the extent of the legal responsibility of digital platforms in preventing and overcoming it. Thus, this research aims to make a conceptual contribution to the development of cyber law and consumer protection in the era of the ever-evolving digital economy(Prastyanti & Sobirov, 2025).

METHOD

This research uses a normative juridical method, which is legal research that focuses on the study of applicable positive legal norms and underlying legal principles. The main focus is to study written legal materials, such as laws and regulations, doctrines, and court decisions to find legal rules that are relevant to the issue under study. This research fully relies on secondary data through analytical and argumentative literature studies in answering the legal problems raised(Lokal et al., n.d.).

The approaches applied include a statutory approach and a conceptual approach. The legislative approach is carried out by systematically examining the provisions in Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) and its amendments, Law Number 8 of 1999 concerning Consumer Protection, and Government Regulation Number 80 of 2019 concerning Trade Through Electronic Systems (PP PMSE). Through this approach, the principles, rules, and legal provisions that govern consumer protection in electronic transactions are analyzed. The conceptual approach is used to examine legal concepts such as electronic transactions, the responsibility of digital business actors, and consumer legal protection to strengthen the framework of thinking in analyzing legal issues(Nainggolan et al., 2023).

The legal materials used consist of primary and secondary legal materials. Primary materials include binding laws and regulations, such as the ITE Law, the Consumer Protection Law, and PP PMSE. Meanwhile, secondary materials are in the form of legal journals, books, and scientific publications that provide interpretations of positive legal norms to strengthen theoretical analysis and expand understanding of the application of law in practice(Nainggolan et al., 2023).

The analysis technique used is prescriptive qualitative analysis, which is to analyze legal and doctrinal provisions through descriptive and analytical interpretation. This analysis focuses on the normative meaning of each legal provision and is prescriptive, namely providing normative recommendations regarding the application of the law to achieve certainty and more effective legal protection in electronic transactions and digital consumer protection.

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. June 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

RESULT AND DISCUSSION

Fake Reviews and Fake Buyers as a Form of Cyber Fraud

The phenomenon of fake reviews and fake buyers is a form of cyber crime (cyber fraud) that is growing rapidly along with the growth of the digital economy. The increase in e-commerce activities and ease of internet access make online platforms vulnerable to manipulative practices that lower user trust levels. In the digital ecosystem, trust is the main asset that determines the sustainability of the online market. However, the presence of fake reviews and fictitious buyers creates a distortion of the product's reputation and the credibility of the seller.

Fake reviews can be interpreted as reviews made to deceive or manipulate public opinion of a product or service. These reviews can be positive to improve the image of the product, or negative to bring down competitors(Pandey, 2022). Meanwhile, a fake buyer is a fake identity that is used to simulate a purchase transaction, thereby improving the seller's reputation or tricking the product recommendation algorithm on an e-commerce platform(Clarisa & Areta A, 2022). Both practices exploit reputation systems and algorithms used by platforms such as Amazon, Tokopedia, and Shopee to rank products based on the number of transactions, ratings, and review frequency(A et al., 2023). In practice, fake reviews take advantage of loopholes in the scoring system to influence the position of products in search results, while fake buyers create pseudo-transactions to make the product look like it sells hard. The language pattern in fake reviews is generally extreme, too positive or negative, lacks personal experience, and is written in close proximity(A et al., 2023). The perpetrator's account is usually newly created and has no history of other activity. Fake buyers can be identified by unnatural transaction patterns, such as bulk purchases in a short period of time or product returns for no logical reason(Shukla & Goh, 2024). This phenomenon is reinforced by the existence of review farms, which are syndicates of fake reputation service providers that use fictitious account networks and automated bots(Clarisa & Areta A, 2022). One of the commonly used techniques is the sybil attack, which is the creation of multiple fake identities to provide reviews and pseudo-transactions simultaneously(Shukla & Goh, 2024). The goal is to build an impression of popularity and authenticity of the product.

