Open access: https://journal.icpa-banyuwangi.ac.id/index.php/skyhawk

SKYHAWK: Jurnal Aviasi Indonesia
Volume. 7, Number. 1, 2027, pp. 895-912

P-ISSN: 2745-6102
E-ISSN: 2776-3854

Consumer Protection in the Digital Economy Era: A Literature Analysis of E-Commerce Regulation in Indonesia

La Ode Mbunai[1], Syaiful Bahari[2], La Ode Irman Jaya[3], Fitra Rahmadani[4], Zahra Malinda Putri[5], Muhammad Panca Prana Mustaqim Sinaga[6], H.S Ulil Albab[7], St. Muslimah Suciati[8]
[12567]Department of Law, Indonesia University of Sciences, Bekasi, Indonesia
[3]Department of Medical, University of Warsaw, Poland
[4]Master's Student in Notarial Law, Pancasila University, Jakarta, Indonesia
[8]Department of Law, Halu Oleo University, Kendari, Indonesia

Email Address: syaifulbahari726@gmail.com[2], laode.jaya@wum.edu.pl[3], fitrarahmadani092@gmail.com[4], zahra.malinda@lecturer.sains.ac.id[5], pancasinaga13@gmail.com[6], muhammad.panca@lecturer.sains.ac.id[7], sitimuslimahsuciati@gmail.com[8]
Email Correspondence: la.ode@lecturer.sains.ac.id[1]

ARTICLE INFO

Article History

Received: May 18, 2026
Revised: August 31, 2026
Accepted: November 02, 2026

Keywords

Consumer protection, Digital literacy, Digital regulation, E-commerce, PDP Law

This is an open access article under the CC BY-SA license.
Copyright ©2025 by the Author. Published by Akademi Penerbangan Indonesia.

ABSTRACT

The growth of Indonesia's digital economy has driven a significant transformation in transaction patterns while posing new challenges regarding consumer protection. Although the Consumer Protection Law and Personal Data Protection Law have been passed, they are not considered optimal in responding to the complexity of the digital ecosystem. This research uses a descriptive qualitative approach based on a structured literature review combined with doctrinal legal analysis and thematic synthesis. This study aims to evaluate the effectiveness of consumer protection regulations in e-commerce transactions in Indonesia by examining legal studies, consumer behavior, and international regulatory comparisons through a literature review approach. The study's results show that regulatory implementation weaknesses, low digital literacy, insufficiently standardized online dispute resolution mechanisms, and institutional enforcement and supervisory gaps remain important obstacles. Additionally, an overly rigid ex-ante regulatory approach has the potential to stifle digital innovation. Therefore, adaptive, participatory policy reformulation based on the principle of equitable consumer protection is needed.

1. INTRODUCTION

The digitalization of the economy has accelerated the development of digital business activities in Indonesia, including fintech and other technology-enabled services, creating a growing need for an adaptive legal framework to balance innovation, consumer protection, and accountability. This shift has significantly affected communication, education, financial transactions, and business operations (Kharisma, 2020). The transformation of the digital economy has also created new forms of interaction and knowledge sharing through digital platforms, reflecting the changing nature of economic activity in the digital era (Yang et al., 2024). Indonesia's digital economy has expanded rapidly through e-commerce, digital transportation, educational technologies, and fintech services. This development requires an adaptive legal framework capable of balancing innovation, market development, consumer protection, and accountability. The development of an inclusive digital economy also requires cooperation among public and private actors and broader institutional coordination within the digital ecosystem (Ha & Chuah, 2023). A robust and inclusive digital ecosystem requires collaboration among government institutions, private-sector actors, academia, and civil society. In this context, digital consumer protection must be understood not only as a matter of individual consumer awareness but also as a matter of platform governance, corporate compliance, data protection, and effective digital dispute resolution.

The e-commerce ecosystem is also increasingly connected with transportation, logistics, and supply-chain activities because digital transactions depend on fulfillment, delivery, information exchange, and coordination among multiple service actors. This connection is particularly relevant in Indonesia, where the growth of e-commerce creates increasing demand for reliable and integrated logistics services. Recent transportation and logistics research published in SKYHAWK also identifies the growth of e-commerce as a factor intensifying demand for fast, reliable, and integrated logistics distribution (Candrarahayu et al., 2026). From a consumer-protection perspective, this interconnected ecosystem means that digital consumer protection cannot be considered solely at the point of online transaction; it also relates to the governance of service interfaces that support the delivery and fulfillment of digitally purchased goods.

Nevertheless, digital transformation presents considerable legal challenges, particularly in consumer protection, platform accountability, and personal data privacy. Indonesia has responded through Law No. 8 of 1999 on Consumer Protection (UUPK), Law No. 27 of 2022 on Personal Data Protection (PDP Law), Law No. 11 of 2008 on Electronic Information and Transactions as amended, most recently, by Law No. 1 of 2024, and Government Regulation No. 80 of 2019 on Trading Through Electronic Systems. Law No. 1 of 2024, effective since 2 January 2024, amended several provisions of the ITE Law and is relevant to the governance of electronic systems, users, and digital information (Indonesia, 2024). These instruments demonstrate that Indonesia has developed a substantial legal framework; however, the central challenge is increasingly located in implementation, institutional supervision, platform accountability, and the compatibility of regulatory mechanisms with rapidly changing digital markets.

Recent literature also reveals a gap between formal legal rules and their implementation. Digital marketplaces operate within a broader transaction and service ecosystem that includes sellers, platforms, payment providers, fulfillment services, and transportation or delivery actors. Within this ecosystem, digital marketplaces already operate internal complaint and dispute-resolution mechanisms, including refund procedures, transaction verification, escrow arrangements,

seller sanctions, and platform-based complaint handling. These mechanisms can be understood as a decentralized or platform-based form of Online Dispute Resolution (ODR). However, their legal position, procedural transparency, accountability, human-review mechanisms, and relationship with formal dispute-resolution institutions remain insufficiently standardized. At the same time, the regulatory position of platforms must be distinguished from the liability of sellers. For Private Electronic System Providers (PSE), Minister of Communication and Informatics Regulation No. 5 of 2020, as amended by Regulation No. 10 of 2021, provides an important regulatory foundation for registration, governance, content moderation, and platform responsibilities (Republic of Indonesia, 2020).

