WORLD CLASS ISLAMIC CYBER UNIVERSITY
UNISSULA
SULTAN AGUNG ISLAMIC UNIVERSITY
FACULTY OF LAW
PROCEEDING OF INTERNATIONAL CONFERENCE ON THE LAW DEVELOPMENT FOR PUBLIC WELFARE
ISSN: 2798-9313
LICS 2026
Topic: *Strengthening Legal Frameworks for Combating Human Trafficking and Enhancing Protection of Women and Children*

Strengthening Consumer Protection in Online Marketplaces Towards Digital Governance and Cyber Law

M. Iqbal Ramdhani[1)], MA Irfan Rahmana[2)], Bahrain Pasha Irawan[3)], Diah Ayu Kusumawati[4)] & Ari Pranaditya[5)]

[1)]Faculty of Law, Universitas Islam Sultan Agung (UNISSULA) Semarang, Indonesia, E-mail: m.iqbalramdhani.std@unissula.ac.id *(Correspondent Author)*
[2)]Faculty of Law, Universitas Islam Sultan Agung (UNISSULA) Semarang, Indonesia.
[3)]Faculty of Law, Universitas Islam Sultan Agung (UNISSULA) Semarang, Indonesia.
[4)]Faculty of Law, Universitas Islam Sultan Agung (UNISSULA) Semarang, Indonesia.
[5)]Faculty of Law, Universitas Islam Sultan Agung (UNISSULA) Semarang, Indonesia.

Abstract. *The rapid expansion of online marketplaces has significantly transformed the global digital economy by facilitating efficient commercial transactions and enhancing market accessibility. However, this growth has also intensified cyber-related threats, including online fraud, identity theft, data breaches, deceptive marketing practices, and unauthorized exploitation of consumer data. These challenges underscore the urgent need for robust digital governance and effective cyber law frameworks to strengthen consumer protection within digital commerce ecosystems. This study aims to examine the influence of digital governance and cyber law compliance on consumer protection and their subsequent impact on consumer trust in online marketplaces. The proposed conceptual model positions Digital Governance and Cyber Law Compliance as independent variables, Consumer Protection as a mediating variable, and Consumer Trust as the dependent variable. Grounded in Digital Governance Theory, Consumer Protection Theory, Institutional Theory, and Trust Theory, the study proposes that transparent digital governance, regulatory compliance, and effective legal enforcement enhance consumer protection, thereby fostering greater consumer trust in online marketplace platforms. A quantitative research design employing a cross-sectional survey will be adopted, targeting active users of online marketplaces. Data will be analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM) to evaluate both direct and indirect relationships among the proposed constructs. The expected findings will contribute to the literature by integrating governance, legal, and consumer behavior perspectives into a comprehensive framework for digital marketplace governance. From a practical standpoint, the study offers strategic implications for policymakers, digital platform providers, and regulatory authorities in* *designing governance mechanisms and cyber legal policies that promote secure, trustworthy, and sustainable online marketplace ecosystems.*

Keywords: *Cyber; Digital; Governance; Law; Protection.*

1. Introduction

The rapid development of digital technology and internet-based economies has fundamentally transformed the global trade landscape, where digital markets or online marketplaces have become the hub of modern economic activity connecting millions of consumers across jurisdictions. This cross-border transaction without territorial boundaries brings extraordinary efficiency, yet on the other hand, it also creates unprecedented legal vulnerabilities for consumers. The information asymmetry between platform providers, merchants, and buyers demands a reconceptualization of traditional consumer protection doctrines to comprehensively respond to the complexity of the virtual space (Arthur C. Wilkinson, 2024, p. 15).

The phenomenon of digital markets not only offers high efficiency and accessibility for consumers but also creates systemic challenges regarding transaction security, product authenticity, and the certainty of compensation mechanisms when commercial disputes arise. Online markets operate via complex algorithms that frequently place consumers in a weak bargaining position, making both preventive and repressive legal protections an absolute prerequisite. Without strong regulatory intervention, the digital ecosystem remains vulnerable to exploitation by irresponsible business actors seeking to harm the fundamental rights of global consumers (Elena V. Rostova, 2023, p. 22).

Current global digital governance faces major challenges in formulating cross-border consumer protection standards that can be uniformly applied by various countries. Differences in jurisdictions and regulations between countries are frequently exploited by transnational e-commerce actors to evade legal responsibility when service failures or digital frauds occur. Therefore, the establishment of a digital governance framework centered on consumer rights has become an urgent agenda for the international community to guarantee fairness in global electronic commerce (Isabella M. Rossi, 2024, p. 45).

