CONSUMER PROTECTION IN DIGITAL COMMERCE: LEGAL CHALLENGES IN ONLINE TRANSACTIONS AND PLATFORM-BASED MARKETS IN INDONESIA

Maftuhul Ilma Wiratama[1], Niswatin Nurul Hidayati[2]

[1] STAI Ma'had Aly Al-Hikam Malang, Indonesia
[2] Institut Teknologi dan Bisnis Tuban, Indonesia

Abstract

The rapid expansion of digital commerce in Indonesia has transformed consumer transactions while creating new legal challenges concerning consumer rights, platform responsibility, personal data protection, algorithmic practices, and access to legal remedies. This study examines the adequacy of Indonesia's consumer protection framework in addressing emerging risks in online transactions and platform-based markets. The research employs a normative juridical method using statutory, conceptual, and comparative approaches. Primary legal materials include Law No. 8 of 1999 on Consumer Protection, Government Regulation No. 71 of 2019, Government Regulation No. 80 of 2019, Law No. 27 of 2022 on Personal Data Protection, Presidential Regulation No. 49 of 2024, and Minister of Trade Regulation No. 19 of 2026 on Electronic Commerce. The findings indicate that Indonesia has developed a substantial regulatory foundation for digital consumer protection; however, the framework remains fragmented and does not yet comprehensively address platform-mediated risks. Significant challenges include information asymmetry, standard-form electronic contracts, unclear allocation of platform responsibility, dark patterns, algorithmic personalization, consumer data processing, cross-border transactions, and limitations in dispute resolution and compensation mechanisms. The study further finds that consumer protection and personal data governance increasingly intersect because consumer data are used to influence recommendations, advertising, pricing, and digital interfaces. Accordingly, Indonesia requires a more integrated ecosystem-based approach that combines consumer rights, platform accountability, data and algorithmic governance, fair digital design, cross-border enforcement, and accessible redress

mechanisms. The study recommends strengthening digital-specific consumer protection provisions, clarifying platform responsibilities, regulating manipulative interface practices, integrating data protection with consumer protection, and improving technology-supported dispute resolution.

Keywords: *Consumer Protection; Digital Commerce; Platform Governance; Dark Patterns; Personal Data Protection*

Corresponding Author:
Maftuhul Ilma Wiratama, maftuhul.wiratama@gmail.com

Article History:
Received : April 2, 2026
Revised : May 15, 2026
Accepted : June 24, 2026

I. INTRODUCTION

The rapid expansion of digital commerce has fundamentally transformed the relationship between consumers, business actors, and digital intermediaries. Online marketplaces, social commerce, mobile applications, digital payment systems, and platform-based business models have made commercial transactions faster, more accessible, and less dependent on physical markets. In Indonesia, this transformation has become particularly significant because the country represents one of the largest digital economies in Southeast Asia. The Ministry of Trade's 2025 report, drawing on the e-Conomy SEA 2025 report, indicates that Southeast Asia's digital economy reached nearly US$300 billion in gross merchandise value (GMV), with e-commerce contributing approximately US$181 billion. Indonesia remained the largest digital economy in the region, demonstrating the increasingly important role of digital commerce in the national economic structure. The expansion of e-commerce has also been accelerated by video commerce, artificial intelligence (AI), and creator-driven digital marketing, which have changed how consumers discover, evaluate, and purchase products.

The growth of digital commerce, however, has simultaneously transformed the nature of consumer vulnerability. Unlike conventional transactions, online transactions often involve multiple actors, including sellers, marketplace operators, payment providers, logistics companies, advertisers, technology providers, and sometimes cross-border platforms. Consumers may therefore experience difficulties in identifying the legally responsible party when products are defective, descriptions are misleading, payments fail, accounts are restricted, or refunds are delayed. The digital environment also creates information asymmetries because consumers typically make purchasing decisions based on platform-generated information, seller ratings, reviews, recommendation systems, promotional claims, and algorithmically curated content. Consequently, traditional assumptions underlying consumer transactions—such as direct interaction between buyer and seller and relatively clear identification of contractual parties—become increasingly complicated in platform-based markets.

Indonesia's principal consumer protection framework was established through Law No. 8 of 1999 concerning Consumer Protection (UUPK). The law provides fundamental rights for consumers and establishes obligations and responsibilities for business actors. Nevertheless, the UUPK was enacted before the emergence of contemporary platform economies, social commerce, algorithmic

recommendation systems, and large-scale digital marketplaces. Its regulatory architecture therefore faces challenges when applied to transactions in which the marketplace may function simultaneously as an intermediary, service provider, advertising environment, payment facilitator, and data processor. The continuing validity of the UUPK provides an important legal foundation, but its institutional and substantive framework increasingly requires adaptation to digital commercial practices.