The main drawback lies in the identity verification system that is not yet strict. Many platforms still allow reviews without valid proof of purchase, thus opening up the opportunity to buy and sell fake reviews(Marios Kokkodis, 2022). Another mode that often occurs is the brush scam, which is sending cheap goods to create fake transactions so that the store looks active and trustworthy(Anand et al., 2025)

The development of artificial intelligence makes detection even more difficult. Technologies like FuzzyFakeRoberta are capable of generating reviews with a linguistic structure that resembles human writing(Shukla & Goh, 2024). In addition to damaging consumer trust, fake buyer networks are also used for digital money laundering, through fictitious transactions that disguise the origin of illegal funds(Mutemi & Bacao, 2024). From a legal perspective, fake reviews and fake buyers meet the elements of electronic fraud, because they contain fraudulent intent and manipulative actions that mislead consumers. This practice is contrary to the principle of honesty in the ITE Law and belongs to the category of cyber-enabled fraud that is difficult to trace because it is cross-border(Zulham, 2023).

The impact is very significant on consumer behavior and market structure. Fake reviews encourage wrong purchasing decisions, harm consumers, and create unfair competition(Pandey, 2022). In terms of digital ethics, this practice violates the principles of data integrity and information authenticity, so platforms can be held accountable if they neglect to supervise(A et al., 2023).

The link between fake buyers and digital money laundering is also a concern for international institutions such as the FATF(Mutemi & Bacao, 2024). Therefore, countermeasures must be carried out multidimensionally through the use of machine learning for the detection of suspicious patterns(Paul & Nikolaev, 2021), strengthening regulations, as well as algorithm transparency obligations as implemented in the European Union's Digital Services Act. Collaboration between regulators, platforms, law enforcement, and the public is key to creating an ethical and trusted e-commerce ecosystem.

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. June 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

LEGAL REGULATION OF FAKE REVIEWS AND FAKE BUYERS

The phenomenon of fake reviews and fake buyers is a negative impact of the rapid growth of electronic commerce which has the potential to mislead consumers and undermine trust in the digital ecosystem. This practice in Indonesia is regulated through the ITE Law, UPK, and PP PMSE which complement each other in supervising and cracking down on information manipulation on e-commerce platforms. The ITE Law is the main legal basis because it regulates electronic-based legal activities. Article 28 paragraph (1) prohibits the dissemination of false and misleading information that is detrimental to consumers in electronic transactions, so that it can be used to ensnare the practice of false reviews that affect consumer purchasing decisions. This provision functions as a preventive and repressive instrument in maintaining the honesty of digital information(Kaharu & Puluhulawa, 2025).

In addition, the practice of using fake accounts and fake buyers to improve product reputation can also qualify as electronic data manipulation as prohibited in Article 32 of the ITE Law. Although the ITE Law does not explicitly mention fake reviews, the norms regarding misleading information can be used as a basis for law enforcement against such practices (Shukla & Goh, 2024). The main obstacle in its implementation lies in digital proofing, especially in distinguishing between original reviews and artificial reviews generated by bots or automated systems(Santiago et al., 2025). Therefore, fake reviews can be seen as a form of cybercrime that has an impact on economic losses and a decrease in public trust.

From the perspective of consumer protection, the UUPK guarantees the right to true, clear, and honest information as stipulated in Article 4. Fake reviews violate this principle because they give a false impression of product quality and cause unfair business competition(Clarisa & Areta A, 2022). Business actors who spread false reviews can also be subject to Article 8 of the UUPK which prohibits misleading statements about goods or services. The synergy between the ITE Law and the UUPK is important because the ITE Law emphasizes aspects of technology and electronic data, while the UUPK regulates the substance of the legal relationship between consumers and business actors(Wulandari & Pitriani, 2025). In the digital context, the misleading advertising provisions in Article 9 of the UUPK also need to be interpreted broadly to include user reviews and digital content-based promotions(Gultom & Tamba, 2025). The government plays a role in encouraging consumer education and review verification systems on e-commerce platforms(Al & Hardyanthi, 2024)

Furthermore, PP PMSE emphasizes the responsibility of digital business actors to convey correct and honest information. Article 23 requires the authenticity of product information, so that fake reviews can be qualified as administrative or criminal violations if they mislead consumers(Sari et al., 2024). PP PMSE complements the ITE Law and UUPK with technical arrangements, although it still faces supervisory obstacles and low legal awareness among the public(Nurhidayah & Wahid, 2025). Therefore, a derivative regulation is needed that governs review authentication and platform liability.