Comparative research also demonstrates that personal data protection requires structural accountability rather than relying exclusively on consumer awareness. Indonesia's PDP Law establishes obligations for data controllers and processors, including requirements concerning lawful processing, security, accountability, and the appointment of officials or officers performing personal data protection functions in specified circumstances under Article 53 (Indonesia, 2022). The law therefore supports a corporate-compliance approach in which protection is incorporated into organizational processes and system design. The principles commonly associated with Privacy by Design and Privacy by Default are relevant in this context because privacy safeguards should be considered from the design stage of digital services rather than imposed only after a violation occurs. Nevertheless, regulatory safeguards must remain proportionate so that consumer protection does not unnecessarily suppress innovation. The effectiveness of digital regulation therefore depends on balancing ex-ante safeguards, ex-post enforcement, institutional capacity, and consumer rights.

In light of these considerations, this study aims to evaluate the adequacy and effectiveness of Indonesia's consumer protection framework in addressing the evolving challenges of e-commerce and the broader digital economy. The analysis focuses on the interaction between the Consumer Protection Law (UUPK), the Personal Data Protection Law (PDP Law), the ITE Law as amended by Law No. 1 of 2024, Government Regulation No. 80 of 2019, and regulations governing electronic system providers and electronic commerce. Particular attention is given to the gap between formal regulatory provisions and practical implementation, including consumer literacy, corporate compliance, platform accountability, privacy governance, platform-based online dispute resolution (ODR), and comparative regulatory developments. Accordingly, this study addresses three research questions: (1) How adequate and effective is Indonesia's existing legal framework for protecting consumers in e-commerce transactions in addressing the challenges of the digital economy? (2) What implementation, institutional, platform-accountability, privacy-governance, and dispute-resolution gaps affect the effectiveness of consumer protection in Indonesia's e-commerce ecosystem? and (3) What regulatory lessons and policy directions from comparative approaches can support a more adaptive, accountable, and consumer-oriented framework for e-commerce regulation in Indonesia?

The contribution of this study lies in providing an integrated legal synthesis that connects Indonesia's fragmented consumer-protection, personal-data, electronic-transaction, and platform-governance frameworks with their practical implementation challenges. Rather than treating consumer literacy, corporate compliance, platform accountability, and dispute resolution as separate regulatory issues, the study examines them as interconnected components of digital consumer protection. In particular, the analysis conceptualizes marketplace complaint-handling and dispute-resolution mechanisms as an emerging form of decentralized, platform-based ODR and identifies the

minimum legal safeguards required for transparency, fairness, human review, data protection, evidence preservation, accountability, and escalation to formal dispute-resolution institutions. The study further connects these findings with comparative regulatory developments to formulate policy directions for a more adaptive and accountable consumer-protection framework in Indonesia.

2. METHODS

Research Design

This study employed a descriptive qualitative research design using a structured literature review combined with doctrinal legal analysis and thematic synthesis. The review was designed to examine the adequacy and implementation of Indonesia's consumer protection framework in e-commerce and to identify regulatory lessons from comparative approaches. In accordance with the research questions, the analysis focused on the relationship between consumer protection law, electronic transactions, personal data protection, platform governance, institutional enforcement, online dispute resolution, and comparative regulatory developments.

The review was conducted as a structured literature review with doctrinal and thematic legal analysis rather than a statistical systematic review or meta-analysis. The study did not estimate causal effects or produce quantitative effect-size estimates. Instead, it synthesized legal norms, scholarly findings, comparative regulatory developments, and documented policy issues to address the research questions concerning the adequacy, implementation gaps, and future regulatory directions of consumer protection in Indonesia's e-commerce ecosystem.

Population and Sample

For this literature-based study, the population consisted of scholarly publications relevant to consumer protection and regulation in the digital economy, particularly e-commerce and electronic transactions. The evidence sample consisted of scholarly journal articles selected through predefined eligibility criteria. The literature search used five academic search and discovery platforms identified in the research design: Google Scholar, ResearchGate, ScienceDirect, SpringerLink, and the Directory of Open Access Journals (DOAJ). The search strategy used nine predefined keywords: "digital economy law," "fintech and economic law in Indonesia," "online consumer protection policy," "digital economy legal certainty," "digital consumer protection," "Indonesian digital economy regulation," "electronic transaction regulation," "personal data protection law," and "ITE Law."

For the search strategy, the predefined keywords were conceptually organized using Boolean operators to combine broader digital-economy and legal-regulatory terms with consumer-protection, electronic-commerce, data-protection, and ITE-related terms. The search framework therefore used OR to combine related terms within a conceptual category and AND to connect the relevant categories. Illustrative combinations included ("digital economy law" OR "digital economy regulation" OR "digital economy legal certainty") AND ("consumer protection" OR "online consumer protection" OR "digital consumer protection"), as well as ("electronic transaction regulation" OR "ITE Law") AND ("consumer protection" OR "e-commerce"). These combinations were used as a reproducible search framework for identifying literature relevant to the research questions.

The literature was restricted to publications issued between 2015 and 2025, written in Indonesian or English, available in full text, and substantively relevant to consumer protection, e-commerce, digital economy regulation, electronic transactions, personal data protection, platform governance, or online dispute resolution. Comparative studies were included when their regulatory

findings provided relevant lessons for Indonesia. Publications were excluded when they were outside the 2015–2025 period, duplicate records, lacked sufficient relevance to the research questions, focused exclusively on technical, economic, marketing, or other non-legal issues without a relevant regulatory dimension, lacked verifiable full-text information, or did not provide a substantive contribution to the analysis.

The quality of the included literature was assessed through relevance, substantive contribution to the research questions, availability of verifiable full-text information, and the extent to which each publication provided a clear legal, regulatory, institutional, or comparative basis for analysis. Because this study is a qualitative legal literature review rather than a quantitative systematic review or meta-analysis, no statistical risk-of-bias instrument or effect-size appraisal was applied. Studies that did not meet the substantive relevance and source-verifiability requirements were excluded from the core evidence base.