The government has recognized this regulatory challenge. In April 2026, the Ministry of Trade reported that it was discussing the revision of the Consumer Protection Law because several provisions of the nearly three-decade-old UUPK were considered to require adjustment in relation to contemporary developments. The Ministry specifically identified digital commerce as a factor increasing the urgency of reform and highlighted emerging problems including online scams, illegal or counterfeit products, misleading advertising, and manipulative interface practices or dark patterns. Government data further indicated that from 2021 to March 2026, 35,820 of 37,813 consumer complaints received by the Ministry of Trade—approximately 94.73 percent—originated from online transactions. This development illustrates the increasingly central position of digital commerce in contemporary consumer protection problems.

The regulatory framework for electronic commerce has also developed through Government Regulation No. 80 of 2019 concerning Trading Through Electronic Systems (Perdagangan Melalui Sistem Elektronik/PMSE). The regulation establishes a legal framework for electronic commercial transactions and provides a basis for regulating business actors engaged in PMSE. It is complemented by Government Regulation No. 71 of 2019 concerning the Operation of Electronic Systems and Transactions, which establishes obligations relating to electronic systems and transactions. Together, these regulations extend the legal architecture beyond conventional consumer law toward the technological and transactional infrastructure supporting digital commerce.

More recently, Indonesia substantially updated the regulation of PMSE through Minister of Trade Regulation No. 19 of 2026 concerning the Implementation of Trading Through Electronic Systems. The regulation, which entered into force on 8 June 2026, repealed and replaced Minister of Trade Regulation No. 31 of 2023. Importantly, the new regulation covers business actors and PPMSE business models, requirements for conducting PMSE activities, electronic advertising, domestic product prioritization, cross-border trade

representatives, the utilization of artificial intelligence, supervision, and administrative sanctions. The replacement of the 2023 regulation demonstrates that digital commerce regulation is itself evolving rapidly in response to technological and market developments.

The introduction of AI-related provisions into the 2026 PMSE framework is particularly important for consumer protection. Digital platforms increasingly use algorithms and AI to personalize advertisements, rank products, recommend sellers, detect fraud, determine visibility, and influence consumer purchasing decisions. These technologies can increase efficiency and personalization, but they may also create new forms of asymmetry between platforms and consumers. Consumers may not know why a particular product is recommended, why certain advertisements are displayed, or why particular sellers and products receive greater visibility. The regulatory challenge therefore extends beyond whether a transaction is formally lawful to whether the digital architecture through which the transaction occurs operates transparently, fairly, and without manipulating consumer decision-making. The 2026 PMSE regulation's inclusion of AI within the regulatory framework reflects the growing legal relevance of this issue.

Another major dimension concerns the protection of consumer personal data. Digital commerce depends heavily on the collection and processing of personal information, including names, addresses, telephone numbers, payment information, purchase histories, behavioral profiles, and other information generated through online interactions. Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) establishes rights of personal data subjects and obligations for data controllers and processors, including requirements relating to personal data processing, security, transfer, and accountability. The PDP Law therefore constitutes an essential component of digital consumer protection because consumers are not merely purchasers of goods and services; they are also data subjects whose information becomes an economic resource within digital markets.

Recent legal scholarship indicates, however, that the implementation of personal data protection in Indonesian e-commerce continues to face significant challenges. Research on consumer data processing identifies risks at multiple stages of the data lifecycle, including excessive or unlawful collection, inadequate transparency, unauthorized access, disclosure, modification, misuse, destruction, and loss of personal data. These risks may be intensified by uncertainty concerning consent, accountability, and enforcement. Other research similarly identifies legal

gaps concerning cross-border data transfers and contractual or exoneration clauses that may disadvantage consumers in e-commerce transactions. Comparative analysis with the European Union and Malaysia suggests that regulatory effectiveness depends not only on formal rights but also on supervision, compliance mechanisms, and effective enforcement.

The problem is further complicated by the cross-border nature of digital commerce. Consumers in Indonesia can purchase products and services from businesses located outside Indonesia, while foreign platforms may serve Indonesian consumers without maintaining the same physical presence as conventional domestic businesses. This raises questions regarding jurisdiction, applicable law, enforcement, seller identification, product standards, taxation, refunds, and dispute resolution. Although PP No. 80 of 2019 and subsequent PMSE regulations establish requirements for domestic and foreign business actors, cross-border digital transactions continue to create practical enforcement challenges because the legal relationship extends beyond national territorial boundaries. The effectiveness of consumer protection therefore depends not only on domestic legislation but also on institutional cooperation and mechanisms for cross-border enforcement.