PP PMSE also functions to build digital trust because fake reviews create distortion of information that is detrimental to consumers(Badruzaman, 2025). As AI develops, e-commerce platforms need to develop an unnatural review pattern detection system as part of technology-based law enforcement. On the other hand, strengthening people's digital literacy is important because many consumers still judge products only from ratings without critical analysis(Mansyah, 2025)

Overall, the ITE Law, UPK, and PP PMSE form an integrated legal framework in tackling the practice of fake reviews and fake buyers. However, there is still a void in explicit norms that specifically govern fake reviews, so regulatory updates are needed to clarify the boundaries between freedom of expression and the manipulation of information that harms consumers(Zulham, 2023). A progressive and adaptive legal approach is expected to be able to create a transparent, fair, and accountable electronic trading system.

Legal Responsibility of Digital Platforms

Digital platforms have evolved from passive intermediaries to active actors in the management of information, personal data, and public opinion. This role raises questions about the limits of legal liability for user content and activities in the electronic systems they manage. In Indonesian law, digital platforms are categorized as Electronic

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. June 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

System Operators (PSE) based on the ITE Law, so they are obliged to maintain system security and prevent cyber law violations. These responsibilities include the prevention of illegal content, copyright infringement, and misuse of personal data(Sihombing & Mahatmanta, 2020). Globally, similar obligations are regulated in the Digital Services Act and the European Union's Digital Markets Act which emphasize platform transparency and due diligence(Frosio & Geiger, 2023).

The platform liability regime rests on the principles of due diligence and safe harbor. Due diligence demands proactive measures such as moderation and removal of illegal content, while safe harbors provide limited protection as long as those obligations are met. The concept of safe harbor originally developed in the EU e-Commerce Directive and the United States DMCA which protects passive platforms(Allgrove & Groom, 2020). However, the increasing role of algorithms is driving a shift towards the concept of responsible intermediaries that align responsibilities with the level of control of the platform(Bertolini et al., 2021).

In Indonesia, safe harbors are still partial because the obligation to remove content in the Minister of Communication and Informatics Regulation Number 5 of 2020 has not been accompanied by clear legal protection for platforms in good faith(Sihombing & Mahatmanta, 2020). In contrast to the Digital Services Act, which links legal protection with compliance with transparency and systemic risk mitigation(by las Heras Ballell, 2023).

Platform responsibilities are differentiated into direct and indirect liabilities. Direct liability arises if the platform actively promotes or curates illegal content, including through algorithmic systems that generate constructive knowledge of the violation(Rosati, 2025). In Indonesian law, failure to do due diligence can be qualified as negligence under Article 1367 of the Civil Code(Bertolini et al., 2021).

Meanwhile, indirect liability arises when the platform gains economic advantage or has control over user violations without exercising reasonable precautions(Montagnani & Cavallo, 2021). This approach is in line with the doctrine of vicarious infringement in the United States, although the boundaries of liability are increasingly blurred by algorithmic automation(Kinikoglu, 2023).

This development represents a shift from technological neutrality to algorithmic accountability, where platforms are seen as managers of digital ecosystems with broad social impact(Chirosca, 2025). A governance by design approach through audits and risk assessments is also adopted in the EU's DSA and AI Act(Frosio & Geiger, 2021). In Indonesia, the absence of explicit regulations on safe harbors creates legal uncertainty, especially regarding gray content. Therefore, it is necessary to strengthen the principle of conditional immunity based on responsibility follows control through effective control parameters, algorithmic audits, and periodic transparency(Sihombing & Mahatmanta, 2020).