The screening process consisted of identification, duplicate removal, title and abstract screening, full-text eligibility assessment, and final inclusion. The original database-level search log was not retained; therefore, the exact number of records retrieved from each platform, duplicates removed, records screened, full texts assessed, and records excluded at each stage cannot be reconstructed reliably. For this reason, the study does not report retrospective PRISMA flow counts that could not be verified. Instead, the review transparently reports the search platforms, predefined keywords, eligibility criteria, screening stages, and final evidence base. Following the eligibility assessment, 25 journal articles were retained as the core scholarly evidence base for the qualitative synthesis.

Table 1. Evidence Base of Included School 1

No.	Author(s) & Year	Main Focus	Context / Scope	Key Relevance to the Review	RQ
1	Kharisma, 2020 (Kharisma, 2020)	Digital economy and fintech regulation	Indonesia	Provides contextual understanding of Indonesia's digital economy and the need for adaptive legal regulation.	RQ1
2	Yang et al., 2024 (Yang et al., 2024)	Digital economy development	Digital economy	Provides contextual evidence on the changing digital-economy environment underlying the need for adaptive regulation.	RQ1
3	Ha & Chuah, 2023 (Ha & Chuah, 2023)	Digital economy challenges and opportunities	Southeast Asia	Provides regional context on digital-economy development and cooperation among public and private actors.	RQ3
4	Susanti Sari et al., 2024 (Susanti Sari et al., 2024)	Legal protection in e-commerce transactions	Indonesia	Examines consumer legal protection and the position of consumers in electronic commerce.	RQ1
5	Azzaprillia, 2023 (Azzaprillia, 2023)	E-commerce opportunities and legal challenges	Indonesia	Identifies regulatory challenges involving consumer protection, personal data,	RQ1/RQ2

No.	Author(s) & Year	Main Focus	Context / Scope	Key Relevance to the Review	RQ
				competition, intellectual property, and taxation.	
6	Azis et al., 2024 (Romdoni, 2024)	Consumer protection in e-commerce	Indonesia	Examines the implementation of Government Regulation No. 80 of 2019 and information obligations in electronic transactions.	RQ1/RQ2
7	Wibowo & Retno Mumpuni, 2024 (Wibowo & Retno Mumpuni, 2024)	Consumer protection and platform responsibility	Grab Toko platform	Provides a case study illustrating consumer-protection problems and delayed complaint resolution in an e-commerce platform context.	RQ2
8	Lubis, 2022 (Lubis, 2022)	Cybercrime and e-commerce transactions	Indonesia	Highlights cybercrime, data forgery, privacy violations, and challenges to conventional enforcement.	RQ2
9	Septiningsih & Karimullah, 2024 (Septiningsih & Karimullah, 2024)	Consumer protection in the digital era	Indonesia	Identifies continuing consumer-literacy and consumer-protection challenges in e-commerce.	RQ2
10	Dudi Badruzaman, 2025 (Dudi Badruzaman, 2025)	Legal protection of consumers in e-commerce	Indonesia	Provides legal analysis of consumer protection and implementation challenges in online transactions.	RQ1/RQ2
11	Fauzie, 2024 (Fauzie, 2024)	Personal data protection and privacy	Indonesia / IoT	Examines implications of Indonesia's Personal Data Protection Law for data privacy and institutional protection.	RQ2
12	Judijanto et al., 2024 (Judijanto et al., 2024)	Data-protection regulation and privacy rights	Indonesia	Identifies gaps between formal data-protection regulations and practical implementation of privacy rights.	RQ2
13	Handoyo, 2024 (Handoyo, 2024)	Consumer trust, risk and security	E-commerce	Provides evidence concerning trust, perceived risk, security, and electronic word-of-mouth in digital purchasing.	RQ2
14	Rohaini et al., 2025 (Rohaini et al., 2025)	Online dispute resolution	E-commerce	Examines the need to reform ODR regulation to improve legal certainty and consumer protection.	RQ2
15	Hardigaluh & Pulungan, 2022 (Hardigaluh & Pulungan, 2022)	Comparative consumer-protection regulation	Indonesia, India & United States	Provides comparative evidence on legal certainty and consumer protection across	RQ3

No.	Author(s) & Year	Main Focus	Context / Scope	Key Relevance to the Review	RQ
				different regulatory approaches.	
16	Arai, 2025 (Arai, 2025)	Ex-ante and ex-post digital regulation	Comparative digital markets	Provides comparative evidence concerning regulatory approaches and adaptive regulation in digital markets.	RQ3
17	Bintarawati & Rismana, 2024 (Bintarawati & Rismana, 2024)	Effectiveness of consumer protection law	Indonesia	Examines the effectiveness of consumer protection law for e-commerce users in the digital economy era.	RQ1
18	Dzuhriyan et al., 2025 (Dzuhriyan et al., 2025)	Consumer legal protection in online transactions	Indonesia	Identifies challenges and opportunities in consumer legal protection within Indonesia's digital economy.	RQ1/RQ2
19	Widiarty et al., 2024 (Widiarty et al., 2024)	Consumer protection in commercial transactions	Indonesia	Examines consumer rights and legal safeguards in Indonesian commercial transactions.	RQ1
20	Satwiko, 2021 (Satwiko, 2021)	Privacy and data protection	Indonesia	Provides a legal framework for understanding privacy and personal-data protection in Indonesia.	RQ2
21	Sudarwanto & Kharisma, 2021 (Sudarwanto & Kharisma, 2021)	Comparative personal-data protection	Indonesia, Hong Kong & Malaysia	Provides comparative regulatory perspectives on personal-data protection and institutional safeguards.	RQ2/RQ3
22	Maleno & Kusumawati (2024)(Maleno & Kusumawati, 2024)	Comparative data-protection law	Indonesia, EU & California	Compares data-protection frameworks and identifies regulatory practices relevant to privacy protection in Indonesia.	RQ2/RQ3
23	Iman, 2024 (Iman, 2024)	Data, privacy and digital platforms	Digital platforms	Examines the relationship between personal data, privacy, and digital-platform governance.	RQ2
24	Belwal et al., 2020 (Belwal et al., 2020)	Consumer protection and e-commerce	Oman	Provides comparative evidence on consumer protection in electronic commerce from another jurisdiction.	RQ3
25	Salisu et al., 2025 (Salisu et al., 2025)	E-commerce policy and regional cooperation	ASEAN	Provides regional policy evidence concerning e-commerce cooperation and regulatory strategies among ASEAN countries.	RQ3

Data Collection Technique

Data were collected through documentary literature searching and legal-document review. Scholarly publications were identified using the predefined keywords and search platforms, while primary legal materials were collected separately as authoritative sources for the doctrinal analysis. The primary legal materials examined included the Consumer Protection Law, Personal Data Protection Law, ITE Law as amended by Law No. 1 of 2024, Government Regulation No. 80 of 2019, and regulations concerning electronic system providers and electronic commerce. These legal materials were not treated as journal articles in the evidence sample but were analyzed alongside the selected scholarly literature to assess the development and implementation of Indonesia's regulatory framework.