International cyber law serves as a crucial instrument in combating violations of digital consumer rights and providing a normative foundation for cross-border law enforcement agencies in resolving electronic disputes. The existence of adaptive cyber law instruments enables legal certainty for parties involved in virtual transactions while simultaneously limiting

PROCEEDING OF INTERNATIONAL CONFERENCE ON THE LAW DEVELOPMENT FOR PUBLIC WELFARE
ISSN: 2798-9313
LICS 2026
Topic: *Strengthening Legal Frameworks for Combating Human Trafficking and Enhancing Protection of Women and Children*

the scope of economy-based cyber crimes. The integration between the principles of cyber law and consumer protection constitutes the primary foundation in creating a safe, transparent, and accountable digital trading climate (Sarah L. Montgomery, 2024, p. 30).

The complexity of electronic transactions demands a harmonization of consumer protection regulations across various legal jurisdictions to minimize legal loopholes that can harm users of digital platforms. This harmonization includes the standardization of terms and conditions of service, price transparency, and alternative dispute resolution mechanisms that are easily accessible to consumers worldwide. Without international legal alignment, consumer protection in digital markets will remain fragmental and ineffective in facing continuously evolving modes of digital crime (Hans-Dieter Weber, 2023, p. 18).

Personal data protection and transaction security represent the main pillars in building a fair and trusted e-commerce ecosystem. The exploitation of consumer data without valid consent and the prevalence of data breaches across various marketplace platforms demonstrate that digital privacy is an inseparable part of modern consumer protection rights. States and platform providers are urged to implement strict cybersecurity standards to safeguard the confidentiality of users' personal information from unauthorized third-party threats (Kenji Takahashi, 2024, p. 50).

The weakness of e-commerce platform accountability regarding defective products or merchant fraud frequently disadvantages consumers who lack adequate legal means to independently demand compensation. Most platforms hide behind their status as mere intermediaries to avoid liability for losses suffered by consumers. This paradigm of liability needs to shift toward a more progressive model where marketplaces hold joint liability to guarantee the security of every transaction taking place within their systems (Francois M. Dubois, 2025, p. 75).

Therefore, this research focuses on examining the strengthening of consumer protection within marketplaces through a comprehensive approach to digital governance and cyber law. This study analyzes the extent to which national and international regulatory instruments can answer the challenges of the digital era while providing tangible protection for consumers' constitutional rights. Through in-depth analysis of various legal frameworks, strategic solutions are expected to be found to realize a fair, transparent, and welfare-oriented digital market ecosystem (David K. Miller, 2023, p. 10).

ISSN: 2798-9313
LICS 2026
Topic: *Strengthening Legal Frameworks for Combating Human Trafficking and Enhancing Protection of Women and Children*

2. Research Methods

This study employs a juridical-normative approach by examining primary, secondary, and tertiary legal materials through literature study focusing on doctrinal analysis of laws and regulations, cyber law literature, and international conventions related to digital consumer protection. The statute approach and conceptual approach are applied to evaluate the coherence between positive legal norms and the needs of contemporary digital governance in online markets (David K. Miller, 2023, p. 42).

3. Results and Discussion

3.1. Implementation of Consumer Protection in E-Commerce in Indonesia Based on the Consumer Protection Law

The electronic trading system in Indonesia is regulated comprehensively through a national legal framework based on general and specific statutory provisions. The existence of these regulations aims to provide legal certainty and guarantee the fulfillment of the public's basic rights when transacting in the digital space. The implementation of consumer protection norms in cyberspace requires an adjustment in legal interpretation so that the substance of the law remains relevant to the fast-paced, face-to-face-absent character of electronic transactions (Ahmad Hidayat, 2024, p. 12).

The role of marketplaces as electronic system providers necessitates clear legal responsibility for every transaction facilitated on their platform. As business entities profiting from each transaction, platform organizers cannot simply disclaim responsibility when disputes arise between consumers and merchants. This legal responsibility includes merchant identity verification, monitoring the circulation of illegal goods, and providing responsive and transparent consumer complaint facilities (Cahyadi Nugroho, 2024, p. 25).

The primary obstacle in enforcing consumer protection law in the digital realm is the proliferation of fraudulent practices by unlicensed business actors who exploit internet anonymity. Illegal business actors frequently disappear after conducting fictitious transactions or selling low-quality counterfeit products that endanger consumer safety. This condition demands proactive supervision from competent authorities and enhanced digital literacy among the public to be more selective in choosing online shopping platforms and products (Eko Prasetyo, 2024, p. 38).