Effectiveness of Law Enforcement and Barriers

The effectiveness of law enforcement against cyber fraud in Indonesia still faces various obstacles even though the ITE Law has provided a normative basis. Online fraud occurs a lot on social media and marketplaces through the use of fake identities, making it difficult to track perpetrators and prove digital(Tuju et al., 2025). The effectiveness of the law is greatly influenced by coordination between law enforcement agencies which is still not optimal, especially in handling cross-regional cases(Syahril & Aris, 2024). In addition, there is still indecisiveness in the application of the lex specialis principle between the ITE Law and the Criminal Code, so that the authorities often use conventional fraud articles that are less relevant to the character of digital crimes(Bahran & Rahardiansah, 2025).

The main obstacle is also in electronic proof that is prone to manipulation and the limitations of the digital forensic capabilities of law enforcement officials(Widhaningroem & Widowaty, 2024). Judges' doubts about the validity of digital evidence also weaken the effectiveness of law enforcement(Mansyah, 2025). The absence of specific regulations regarding fake reviews and fake buyers makes digital manipulation difficult to prosecute, even though it harms consumers and creates market distortions(Hasibuan & Rasyid, 2026). Consumer protection is still reactive and is not supported by a robust identity verification system on e-commerce platforms(Rahardjo et al., 2025). The problem of cross-border jurisdiction, the limited resources of the Cyber Directorate of the National Police, and the low digital literacy of the community further weaken the effectiveness of law enforcement(Tuju et al., 2025). Therefore,

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. June 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

regulatory reform, capacity building of apparatus, and standardization of electronic evidence are needed so that law enforcement against cyber fraud can run effectively in cyberspace.

Critical Analysis in a Consumer Protection Perspective

Consumer protection in the digital era has undergone a major transformation along with the advancement of information and communication technology. Transactions that used to be carried out in person are now shifting to digital platforms, posing new challenges in legal and ethical aspects of business. Consumers now interact with business actors through electronic systems that often weaken their bargaining positions. Digitalization requires legal adaptation to maintain legal certainty while ensuring that the principles of justice and social benefits are protected(Situmeang et al., 2025).

Consumer protection is a human right that must be guaranteed by the state as stipulated in Law Number 8 of 1999. However, in the digital context, existing regulations need to be strengthened to be able to accommodate data-based forms of transactions, algorithms, and the use of smart technology. In practice, digital marketing activities often contain manipulative elements, such as unrealistic product claims, exploitation of personal data, and misleading covert advertising(Nandavita et al., 2025). Therefore, ethical and legal supervision needs to be carried out more strictly and adjusted to the characteristics of the digital market.

Enforcement of consumer protection in the digital realm does not rely on legal norms alone, but also requires the ability of supervisory institutions to adapt to technological developments. Weaknesses in regulation often arise because the law moves more slowly than the dynamics of the electronic market(Novita & Santoso, 2021). For this reason, responsive legal principles are needed, not only to crack down on violations that have occurred, but also to prevent irregularities through increasing digital literacy and information transparency for consumers.

The right to personal data and information security are integral to digital consumer protection. Data collection and processing must be carried out ethically because data is not only an economic asset, but also part of an individual's right to privacy(Fauziah, 2023). When business actors ignore the principle of transparency, digital justice is threatened. Therefore, an independent institution is needed that is able to supervise digital business practices while ensuring consumer rights in cyberspace so that there are no violations of justice and freedom of information.

Digital business ethics are a moral pillar in maintaining a balance between economic interests and social responsibility. In the practice of economic digitalization, business actors often face a dilemma between technological efficiency and moral integrity. Digital business ethics need to be based on the values of honesty, fairness, and social responsibility towards consumers and the business environment(Rahayu et al., 2025). Many partnerships between MSME actors and digital platforms have not implemented the principle of contractual transparency, so it has the potential to create inequality in bargaining positions and disrupt legal certainty.

Ethical digital businesses must respect consumer rights, ensure transaction security, and avoid data exploitation and algorithmic manipulation. The modern business law paradigm cannot be separated from the ethics of using technology and the protection of the public interest(Laksito & Putra, 2023). In this context, business ethics serve as social norms that complement positive laws, since not all unethical behavior can be reached by formal regulation. The integration between regulation and ethics is key in creating a fair and sustainable digital business ecosystem.