Because the original database-level search log was not retained, the number of records initially retrieved from each platform could not be reconstructed reliably. Accordingly, database-specific retrieval counts are not retrospectively reported. Instead, the study documents the search platforms, keywords, eligibility criteria, screening stages, and final evidence base of 25 journal articles to maintain methodological transparency.

Data Analysis Technique

The selected literature was analyzed using thematic synthesis and doctrinal legal interpretation. First, the 25 selected journal articles were organized according to their relevance to the three research questions. Second, each article was coded according to its substantive focus, regulatory issue, institutional or actor dimension, and relevance to RQ1, RQ2, or RQ3. The thematic coding focused on the effectiveness of the consumer protection framework, implementation and institutional gaps, platform accountability, consumer literacy, corporate compliance, personal-data and privacy governance, online dispute resolution, and comparative regulatory approaches. Third, related codes were grouped into broader analytical themes that corresponded to the structure of the Results and Discussion sections. Fourth, the findings from the scholarly literature were examined alongside the relevant Indonesian legal framework. Fifth, the evidence was synthesized to distinguish documented findings from doctrinal interpretation and the authors' normative analysis. This analytical distinction was used to ensure that findings reported from the literature were not presented as empirical findings generated independently by the authors. Finally, the synthesized evidence was used to formulate the regulatory analysis and policy directions concerning consumer protection in Indonesia's e-commerce ecosystem.

3. RESULTS

Findings on the Indonesian Consumer Protection Framework

The reviewed literature indicates that Indonesia has developed a substantial legal framework for consumer protection in e-commerce. The Consumer Protection Law (UUPK), ITE Law as amended by Law No. 1 of 2024, Personal Data Protection Law, Government Regulation No. 80 of 2019, and regulations concerning electronic system providers and electronic commerce collectively provide legal foundations for digital transactions and consumer protection. Sari et al. (2024) emphasize the continuing importance of consumer protection because consumers may have weaker economic resources, information, education, and bargaining power than business actors (Susanti Sari et al., 2024).

The literature also identifies continuing regulatory and implementation challenges. Azzaprillia (2024) identifies consumer and personal-data protection, business competition, intellectual property, and taxation among the regulatory issues associated with e-commerce development in Indonesia (Azzaprillia, 2023). Romdoni (2024) notes that the implementation of Government Regulation No. 80 of 2019, including requirements concerning business information, remains uneven. These findings indicate that the existence of legal provisions does not automatically ensure consistent implementation across digital transactions (Romdoni, 2024).

The reviewed literature further identifies challenges associated with cybercrime, data forgery, privacy violations, and other digital risks (Lubis, 2022). Wibowo and Mumpuni (2024), through their case study of the Grab Toko platform, document consumer-protection problems associated with e-commerce transactions and complaint resolution. Taken together, these findings show that consumer protection in e-commerce involves not only substantive consumer rights but also implementation, platform governance, information management, and access to remedies (Wibowo & Retno Mumpuni, 2024).

Findings on Consumer Literacy, Corporate Compliance, and Privacy Governance

The reviewed literature identifies consumer literacy as an important component of digital consumer protection. Septiningsih (2024) and Badruzaman (2025) identify continuing gaps in consumer understanding of rights and complaint procedures (Dudi Badruzaman, 2025; Septiningsih & Karimullah, 2024). Fauzie (2024) and Judijanto et al. (2024) also identify challenges concerning privacy awareness and the implementation of data-protection rights (Fauzie, 2024; Judijanto et al., 2024). The literature further indicates that consumer protection involves obligations beyond consumer awareness. The Personal Data Protection Law establishes obligations for personal-data controllers and processors, including organizational responsibilities for personal-data protection. Handoyo (2024) identifies trust, perceived risk, perceived security, and electronic word-of-mouth as relevant factors in digital purchasing behavior (Handoyo, 2024). Satwiko (2021), Sudarwanto and Kharisma (2022), and Maleno and Kusumawati (2024) provide additional perspectives concerning Indonesia's personal-data protection framework and comparative data-protection regulation (Maleno & Kusumawati, 2024; Satwiko, 2021; Sudarwanto & Kharisma, 2021).

The reviewed evidence therefore identifies two interconnected dimensions of digital consumer protection: consumer capability and institutional or corporate safeguards. The literature does not support an approach based exclusively on consumer awareness, as privacy and transaction risks are also affected by organizational compliance, platform practices, and regulatory supervision.

Findings on Platform-Based Dispute Resolution and Comparative Regulation

The literature identifies the emergence of digital and platform-based mechanisms for handling consumer complaints and disputes. Rohaini et al. (2025) discuss the development of online dispute-resolution mechanisms in e-commerce, including technology-assisted complaint handling (Rohaini et al., 2025). Government Regulation No. 80 of 2019 also provides a legal basis for electronic complaint and dispute-resolution arrangements. The reviewed literature also provides comparative evidence. Hardigaluh and Pulungan (2022) compare consumer-protection regulation in Indonesia, India, and the United States, identifying differences in regulatory approaches concerning legal certainty, transparency, and consumer protection (Hardigaluh & Pulungan, 2022). Belwal et al. (2021) provide evidence from Oman concerning consumer protection and electronic commerce,

while Salisu et al. (2025) examine policy developments affecting e-commerce cooperation among ASEAN countries (Belwal et al., 2020; Salisu et al., 2025).

Comparative data-protection literature also identifies institutional accountability as an important element of effective regulation. Sudarwanto and Kharisma (2022) compare data-protection regulations in Indonesia, Hong Kong, and Malaysia, while Maleno and Kusumawati (2024) compare Indonesia's framework with the European Union and California (Maleno & Kusumawati, 2024; Sudarwanto & Kharisma, 2021). The comparative literature indicates differences in institutional arrangements, regulatory design, and approaches to digital consumer and data protection.