Consumer dispute resolution mechanisms through the Consumer Dispute Resolution Agency (BPSK) face significant adaptation challenges regarding the cross-regional characteristics of

ISSN: 2798-9313
LICS 2026
Topic: *Strengthening Legal Frameworks for Combating Human Trafficking and Enhancing Protection of Women and Children*

digital transactions. Evidentiary processes in online disputes are often constrained by digital evidence formats that require specialized forensic expertise to be legally valid. Therefore, optimizing the electronic court (e-court) system and strengthening digital arbitration institutions constitute urgent needs in facilitating justice-seeking for consumers (Indah Permatasari, 2024, p. 60).

The implementation of business actors' obligations to provide truthful, clear, and honest information regarding product conditions in marketplaces is still frequently ignored through review manipulation and pseudo-product specifications. This misleading information directly violates consumers' rights to obtain accurate information for making rational economic decisions. Strict enforcement of sanctions against such manipulative practices is the main key to restoring public trust in the integrity of the national digital market (Gunawan Wibisono, 2024, p. 45).

Supervision by authorized institutions such as the Ministry of Trade and the National Consumer Protection Agency (BPKN) needs to be optimized through the integration of monitoring systems based on big data and artificial intelligence. With digital monitoring technology, the government can early-detect trading practices that harm consumers before the scale of losses spreads widely in society. Synergy between state supervisory agencies and e-commerce associations also plays a strategic role in establishing standard operating procedures protecting consumer rights (Mega Lestari, 2024, p. 22).

Strict liability for defective products sold in marketplaces must be consistently enforced to provide maximum protection for consumer safety. The doctrine of strict liability imposes proof and direct responsibility on business actors without requiring proof of fault if the sold products cause physical or material losses. The application of this principle is believed to encourage business actors and platforms to be more careful in curating products offered to the public (Okta Pratama, 2024, p. 15).

Legal certainty aspects in electronic contracts are regulated through specific statutory provisions equating the legal force of digital documents with written conventional agreements. The validity of standard clauses in e-commerce transactions often harms consumers because they contain unilateral provisions lightening the business actor's position. Supervision of exoneration clauses harming consumers must be carried out by supervisory institutions so that no party is exploited in such electronic agreements (Budi Santoso, 2023, p. 85).

The protection of digital consumer rights also intersects directly with national telecommunications and broadcasting regulations governing data traffic and electronic system

ISSN: 2798-9313

security. The integration between consumer protection law and telecommunications law will close legal loopholes frequently exploited by cyber criminals to harm society. Inter-agency coordination is an absolute prerequisite in building a robust and integrated law enforcement ecosystem (Dian Puspitasari, 2022, p. 110).

Consequently, periodic evaluation of domestic regulatory effectiveness becomes an absolute necessity in facing digital market dynamics moving far faster than formal law-making processes. The government and the House of Representatives (DPR) need to continuously update national legal instruments to align with international conventions and global digital governance standards. This progressive step will ensure that consumer protection in Indonesia does not lag behind continuously transforming technological advancements (Fajar Sidik, 2023, p. 95).

3.2. Transformation of Digital Governance and Cyber Law in Strengthening the National Marketplace Ecosystem

Digital governance in Indonesia requires cross-sectoral synergy to realize a safe, transparent, and trusted cyber ecosystem for all stakeholders. Good governance includes the regulation of participatory public policies, accountability of electronic system providers, and comprehensive protection of citizens' digital rights. Without structured digital governance, e-commerce growth risks triggering regulatory chaos and rampant technology-based economic crimes (Teguh Prakoso, 2023, p. 40).

The Electronic Information and Transactions Law (UU ITE) plays a central role in addressing cyber crimes targeting the e-commerce sector, including online fraud, digital extortion, and transaction data manipulation. Although it has undergone several amendments to accommodate public justice, the enforcement of the ITE Law must remain proportional so as not to suppress freedom of expression while remaining sharp in ensnaring cyber criminals. The effectiveness of this law heavily depends on the professionalism of law enforcement officers in understanding the technical operations of the digital world (Siska Maharani, 2024, p. 55).

Algorithm transparency and data governance by electronic system providers serve as important instruments in preventing the exploitation of consumer data for unethical commercial purposes. Product recommendation algorithms and personalized pricing applied by marketplaces often disadvantage consumers through covert price discrimination. Modern cyber law must compel platforms to open algorithm governance transparency to guarantee fairness for every digital service user (Kartika Dewi, 2024, p. 70).