Alignment between law and ethics is essential, especially when it comes to the responsibility of platform companies in ensuring the security of data and digital content(Rohendi, 2025). Many digital companies take advantage of legal loopholes on the grounds that they only act as intermediaries between sellers and buyers. In fact, moral and social responsibilities remain attached to them. This practice is contrary to the principle of substantive justice which requires a balance of benefits between business actors and service users.

In the realm of digital marketing, ethics are closely related to honesty in commercial communication. Legal certainty for consumers is impossible without the ethical integrity of business people who uphold the value of truth in promotion(Siregar, 2024). The law will only be effective if it is accompanied by an ethical awareness inherent in the company's culture. Therefore, the application of digital business ethics needs to be made part of the corporate strategy, not just a normative obligation.

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. June 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

Companies that adhere to the principles of digital business ethics actually gain a competitive advantage in the global ecosystem because they increase public trust and brand reputation. The balance between technological innovation and ethical responsibility is an important factor for business sustainability amid increasing consumer awareness of digital justice and privacy issues(Hafis et al., 2024). Thus, the application of business ethics is not only a moral obligation, but also a long-term sustainability strategy.

The three main principles of law, namely justice, certainty, and utility, are the normative basis for the consumer protection framework in the digital era. Justice reflects the balance of rights and obligations between consumers and business actors; legal certainty ensures that each party understands its responsibilities; Meanwhile, the benefits ensure that the law provides added value for the wider community. The modern legal paradigm demands a balance between procedural certainty and substantive justice(Laksito & Putra, 2023). This means that the law must be able to respond to dynamic social needs without losing the basis of certainty.

Rapid technological developments often exceed the ability to form regulations, creating gray areas that have not been clearly regulated. In such a situation, the principle of usefulness is important so that the law is not only repressive, but also able to empower consumers and support innovation. Effective legal protection is expected to increase consumer confidence in the digital market, while encouraging equitable economic growth(Firmansyah & Ramadhan, 2025)

Legal certainty in the context of digital consumer protection must be complemented by efficient and accessible enforcement mechanisms(Ridha et al., 2025). The law should not only be declarative, but must be able to provide real benefits to society. For this reason, collaboration is needed between government agencies, business actors, and civil society in order to create an adaptive and equitable consumer protection system.

The dimension of legal certainty is also closely related to the protection of personal data. Modern e-commerce presents new challenges where consumer data breaches can cause economic, social, and even psychological losses(Prayuti, 2024). Therefore, the law must ensure a proportionate compensation mechanism and apply strict sanctions for business actors who neglect to maintain data security. This is a concrete form of legal protection oriented towards corrective justice.

The main objective of consumer protection regulatory reform is to balance three main principles: justice for consumers, legal certainty for business actors, and benefits for the wider community(Novita & Santoso, 2021). Only with this balance, the legal system can answer the complexity of the digital economy that continues to grow. In practice, the principle of justice is not only distributive, but also corrective, i.e. correcting the power imbalance between large digital platforms and individual consumers.

Regulations on algorithm transparency, the right to be forgotten, and the obligation to disclose privacy policies are concrete examples of the application of the principles of justice and legal certainty in the digital era. With clear regulations and strong oversight, consumers will be better protected from data exploitation and information misuse practices.

The success of digital business law is not only measured by the completeness of regulations, but also by the extent to which the law is able to provide real benefits in the form of consumer protection, increased public trust, and economic sustainability(Rohendi, 2025). Therefore, the principle of usefulness is the main benchmark for the effectiveness of a legal system that is fair and adaptive to social change. A good legal system must be able to protect consumers, strengthen business ethics, and encourage a balance between innovation and social responsibility in facing the challenges of the digital world.