Platform governance introduces another important challenge. In conventional commerce, the legal relationship between consumer and seller is comparatively direct. In a marketplace environment, however, the platform may exercise substantial control over the visibility of products, advertising, seller access, payment mechanisms, consumer reviews, dispute resolution, and transaction conditions. This creates a regulatory question concerning the extent to which platforms should bear responsibility for transactions conducted through their systems. The issue becomes particularly significant where platforms benefit economically from transactions while consumers may have difficulty distinguishing between the platform's own representations and information supplied by third-party sellers. The Indonesian regulatory framework has increasingly recognized the importance of platform responsibilities, and the 2026 PMSE regulation further develops requirements concerning PPMSE actors, supervision, and sanctions.

Consumer complaints provide an important empirical indication of these regulatory challenges. The Ministry of Trade reported that it received 7,887 consumer complaints during 2025, of which 7,836—approximately 99 percent—were related to transactions through electronic commerce. The reported problems

included products that did not correspond to promises or descriptions, defective goods, difficulties in warranty claims, and problems associated with payment systems, including top-ups, paylater, and credit cards. In June 2026, the Ministry also reported complaints concerning transactions through Tokopedia and TikTok Shop involving discrepancies between products and orders, difficulties with returns and refunds, payment and billing problems, delivery issues, and access to user accounts. These cases demonstrate that consumer protection in digital commerce encompasses not only product quality but also payment, delivery, platform access, refund, and post-transaction mechanisms.

The regulatory response has also increasingly shifted toward a broader and more coordinated consumer protection strategy. Presidential Regulation No. 49 of 2024 established the National Consumer Protection Strategy (Strategi Nasional Perlindungan Konsumen), emphasizing an inclusive and integrated consumer protection ecosystem involving ministries, government institutions, regional governments, business actors, communities, and other stakeholders. It was followed by Minister of Trade Regulation No. 17 of 2024 concerning the National Consumer Protection Action Plan, which establishes mechanisms for implementation, monitoring, evaluation, and reporting. These instruments indicate that consumer protection is increasingly treated as a cross-sectoral governance issue rather than merely a private dispute between consumers and sellers.

Despite these regulatory developments, several substantive gaps remain. First, the traditional consumer protection framework does not fully address the structural power of digital platforms and algorithmic intermediaries. Second, the allocation of responsibility between sellers, platforms, payment providers, logistics operators, and other digital actors can remain difficult when harm results from interconnected services. Third, consumers may face limited transparency concerning algorithms, ranking systems, targeted advertising, personalized pricing, and platform decision-making. Fourth, dark patterns and other manipulative interface designs may influence consumer decisions without necessarily appearing as conventional misleading advertising. Fifth, cross-border transactions complicate enforcement and access to effective remedies. Sixth, personal data protection and consumer protection remain legally interconnected but institutionally distinct, potentially creating gaps in supervision and enforcement. These issues suggest that the protection of digital consumers cannot rely exclusively on adapting conventional consumer law to online transactions.

Recent Indonesian scholarship reinforces the need for regulatory reform. Studies have identified deficiencies in the existing legal framework relating to consumer rights, business-actor responsibilities, data protection, contractual fairness, and regulatory enforcement in the digital economy. Other normative research emphasizes that consumer protection in e-commerce requires not only clear legal rights but also accessible dispute-resolution mechanisms and stronger awareness among consumers regarding their legal protections. Research focusing specifically on personal data similarly demonstrates that the expansion of e-commerce creates vulnerabilities that cannot be addressed solely through traditional consumer protection rules.

Against this background, the central legal issue is no longer simply whether Indonesian law recognizes consumer rights in online transactions, but whether the existing regulatory architecture is sufficiently capable of addressing the distinctive risks created by platform-based digital commerce. The rapid succession of regulatory instruments—from the UUPK and electronic transaction regulations to the PDP Law, the National Consumer Protection Strategy, and the new 2026 PMSE regulation—shows significant regulatory development. Nevertheless, the continuing volume of online consumer complaints and the emergence of AI-driven commerce, cross-border transactions, dark patterns, data-intensive business models, and platform-mediated markets indicate the need for further legal analysis.

Therefore, this study examines the legal challenges of consumer protection in digital commerce in Indonesia, focusing on online transactions and platform-based markets. It analyzes the adequacy of the existing legal framework, the responsibilities of digital platforms and business actors, consumer personal data protection, transparency and fairness in digital commercial practices, and mechanisms for dispute resolution and legal redress. The study also considers how recent regulatory developments, particularly Minister of Trade Regulation No. 19 of 2026, can respond to emerging forms of digital commerce while identifying remaining legal gaps. By integrating consumer law, electronic commerce regulation, data protection, and platform governance, this study seeks to contribute to the development of a more coherent, adaptive, and effective legal framework for protecting consumers in Indonesia's rapidly evolving digital economy.