4. DISCUSSION

Regulatory Fragmentation and Shared Responsibility

The findings indicate that the central challenge in Indonesian digital consumer protection is not merely the absence of legal instruments. Indonesia has established multiple legal instruments governing consumer rights, electronic transactions, personal data protection, and electronic commerce. The more significant issue concerns the coordination, implementation, and enforcement of these instruments across different actors and institutional domains. This regulatory fragmentation has practical implications because e-commerce transactions involve multiple actors, including consumers, sellers, platforms, payment providers, and public authorities. Each actor performs different functions and consequently requires a corresponding allocation of rights, obligations, and responsibilities. Consumer protection therefore cannot be addressed effectively through a single regulatory instrument or by placing responsibility exclusively on consumers or sellers.

The findings support a shared-responsibility approach in which consumer protection is distributed according to the role and function of each actor within the digital transaction ecosystem. Such an approach requires consistency between substantive consumer rights, platform obligations, personal-data governance, institutional supervision, and mechanisms for resolving consumer complaints and disputes.

Platform Accountability and Differentiated Liability

The findings concerning the Grab Toko case demonstrate the practical importance of platform accountability in e-commerce transactions. However, platform accountability should not be interpreted as establishing identical liability for every e-commerce platform or as automatically equating platforms with sellers. The responsibility of each actor needs to be determined according to its role, contractual relationship, activities, and applicable legal obligations. This distinction becomes increasingly relevant as digital platforms perform functions beyond providing technological infrastructure. Platforms may facilitate transaction information, payment processes, seller management, consumer complaints, and other aspects of marketplace governance. Their position within the transaction structure therefore creates responsibilities that are different from, but complementary to, those of sellers.

Accordingly, the regulatory framework should establish differentiated responsibilities based on the actual functions performed by each actor. Sellers remain responsible for their products, services, and compliance with applicable consumer-protection obligations, while platforms should be accountable for functions and risks arising from their own systems and marketplace activities.

This allocation can provide greater legal clarity while preventing either excessive platform liability or insufficient accountability for platform-related risks.

This differentiated responsibility is also relevant when e-commerce transactions are connected with fulfillment, transportation, and delivery services. In such transactions, consumer protection may involve several interconnected service interfaces, including the seller, digital platform, payment or fulfillment provider, and transportation or delivery service provider. The allocation of responsibility should therefore consider the specific function performed by each actor, the degree of control over the relevant transaction or service stage, and the applicable legal obligations. This approach allows consumer protection to be extended across the digital commerce and logistics ecosystem without imposing identical liability on actors that perform different functions.

The distinction between platform accountability and seller liability should also be considered in relation to the intermediary function of digital platforms. PP No. 80 of 2019 recognizes intermediary services and provides differentiated treatment for certain intermediary functions, including mere conduit, caching, and hosting. For hosting functions, the regulatory framework provides a conditional limitation of responsibility where the intermediary lacks actual knowledge of unlawful information and, after obtaining such knowledge, takes the required action to remove or disable access to the relevant information. This framework can be understood as a form of conditional safe-harbor approach rather than an absolute exemption from liability. Accordingly, a platform should not be treated as automatically liable for every act of a seller merely because the transaction occurs through its system. However, the platform's responsibility may arise from its own functions, regulatory obligations, knowledge, control, or failure to take appropriate action after receiving information concerning unlawful content or conduct (Indonesia, 2019).

The possibility of platform liability should also be distinguished from the potential application of Article 1365 of the Indonesian Civil Code concerning unlawful acts (voor Indonesie, 2014). Article 1365 establishes liability where the elements of an unlawful act, fault, loss, and causal relationship are satisfied. Therefore, the involvement of both a seller and a platform in the same transaction does not by itself establish joint liability. Joint or concurrent responsibility would require an assessment of the conduct of each actor and whether the platform's own act or omission contributed causally to the consumer's loss. This approach preserves the distinction between liability arising from the seller's underlying transaction or product and liability arising from the platform's own conduct or failure to perform applicable duties. It also provides a basis for assessing platform responsibility according to actual control, knowledge, and contribution to the harm rather than imposing automatic liability merely because the platform facilitated the transaction.

Decentralized and Interoperable ODR

The findings concerning platform-based complaint mechanisms and comparative regulatory developments have implications for the design of online dispute resolution (ODR) in Indonesia. Digital dispute resolution does not necessarily have to depend on a single centralized mechanism. Platform-based complaint systems can provide an initial layer of redress because transaction records, payment information, communication records, and seller information are already available within the digital transaction environment.

However, platform-based ODR requires minimum procedural safeguards to ensure that digital convenience does not undermine consumer rights. These safeguards should include accessibility, transparency of procedures, clear information regarding dispute status and outcomes, human review

for contested cases, protection of personal data, preservation of electronic evidence, and an effective mechanism for escalation to formal alternative dispute resolution or judicial proceedings.

An interoperable ODR framework can therefore connect platform-level complaint mechanisms with existing formal dispute-resolution institutions. Under this approach, platforms can provide the initial mechanism for resolving transaction-related complaints while consumers retain access to external dispute-resolution mechanisms when internal resolution is unsuccessful. Such an arrangement can improve accessibility without requiring all consumer disputes to be transferred immediately to a centralized institutional platform. The relationship between platform-based ODR and formal consumer dispute-resolution institutions should therefore be understood as complementary rather than substitutive. A platform's internal complaint mechanism operates as an initial or private layer of redress based on the contractual and technological environment of the transaction, whereas the Badan Penyelesaian Sengketa Konsumen (BPSK), or Consumer Dispute Settlement Agency, is a statutory institution with authority to handle and resolve consumer disputes through mediation, arbitration, or conciliation under the Consumer Protection Law. Accordingly, an unsuccessful internal complaint should not prevent consumers from accessing legally recognized external dispute-resolution mechanisms. The platform mechanism can instead function as an initial stage that facilitates early resolution while preserving the consumer's right to escalate the dispute when internal resolution is unsuccessful (Indonesia, 1999).