CONCLUSION

The phenomenon of fake reviews and fake buyers in the e-commerce ecosystem is a new form of cybercrime that uses digital loopholes to manipulate information. Both practices meet the characteristics of cyber fraud, as they deliberately deceive consumers through the creation of a false reputation that does not reflect the actual condition of the product or service. This action not only misleads potential buyers, but also undermines public trust in the e-commerce system that is supposed to guarantee transparency and honesty in transactions. In the context of Indonesian

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. June 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

law, the Electronic Information and Transaction Law (UU ITE) can be implicitly applied to this act, especially in articles that regulate the dissemination of false or misleading information that harms other parties. However, the application is still interpretive because there is no explicit provision that directly regulates the manipulation of digital reviews as a separate criminal act.

The responsibility of digital platforms in tackling this practice is still limited and not optimal. Most platforms only implement user reporting systems or automated detection algorithms, which are often incapable of identifying increasingly complex fraud patterns. The limitations of the supervisory mechanism and the lack of strict verification standards for seller and buyer accounts exacerbate this situation. As a result, the digital ecosystem becomes vulnerable to abuse and reputation manipulation, which can ultimately lower consumer trust in e-commerce in general.

To overcome these problems, it is necessary to harmonize regulations between the ITE Law and regulations on Trade Through Electronic Systems (PMSE) so that there is clarity on norms in cracking down on digital manipulation perpetrators. Strengthening the platform's verification obligations is also an important step to ensure that every account involved in online transactions has a valid and verified identity. In addition, it is necessary to establish special legal norms that strictly regulate the practice of manipulating digital reviews, both by individuals and corporations, so that law enforcement can run more effectively and adaptively to technological developments. This approach will encourage the creation of a safer, more transparent, and fair digital ecosystem for all parties involved in electronic transactions.

REFERENCES.

Rahardjo, S. (2021). Legal Science: An Introduction. Jakarta: Rajawali Press.
Frosio, G. (2020). Oxford Handbook of Online Intermediary Liability. Oxford University Press.
Allgrove, B., & Groom, J. (2020). Enforcement in a Digital Context: Intermediary Liability. Edward Elgar Publishing.
Rohendi, H. A. (2025). Digital Business Law: Regulation, Ethics, and Protection in the Digital Economy Era. Digital Books, Google Scholar.
Trivedi, A. (2025). E-Commerce Fraud: Awareness and Prevention Strategies for Shoppers. Dalam FinTech – Innovations, Opportunities and Challenges. Springer.
Pandey, A.K. (2022). Role of Fake Reviews in Indian E-Commerce Market: Perspective of Consumer Protection Act 2019. Indian Journal of Law & Legal Research.
Clarisa, H. (2022). Fake Review and Liabilities Defect Goods in E-Commerce. The Lawpreneurship Journal.
Luo, J., Nan, G., & Li, D. (2023). Fake Review Detection System for Online E-Commerce Platforms. Decision Support Systems, Elsevier.
Hasibuan, A.H.H., & Rasyid, Y.A. (2026). Legal Protection for Consumers Against Fake Reviews on E-Commerce Platforms. Journal of Indonesian Humanitarian Law.
Aris, T.E.H.N.M. et al. (2025). FuzzyFakeRoberta: Fake Review Identification in E-Commerce Platform. Journal of Theoretical and Applied Information Technology.
Anand, L., Goh, H.N., & Ting, C.Y. (2025). Identifying Fraud Sellers in E-Commerce Platform. JOIV International Journal on Informatics and Visualization.
Mutemi, A., & Bacao, F. (2024). E-commerce Fraud Detection Based on Machine Learning Techniques. Big Data Mining and Analytics, IEEE.
Zulham, Z. (2023). A Critical Review of Indonesian Online Consumer Protection: False Advertising and Legal Protection for E-Commerce Consumers. Journal of Law and Sustainable Development.
Garg, S., Gupta, S., & Gupta, B. (2022). Issues and Challenges with Fake Reviews in Digital Marketing. IEEE International Conference Proceedings.
Paul, H., & Nikolaev, A. (2021). Fake Review Detection on Online E-Commerce Platforms: A Systematic Literature Review. Data Mining and Knowledge Discovery, Springer.
Alsubari, S.N., Deshmukh, S.N., & Aldhyani, T.H.H. (2023). Rule-Based Classifiers for Identifying Fake Reviews in E-Commerce: A Deep Learning System. Springer Nature.