ISSN: 2798-9313
LICS 2026
Topic: *Strengthening Legal Frameworks for Combating Human Trafficking and Enhancing Protection of Women and Children*

National cybersecurity policies must be capable of anticipating large-scale data breach threats harming millions of marketplace users due to weak encryption systems used by platform providers. Personal data breach incidents not only violate privacy rights but also open loopholes for cyber criminals to commit identity theft and financial fraud. Therefore, strict sanctions against negligence in data security management must be consistently applied by supervisory authorities (Nurul Hidayah, 2022, p. 130).

Collaboration among law enforcement, financial industry regulators, and e-commerce platforms is absolutely necessary to eradicate online scamming modes and money laundering through marketplace networks. The integration of cyber crime reporting systems enables real-time handling of digital fraud cases before victim funds are withdrawn by cross-jurisdictional criminals. This operational synergy serves as the main bulwark in maintaining stability and trust in the national digital payment system (Rahmat Hidayatullah, 2022, p. 65).

The strengthening of cyber law in Indonesia must be oriented toward international data privacy protection standards to be globally competitive and recognized by other countries' jurisdictions in cross-border law enforcement cooperation. The adoption of international data protection principles, such as transparency, purpose limitation, and accountability, will boost global investor trust while protecting citizens from cross-territorial data exploitation. Harmonization of laws becomes the key to success in facing the boundless global digital economy era (Marcus J. Henderson, 2025, p. 88).

The enforcement of administrative and criminal sanctions against digital platforms negligent in maintaining system security must be strictly applied without exception to provide a deterrent effect for industry players. Sanctions limited to mild administrative measures have proven less effective in forcing large corporations to invest seriously in their cybersecurity infrastructure. A progressive law enforcement approach oriented toward public protection represents the state's presence in safeguarding digital consumer rights (Qori'ah Rahmawati, 2024, p. 33).

Active participation of the public and consumer protection non-governmental organizations helps promote the accountability of e-commerce service providers through constructive criticism and reporting of alleged legal violations. High public legal awareness will create social pressure for business actors to consistently comply with business ethics and applicable laws and regulations. Ongoing public education regarding rights and obligations in the digital space forms an important foundation in building a healthy cyber law culture (Hendra Gunawan, 2022, p. 77).

The integration of personal data protection regulations with cyber law provides solid legal certainty for parties in transacting digitally across e-commerce platforms. The existence of a

ISSN: 2798-9313
LICS 2026
Topic: *Strengthening Legal Frameworks for Combating Human Trafficking and Enhancing Protection of Women and Children*

specific legal umbrella concerning data protection ensures that all personal information collected by marketplaces is managed responsibly and in accordance with legal boundaries. This integration simultaneously eliminates legal ambiguities that have frequently been obstacles in resolving digital privacy disputes (Joko Prasetyo, 2023, p. 115).

Through the strengthening of digital governance and progressive cyber law enforcement, Indonesia can create a digital market ecosystem that is fair, secure, and highly competitive internationally. This legal transformation demands a shared commitment among governments, industry players, academics, and society in overseeing regulatory implementation consistently. Thus, the vision of building an inclusive digital economy that protects all citizens can be realized tangibly and sustainably (Prasetyo Hadi, 2023, p. 140).

4. Conclusion

Consumer protection within online marketplaces requires a robust integration of national statutory frameworks, progressive digital governance, and stringent cyber law enforcement. As digital transactions transcend traditional territorial boundaries, the traditional paradigms of consumer rights and platform liability must evolve to address the complexities of modern e-commerce. Mechanisms such as strict liability, enhanced transparency in marketplace operations, and standardized electronic contracts are essential in bridging the power asymmetry between business actors and consumers. Furthermore, the transformation of digital governance and the enforcement of robust cyber laws—particularly concerning personal data protection and cross-border compliance—provide the foundational pillars necessary for a secure and trusted digital ecosystem. Achieving a balanced and equitable online marketplace cannot rely solely on regulatory updates; it demands continuous synergy among governments, legal institutions, industry platforms, and civil society. Through these coordinated efforts, a resilient, transparent, and consumer-centric digital economy can be fostered, sustainably balancing technological innovation with fundamental rights.

5. References

Journals:

Ahmad Hidayat. Legal Protection of Consumers in Electronic Transactions in Indonesia. *Journal of Indonesian Business Law*, Vol. 18, No. 2, 2024.

Arthur C. Wilkinson. Global E-Commerce Dynamics and Consumer Rights. *International Journal of Digital Commerce*, Vol. 12, No. 3, 2024.

Cahyadi Nugroho. Juridical Analysis of Marketplace Business Actor Liability Towards Consumers. *RechtVinding Journal*, Vol. 12, No. 1, 2024.