Electronic records are also important for ensuring that escalation from platform-based ODR to external dispute resolution remains effective. Transaction confirmations, payment records, product descriptions, seller information, consumer communications, complaint submissions, refund requests, delivery records, and records of the platform's responses may provide documentary evidence concerning the transaction and the parties' conduct. Platform operators should therefore maintain appropriate records and provide consumers with reasonable access to relevant documentation when a dispute is escalated, subject to applicable personal-data protection requirements. Such documentation can reduce evidentiary uncertainty and enable BPSK or another competent dispute-resolution forum to assess the chronology of the transaction, the responsibilities of the parties, and the steps already undertaken through the platform's internal mechanism.

A platform's internal complaint mechanism operates as an initial or private layer of redress based on the contractual and technological environment of the transaction, whereas the Badan Penyelesaian Sengketa Konsumen (BPSK) is a statutory institution with authority to handle and resolve consumer disputes through mediation, arbitration, or conciliation under the Consumer Protection Law. Accordingly, an unsuccessful internal complaint should not prevent consumers from accessing legally recognized external dispute-resolution mechanisms. The platform mechanism can instead function as an initial stage that facilitates early resolution while preserving the consumer's right to escalate the dispute when internal resolution is unsuccessful.

Privacy Governance and Institutional Enforcement

The findings on personal-data protection demonstrate that consumer awareness alone is insufficient to address privacy risks in digital transactions. The protection of consumers' personal data is also influenced by organizational practices, data-processing arrangements, information-system design, internal governance, and institutional supervision. Within this framework, Privacy by Design, Privacy by Default, data minimization, risk assessment, accountability, and appropriate organizational privacy functions can operate as complementary safeguards within the Personal Data

Protection Law. These mechanisms place greater emphasis on preventing privacy risks through organizational and system-level measures rather than relying solely on consumers to protect themselves after data-related incidents occur.

Institutional capacity is also important because the Personal Data Protection Law assigns specific supervisory and enforcement functions to a dedicated data-protection institution. Articles 58–60 of Law No. 27 of 2022 provide the statutory basis for an institution responsible for personal-data protection, including functions relating to policy formulation, supervision, administrative enforcement, and facilitation of out-of-court dispute resolution. The effectiveness of these statutory functions depends not only on the existence of the legal mandate but also on the operationalization of the institution, including its organizational capacity, supervisory mechanisms, enforcement procedures, and coordination with other regulatory authorities.

The operationalization of the institutional framework is therefore relevant to e-commerce because personal-data complaints may involve multiple actors, including platforms, sellers, payment providers, and other service providers. A functioning supervisory authority can provide regulatory guidance, monitor compliance, and support consistent enforcement across these actors. At the same time, institutional enforcement should remain coordinated with sectoral regulators and existing consumer-protection and dispute-resolution mechanisms to avoid overlapping or fragmented supervision. The development of institutional capacity under Articles 58–60 is consequently an important component of translating the formal rights established by the Personal Data Protection Law into effective protection for consumers in digital transactions.

The effectiveness of these safeguards, however, depends on implementation and institutional enforcement. Clear obligations need to be accompanied by adequate supervisory capacity, organizational compliance, accessible complaint mechanisms, and effective remedies for affected consumers. The comparative literature concerning Singapore, the European Union, and other jurisdictions provides regulatory perspectives on institutional accountability and data governance, but those approaches cannot simply be transferred without considering Indonesia's legal and administrative structure.

Adaptive and Risk-Based Regulatory Reform

The combined findings indicate the need for a regulatory approach capable of responding to the rapid development of digital commerce while maintaining effective consumer protection. Digital markets continue to introduce new transaction models, technologies, data-processing practices, and platform arrangements. At the same time, regulatory requirements that are disproportionate to the level of risk may create unnecessary compliance burdens for digital businesses. A proportionate and risk-based regulatory approach can therefore provide a framework for balancing consumer protection and digital innovation. Such an approach should integrate substantive consumer rights, differentiated platform accountability, personal-data governance, institutional supervision, and accessible dispute-resolution mechanisms. Regulatory requirements can be calibrated according to the nature and level of risks associated with particular digital activities while maintaining minimum safeguards that apply across the e-commerce ecosystem.

This proportionality is particularly important for micro, small, and medium-sized enterprises (MSMEs) that participate in e-commerce. Compliance with consumer-protection, electronic-commerce, and personal-data requirements may create organizational and financial burdens for smaller businesses, particularly where compliance requires additional documentation, security

measures, internal procedures, or specialized personnel. The Personal Data Protection Law does not, however, require every data controller or processor to appoint a dedicated personal-data protection officer under identical conditions. Article 53 of Indonesia's Personal Data Protection Law (Law No. 27 of 2022) establishes the obligation to appoint an official or officer performing personal-data protection functions in specified circumstances, including certain forms of large-scale or systematic processing. This differentiated statutory approach provides a basis for developing compliance requirements that are proportionate to the scale, nature, and risk of data processing (Indonesia, 2022).

A risk-tiered compliance framework could therefore distinguish between lower-risk MSME activities and higher-risk processing conducted by larger platforms or businesses handling sensitive or large-scale personal data. Lower-risk businesses could receive simplified compliance templates, standardized privacy notices, basic security guidance, and government-supported compliance assistance, while higher-risk entities could be subject to more extensive governance, documentation, risk assessment, monitoring, and dedicated privacy functions where the statutory conditions are met. Such differentiation would not reduce the minimum rights of consumers; rather, it would calibrate the organizational means of compliance according to the risks generated by the relevant processing activities. This approach would also be consistent with the broader objective of adaptive regulation by reducing disproportionate compliance burdens while maintaining substantive consumer and personal-data protection.

The regulatory framework should also provide mechanisms for continuous adjustment as digital markets and technologies develop. In this context, Permendag No. 19 of 2026 introduces several developments relevant to consumer protection and platform governance. First, the regulation strengthens business-legality requirements for PMSE actors, including requirements concerning business licensing and the identification of business actors through the NIB. This provides a clearer basis for merchant verification and may improve consumer trust by strengthening the traceability of sellers operating through digital platforms. Second, the regulation introduces specific responsibilities concerning the use of Artificial Intelligence (AI), including informing and/or labeling consumers when goods, services, recommendations, promotions, or other relevant information are produced using AI. PPMSE are also required to establish proportionate internal AI governance and mechanisms for handling complaints or corrections related to AI-generated information. These provisions extend consumer protection to emerging risks associated with synthetic or AI-generated commercial content.