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. June 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

Kaharu, S. N., & Puluhulawa, M. R. U. (2025). Article 28 of the ITE Law as a Pillar of Consumer Protection in Online Transactions. Yudhistira: Jurnal Hukum Indonesia.
Santiago, O., & Situmeang, A. (2025). Consumer Protection Against the Sale of Counterfeit Products in E-Commerce. Mediasas Journal of Islamic Law.
Wulandari, B. T., & Pitriani, P. (2025). Consumer Protection Law in Electronic Transactions: Challenges and Solutions in the Digital Era. The Journal of Academic Science.
Gultom, T. M. L., & Tamba, S. (2025). Consumer Protection in Online Business Transactions: A Critical Review of Positive Law in Indonesia. Paralegal International Journal.
Sari, R. S., Ferdiles, L., & Rusdi, A. M. (2024). Model of Legal Protection in E-Commerce Transactions to Improve the Community Economy in Indonesia. Jurnal Hukum Indonesia.
Nurhidayah, A., & Wahid, S. H. (2025). Normative Review of Fake Order Practices in E-Commerce. DiHA: Journal of Interdisciplinary Legal Studies.
Badruzaman, D. B. D. (2025). Legal Review of Consumer Protection in E-Commerce Transactions in Indonesia. Equality Journal of Law and Justice.
Mansyah, M. S. (2025). Legal Protection for Victims of Fraud in Online Buying and Selling Transactions. Justice Law Review.
Sugiarto, D. (2022). Normative Approach in Legal Research and Its Relevance to the Development of Legal Science in Indonesia. Journal of Law and Development, 52(1), 45–60.
Handayani, M., & Prasetyo, B. (2023). Prescriptive Analysis of Legal Responsibility in Electronic Transactions. Scientific Journal of Reform Law, 17(2), 233–248.
Nugroho, Y. (2021). Normative Legal Research Methodology in the Digitalization Era. Journal of Right-Thinking, 10(1), 78–92.
Sihombing, A., & Mahatmanta, M. N. (2020). Safe Harbor 4.0: Exemption of Platform Providers Liability under Indonesian Cyber Laws. ResearchGate.
Bertolini, A., Episcopo, F., & Cherciu, N. A. (2021). Liability of Online Platforms. European Parliamentary Research Service.
de las Heras Ballell, T. R. (2023). The Role of Digital Platforms' Liability in Regulating Global Value Chains: The EU's Approach. Texas International Law Journal, 59(1).
Rosati, E. (2025). The Role, Responsibility and Liability of Online Intermediaries under EU IP Law. Uppsala University.
Montagnani, M. L., & Cavallo, M. (2021). Liability and Emerging Digital Technologies: An EU Perspective. Notre Dame Journal of International & Comparative Law.
Kinikoglu, B. (2023). Liabilities of Virtual World Developers as Intermediary Service Providers: The Case of Second Life. Queen Mary Journal of Intellectual Property, 13(1).
Chirosca, A. (2025). Intermediary Liability within the IP Legal Framework. Intellectus Law Journal.
Frosio, G., & Geiger, C. (2023). Taking Fundamental Rights Seriously in the DSA's Platform Liability Regime. European Law Journal.
Bulgakova, D., & Deruma, S. (2023). The Liability of Online Intermediaries under European Union Law. Kyiv-Mohyla Law and Politics Journal, 9(2).
Schiera, L. (2024). Transatlantic Safe Harbors and Best Efforts: In Search of Fair and Legitimate Uses in Algorithmic Copyright Enforcement. PhD Thesis, University of Bologna.
Sihombing, A. (2020). Safe Harbor 4.0. ResearchGate.
Tuju, M. C., Ramadani, S., & Nasution, C. (2025). Law Enforcement Against Cyber Crimes in Online Buying and Selling Fraud Cases in a Criminology Perspective. Innovative: Journal of Social Sciences.
Syahril, M. A. F., & Aris, A. (2024). Strategies and Dynamics of Online Fraud in Indonesia: Tracing the Effectiveness of the ITE Act. Journal of Law Justice.