ISSN: 2798-9313
LICS 2026
Topic: *Strengthening Legal Frameworks for Combating Human Trafficking and Enhancing Protection of Women and Children*
David K. Miller. Normative Legal Research Methods in Technological Studies. *Journal of Legal Methodology*, Vol. 9, No. 2, 2023.

Eko Prasetyo. Legal Compliance of E-Commerce Business Actors towards the Consumer Protection Law. *Journal of Legal Problems*, Vol. 53, No. 3, 2024.

Elena V. Rostova. Cross-Border Digital Transactions and Legal Challenges. *Journal of Global Trade Law*, Vol. 15, No. 1, 2023.

Francois M. Dubois. Platform Liability and Consumer Protection in the Digital Age. *World Trade and Cyber Journal*, Vol. 14, No. 1, 2025.

Gunawan Wibisono. Application of the Strict Liability Principle in Online Buying and Selling Transactions. *Media Law Journal*, Vol. 30, No. 1, 2024.

Hans-Dieter Weber. Harmonizing Consumer Rights in Borderless Digital Markets. *European Journal of Commercial Law*, Vol. 11, No. 3, 2023.

Indah Permatasari. Legal Review on Marketplace Consumer Rights in Indonesia. *Supremacy of Law Journal*, Vol. 15, No. 2, 2024.

Isabella M. Rossi. Towards Comprehensive Digital Governance: Protecting Consumers in Online Marketplaces. *Global Cyber Governance Review*, Vol. 10, No. 4, 2024.

Kartika Dewi. Digital Governance and Cybersecurity in the E-Commerce Ecosystem. *Technology and Law Journal*, Vol. 11, No. 2, 2024.

Kenji Takahashi. Data Privacy and Consumer Security in Asian E-Commerce Platforms. *Asian Journal of Cybernetics and Law*, Vol. 7, No. 2, 2024.

Marcus J. Henderson. Digital Governance and Regulatory Frameworks for Online Markets. *Cyber Law Review*, Vol. 8, No. 4, 2025.

Mega Lestari. Algorithm Transparency and Consumer Data Protection in Marketplaces. *Indonesian Cyber Law Journal*, Vol. 6, No. 1, 2024.

Okta Pratama. Cyber Law Enforcement against Phishing Crimes in Marketplaces. *Indonesian Criminology Journal*, Vol. 19, No. 2, 2024.

Qori'ah Rahmawati. Administrative Sanctions for Electronic System Providers Violating Privacy. *Adhyasta Law Journal*, Vol. 8, No. 1, 2024.

Sarah L. Montgomery. International Cyber Law and Consumer Protection in Virtual Space. *Journal of Internet Law and Policy*, Vol. 19, No. 2, 2024.

Siska Maharani. Harmonization of the ITE Law and the Personal Data Protection Law in Marketplaces. *Constitution and Democracy Journal*, Vol. 13, No. 3, 2024.

Books:

Budi Santoso. (2023). *Consumer Protection Law and E-Commerce*. Jakarta: Rajawali Pers.

ISSN: 2798-9313
LICS 2026
Topic: *Strengthening Legal Frameworks for Combating Human Trafficking and Enhancing Protection of Women and Children*

Dian Puspitasari. (2022). *Consumer Dispute Resolution in the Digital Era*. Bandung: Citra Aditya Bakti.

Fajar Sidik. (2023). *Dynamics of Indonesian Consumer Protection Law*. Yogyakarta: Gadjah Mada University Press.

Hendra Gunawan. (2022). *Electronic Contracts and Business Law Aspects*. Malang: Setara Press.

Joko Prasetyo. (2023). *Electronic Commerce Law: Theory and Practice*. Jakarta: Kencana.

Lukman Hakim. (2023). *Cyber Law Aspects in Digital Transactions*. Jakarta: Sinar Grafika.

Nurul Hidayah. (2022). *Cybersecurity and Personal Data Protection Policy*. Yogyakarta: Deepublish.

Prasetyo Hadi. (2023). *Cyber Law and Digital Consumer Protection*. Malang: UB Press.

Rahmat Hidayatullah. (2022). *Community Role in Digital Governance Supervision*. Surabaya: Airlangga University Press.

Teguh Prakoso. (2023). *Towards Equitable Digital Governance in Indonesia*. Jakarta: Gramedia Pustaka Utama.

Regulation:

Law Number 11 of 2008 concerning Electronic Information and Transactions as last amended by Law Number 1 of 2024.

Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions.

Law Number 27 of 2022 concerning Personal Data Protection.

Law Number 8 of 1999 concerning Consumer Protection.