Third, Permendag No. 19 of 2026 strengthens transparency and consumer protection in relation to information and costs associated with electronic commerce. Clear information concerning products, services, and applicable costs can reduce information asymmetry and support more informed consumer decisions. Fourth, the regulation strengthens the policy of prioritizing domestic products by requiring PPMSE to provide promotional space and, for specified business models, to prioritize the visibility of domestic products, including products offered by micro and small enterprises. These provisions demonstrate a regulatory approach that combines consumer protection, business formalization, responsible technology use, and support for domestic products within the digital-commerce ecosystem.

These developments are relevant to the adaptive and risk-based regulatory approach identified in this study. The 2026 regulation responds to emerging digital-market practices without treating all

platform activities as subject to identical requirements. However, its effectiveness will depend on implementation, supervisory capacity, merchant compliance, platform governance, and the ability of consumers to understand and exercise their rights. Because Permendag No. 19 of 2026 was issued after the 2015–2025 literature-review period, these provisions are treated as a subsequent legal development and contextual update rather than as part of the 25-article scholarly literature sample.

Overall, the discussion demonstrates that strengthening digital consumer protection in Indonesia requires an integrated regulatory architecture rather than the addition of isolated legal provisions. The principal policy directions emerging from the analysis are clearer allocation of responsibilities among digital-market actors, stronger platform accountability according to functional roles, interoperable ODR mechanisms, institutionalized privacy governance, and adaptive risk-based regulation. These directions provide a basis for addressing the implementation and coordination gaps identified in the literature while maintaining the legal protection of consumers within Indonesia's evolving e-commerce ecosystem.

5. CONCLUSION

This study contributes an integrated legal perspective on digital consumer protection in Indonesia by connecting differentiated seller and platform responsibilities within a shared-responsibility framework. Indonesia has established a substantial regulatory foundation through the Consumer Protection Law, Personal Data Protection Law, ITE Law as amended by Law No. 1 of 2024, Government Regulation No. 80 of 2019, and regulations governing electronic systems and electronic commerce. However, effectiveness remains affected by fragmented implementation, platform accountability, consumer literacy, personal-data governance, institutional supervision, and digital dispute-resolution safeguards. In the short term, the Ministry of Trade should strengthen coordination among PMSE, consumer-protection, and dispute-resolution institutions, while e-commerce platforms should provide accessible complaint mechanisms with minimum standards for transparency, documentation, human review, personal-data protection, and escalation to external dispute resolution. Where transactions involve fulfillment, transportation, or delivery services, complaint procedures should also clarify the responsibilities of relevant logistics and transportation actors.

In the medium term, the institution responsible for personal-data protection supervision should strengthen compliance guidance, monitoring, and enforcement, particularly for high-risk data processing. Coordination should also connect platform-based complaint mechanisms with formal dispute-resolution institutions and clarify evidence preservation, escalation procedures, and differentiated responsibilities. Compliance guidance for MSMEs should be proportionate to the scale, nature, and risk of their activities while maintaining minimum consumer and personal-data protection standards. In the long term, Indonesia should develop an adaptive and risk-based regulatory framework that can respond to changes in digital commerce, platform business models, data processing, and interconnected logistics services. Periodic evaluation and institutional coordination should ensure that regulatory adaptation does not weaken substantive consumer rights and remedies.

The subsequent development of Indonesia’s PMSE framework is also relevant. Permendag No. 19 of 2026 concerning the Implementation of Trading Through Electronic Systems was issued in June 2026 and replaced Permendag No. 31 of 2023. Because it was issued after the 2015–2025 literature-

review period, it is treated as a subsequent legal development and contextual update rather than part of the 25-article scholarly evidence base. This study is limited by its reliance on secondary scholarly literature and doctrinal legal materials and the absence of empirical data from consumers, platforms, regulators, and dispute-resolution institutions. Future research should empirically examine platform-based ODR, consumer access to remedies, institutional coordination, personal-data compliance, and the implementation of Permendag No. 19 of 2026.

6. REFERENCES

Arai, K. (2025). Comparative Impacts of Ex-Ante and Ex-Post Regulation in Digital Markets: An Event Study Analysis of Stock Price Reactions. *Asian Journal of Law and Economics*, *16*(2), 283–305. https://doi.org/10.1515/ajle-2024-2002

Azzaprillia, T. (2023). Opportunities and Challenges: E-Commerce In Indonesia from Business Legal Perspective. *Wajah Hukum*, *7*(2), 370. https://doi.org/10.33087/wjh.v7i2.1257

Belwal, R., Al Shibli, R., & Belwal, S. (2020). Consumer protection and electronic commerce in the Sultanate of Oman. *Journal of Information, Communication and Ethics in Society*, *19*(1), 38–60. https://doi.org/https://doi.org/10.1108/JICES-09-2019-0110

Bintarawati, F., & Rismana, D. (2024). Efektifitas Undang-Undang Perlindungan Konsumen Dalam Memberikan Perlindungan Hukum Bagi Pengguna E-Commerce Di Era Ekonomi Digital. *Risalah Hukum*, *20*(2), 102–112. https://doi.org/10.30872/risalah.v20i2.1570

Candrarahayu, A. M., Raharjo, E. P., Puruhita, H. W., & Adidana, I. K. S. P. (2026). Optimizing Multimodal Freight Transport : Railway–Airport Integration for Sustainable Logistics in Indonesia. *SKYHAWK : Jurnal Aviasi Indonesia*, *6*(1), 575–586. https://doi.org/10.52074/skyhawk.v6i1.360

Dudi Badruzaman, D. B. (2025). Legal Review of Consumer Protection in E-Commerce Transactions in Indonesia. *Equality : Journal of Law and Justice*, *2*(1), 89–102. https://doi.org/10.69836/equality-jlj.v2i1.271

Dzuhriyan, A. R., Permana, S. I., & Gufron, M. K. A. (2025). Consumer Legal Protection in Online Transactions: Challenges and Opportunities in Indonesia's Digital Economy. *Justice Voice*, *3*(1), 9–16. https://doi.org/10.37893/jv.v3i1.1017