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. June 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

Bahran, K., & Rahardiansah, T. (2025). Analysis of Legal Protection for Consumers in Marketplace Fraud Cases in Indonesia. Journal of Management and Economic Research.

Widhaningroem, S., & Widowaty, Y. (2024). Juridical Study on Investigation of Fraud Crime Cases in E-Commerce in Indonesia. Law & Pass International Journal.

Satila, A., Hamzah, I. F., Umar, W., & Wetzal, M. (2024). The Urgency of Identity Verification During Online Transactions. Law and Justice.

Rahardjo, T. M. S., Noerdjaja, H., & Pambudi, G. E. (2025). Consumer Protection Legal Frameworks in Indonesia: The Challenges of E-Commerce and Data Privacy. Research Horizon Journal.

Marifah, M., Slama, S. B., Ruyati, R., & Ribhi, M. (2025). Protection Against Digital Crimes in E-Commerce Transactions. ResearchGate.

Pamungkas, S. J., Bahari, P. N., & Chan, J. (2025). The Role of Investigators in Handling Online Fraud Cases at Cyber Directorate of Metro Jaya Police. VERITAS.

Hasbullah, M. A. (2022). Cybercrime and Business Competition Law in Indonesia. International Journal of Cyber Criminology.

Latuihamallo, J. R. (2024). Electronic Evidence of Anti-Money Laundering Regimes: Comparative Study between UK, US, and Indonesia. Revista de Derecho.

Situmeang, S. M. T., Limbong, B. J., & Utomo, S. S. (2025). Business Ethics in the Era of Digitalization and Law Enforcement in the Perspective of Consumer Protection. Tora: Law and Social Development.

Nandavita, A. Y., Fadla, D. A., & Lizariani, D. (2025). Ethics in Marketing: Efforts to Realize Justice and Consumer Protection in the Digital Era. PENG: Journal of Digital Economics and Business.

Novita, Y. D., & Santoso, B. (2021). The Urgency of Updating Consumer Protection Regulations in the Digital Business Era. Journal of Indonesian Legal Development.

Fauziah, H. N. (2023). The Relevance of Ethical Principles in ICT Consumer Protection Regulations. ResearchGate.

Rahayu, N. P., Tanu, P. A. M., & Karo, S. A. D. (2025). Analysis of Business Ethics and Legal Certainty in the Preparation of Partnership Contracts between Culinary MSMEs and Digital Platforms in Indonesia. Journal of Intellectuals and Scholars.

Laksito, J., & Putra, R. K. (2023). The Legal Paradigm of Consumer Protection in the Era of Indonesia's Digital Economy. Journal of Bureaucracy: Legal and Social Sciences.

Siregar, S. P. (2024). Legal Certainty of Consumer Protection in Accordance with the Provisions of the Consumer Protection Law. Journal of Law, Administration, and Social Policy.

Hafis, M., Yusril, D., & Adrianto, Y. R. (2024). Legal Implications for Consumer Protection in the Digital Era. Journal of Legal and Public Policy Studies.

Firmansyah, M. A., & Ramadhan, R. (2025). Legal Aspects in Business. AXIOM: Journal of Science and Humanities.

Ridha, I., Rahmi, Y., Sofian, W. R., & Maghfirah, Y. (2025). Implementation of Consumer Protection by Consumer Protection Institutions to Uphold Consumer Rights in Indonesia. Journal of Pediaqu Education and Law.

Prayuti, Y. (2024). Consumer Legal Protection in the Digital Era: An Analysis of E-Commerce Practices and Consumer Data Protection in Indonesia. Journal of Legal Interpretation.

Republic of Indonesia. (2008). Law Number 11 of 2008 concerning Information and Electronic Transactions (Article 28 paragraph (1)).

Republic of Indonesia. (2008). Law Number 11 of 2008 concerning Information and Electronic Transactions (Article 32 paragraph (1)).