Fauzie, M. A. (2024). Securing the Future: Indonesia Personal Data Protection Law and It' S Implication for Internet of Things (Iot) Data Privacy. *Sriwijaya Crimen and Legal Studies*, *2*(1), 12. https://doi.org/10.28946/scls.v2i1.3743

Ha, H., & Chuah, C. K. P. (2023). Digital economy in Southeast Asia: challenges, opportunities and future development. *Southeast Asia: A Multidisciplinary Journal*, *23*(1), 19–35. https://doi.org/10.1108/SEAMJ-02-2023-0023

Handoyo, S. (2024). Purchasing in the digital age: A meta-analytical perspective on trust, risk, security, and e-WOM in e-commerce. *Heliyon*, *10*(8), e29714. https://doi.org/10.1016/j.heliyon.2024.e29714

Hardigaluh, D. D., & Pulungan, M. S. (2022). Comparative Study on Legal Certainty of Consumer Protection Regarding E-Commerce Transactions, Between Indonesia, India and the United States. *Musamus Law Review*, *5*(1), 1–17. https://doi.org/10.35724/mularev.v5i1.4858

Iman, N. (2024). The fight for our personal data: analyzing the economics of data and privacy on digital platforms. *International Journal of Law and Management*, *66*(6), 774–791. https://doi.org/10.1108/IJLMA-12-2022-0258

Indonesia, R. of. (1999). Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. *Undang-Undang Nomor 8 Tahun 1999*, (8), 1–19. https://peraturan.bpk.go.id/Home/Details/45288/uu-no-8-tahun-1999

Indonesia, R. of. (2019). Peraturan Pemerintah Republik Indonesia Nomor 80 tahun 2019 tentang Perdagangan Melalui Sistem Elektronik. *Government Regulation*, *80*(019092), 61.

Indonesia, R. of. (2022). Undang-undang RI No. 27 Tahun 2022 tentang Pelindungan Data Pribadi. *Ditama Binbangkum - BPK RI*, (016999), 1–50. https://peraturan.bpk.go.id/Home/Details/229798/uu-no-27-tahun-2022

Indonesia, R. of. (2024). Undang-undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. *Journal of Physics A: Mathematical and Theoretical*, *44*(8), 287.

Judijanto, L., Solapari, N., & Putra, I. (2024). An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia. *The Easta Journal Law and Human Rights*, *3*(01), 20–29. https://doi.org/10.58812/eslhr.v3i01.351

Kharisma, D. B. (2020). Urgency of financial technology (Fintech) laws in Indonesia. *International Journal of Law and Management*, *63*(3), 320–331. https://doi.org/10.1108/IJLMA-08-2020-0233

Lubis, F. (2022). Cyber Crime E-Commerce Business Transactions. *Sasi*, *28*(158), 589–598. https://doi.org/10.47268/sasi.v28i4.1068

Maleno, M., & Kusumawati, A. (2024). Comparative Analysis of Indonesia's Personal Data Protection Law with the European Union and California Regulations to Identify Best Practices in Protecting Public Privacy Rights. *Indonesia Law College Association Law Journal*, *3*(2), 91–98. https://ejournal.psthi.or.id/index.php/ILCALaw/article/view/21

Republic of Indonesia. (2020). Peraturan Kementerian Kominfo No. 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Private. *Kementerian Komunikasi Dan Informatika*.

Rohaini, R., Anjani, E., Rusmawati, D. E., & Wardhani, Y. K. (2025). Reforming Online Dispute Resolution (Odr) Regulationsin Growing E-Commerce for Legal Certainty and Protection. *Cepalo*, *9*(1), 69–80. https://doi.org/10.25041/cepalo.v9no1.3335

Romdoni, I. A. (2024). LEGAL ANALYSIS OF CONSUMER PROTECTION IN E- COMMERCE TRANSACTIONS. *ANAYASA (Journal of Legal Studies)*, *2*(1), 17–34. https://altinriset.com/journal/index.php/anayasa/article/view/191

Salisu, M. A., Marafa, L., Bamiro, N. B., Shokunbi, M. O., & Raimi, B. O. (2025). Systematic review of post-COVID policies and strategies for strengthening e-commerce cooperation among ASEAN countries. *Journal of Economic and Administrative Sciences*. https://doi.org/10.1108/JEAS-04-2024-0102

Satwiko, B. S. (2021). Privacy and Data Protection: Indonesian Legal Framework. *Corporate and Trade Law Review*, *1*(2), 98–118. https://doi.org/10.21632/ctlr.1.2.98-118

Septiningsih, I., & Karimullah, S. S. (2024). Consumer Protection in the Digital Era: An Analysis of Consumer Protection in E-Commerce. *Nusantara: Journal of Law Studies*, *3*(2), 68–80. https://doi.org/10.5281/zenodo.17376951

Sudarwanto, A. S., & Kharisma, D. B. B. (2021). Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia. *Journal of Financial Crime*, *29*(4), 1443–1457. https://doi.org/https://doi.org/10.1108/JFC-09-2021-0193

Susanti Sari, R., Ferdiles, L., & Muhammad Rusdi, A. (2024). Model of Legal Protection in E-commerce Transactions to Improve the Community Economy in Indonesia. *Jurnal Hukum Indonesia*, *3*(2), 87–95. https://doi.org/10.58344/jhi.v3i2.759

voor Indonesie, B. W. (2014). *Kitab Undang-undang Hukum Perdata Burgerlijk Wetboek*. 1–549.

Wibowo, E., & Retno Mumpuni, N. W. (2024). Consumer Legal Protection in E-Commerce Transactions: A Case Study of Grab Toko Platform. *Sultan Jurisprudence: Jurnal Riset Ilmu Hukum*, *4*(2), 175. https://doi.org/10.51825/sjp.v4i2.26104

Widiarty, W. S., Suwarno, S., Harjono, D. K., & Susanto, H. (2024). Consumer Protection Laws in Indonesian Commercial Transactions: Safeguarding Business Transactions and Consumer Rights. *Journal of Law and Sustainable Development*, *12*(1), e3099. https://doi.org/10.55908/sdgs.v12i1.3099

Yang, X., Zhang, H., & Huang, Z. (2024). Negative rivalry in use: toward a knowledge-sharing perspective in the digital economy era. *Journal of Knowledge Management*, *28*(9), 2590–2609. https://doi.org/10.1108/JKM-02-2024-0198.