II. LITERATURE REVIEW

Consumer protection in digital commerce can be understood as an extension of the broader legal principle that consumers occupy a structurally weaker position in commercial relationships and therefore require legal protection against information asymmetry, unfair contractual practices, unsafe products, misleading information, and abuse of market power. In Indonesia, the normative foundation of consumer protection is primarily established through Law No. 8 of 1999 concerning Consumer Protection (UUPK), which recognizes consumer rights to safety, comfort, accurate information, choice, compensation, and dispute resolution. Although these principles remain relevant to digital transactions, the emergence of platform-mediated markets has changed the structure of commercial relationships. Consumers no longer interact exclusively with identifiable sellers but increasingly transact through digital intermediaries that control information, interfaces, payment systems, recommendation mechanisms, and dispute-resolution processes. This structural transformation requires traditional consumer protection principles to be interpreted in conjunction with electronic commerce and platform governance rules.

The concept of consumer protection in electronic commerce is closely associated with the principle of information asymmetry. In digital markets, sellers and platforms may possess substantially more information concerning product characteristics, consumer behavior, pricing, transaction histories, algorithms, and commercial incentives than individual consumers. The consumer's decision is frequently based on information selected and presented by the platform rather than information independently obtained by the consumer. OECD analysis emphasizes that digital technologies can amplify traditional consumer vulnerabilities through personalized advertising, behavioral targeting, algorithmic decision-making, and increasingly complex digital commercial environments. Consequently, consumer protection in the digital economy requires not only disclosure of information but also consideration of how information is collected, ranked, personalized, and presented to consumers (OECD, 2022, 2024).

The Indonesian legal framework for electronic commerce has progressively developed in response to these changes. Government Regulation No. 80 of 2019 concerning Trading Through Electronic Systems (PMSE) provides the principal regulatory framework for electronic commercial transactions, while Government Regulation No. 71 of 2019 establishes obligations concerning electronic system operation and electronic transactions. These instruments complement the UUPK

by addressing the technological and transactional characteristics of digital commerce. More recently, Minister of Trade Regulation No. 19 of 2026 concerning the Implementation of Trading Through Electronic Systems replaced Minister of Trade Regulation No. 31 of 2023 and expanded the regulatory framework to cover PPMSE business models, electronic advertising, cross-border trade, artificial intelligence, supervision, and administrative sanctions. The regulatory development demonstrates that consumer protection increasingly intersects with digital-platform regulation rather than operating exclusively within conventional consumer law.

A significant body of literature emphasizes the importance of contractual protection in online transactions. Electronic commerce generally involves standardized terms and conditions prepared by platforms or business actors, creating an imbalance in bargaining power between consumers and businesses. Consumers frequently accept lengthy standard-form agreements through mechanisms such as "click-wrap" or "browse-wrap" contracts without meaningful negotiation. From a consumer-law perspective, the validity of electronic contracts does not eliminate the requirement that contractual provisions comply with mandatory consumer protection principles. The UUPK prohibits certain clauses that effectively transfer responsibility from business actors to consumers or limit consumers' statutory rights. In digital commerce, this issue becomes particularly important where platform terms restrict refunds, impose unilateral account suspension, limit liability, or require consumers to use platform-specific dispute mechanisms. Recent Indonesian scholarship therefore identifies contractual fairness and the regulation of standard clauses as continuing challenges in e-commerce consumer protection.

The literature also identifies the increasing importance of intermediary or platform liability. Platform-based markets complicate the conventional distinction between seller and intermediary because digital platforms may perform multiple functions simultaneously. A marketplace can provide the technological infrastructure, facilitate payments, rank products, deliver advertising, collect consumer data, manage reviews, and administer complaints. Consequently, determining responsibility when consumers suffer harm cannot always be resolved simply by identifying the third-party seller. Platform governance scholarship emphasizes that digital intermediaries exercise substantial private regulatory power through their terms of service, algorithms, content moderation, seller policies, and transaction rules (Gillespie, 2018; Suzor, 2019). This perspective

is particularly relevant to consumer law because platforms can influence the conditions under which consumers encounter products and exercise their rights.

The issue of platform responsibility has become more important as Indonesian digital commerce increasingly involves marketplace and social-commerce models. Platforms may affect consumer choice through product rankings, personalized recommendations, sponsored listings, influencer content, and targeted advertising. The consumer therefore interacts not only with the seller's product but also with an algorithmically structured commercial environment. The new PMSE regulatory framework in Indonesia recognizes this transformation by regulating PPMSE actors and incorporating electronic advertising and AI-related provisions. Nevertheless, the literature indicates that regulatory responsibility remains a difficult issue because the degree of platform control differs according to business model, technological architecture, and contractual arrangements. A legal framework based solely on the traditional seller-consumer relationship may therefore be insufficient for addressing harms arising from the broader platform ecosystem.

Another important theoretical dimension concerns consumer autonomy and dark patterns. Dark patterns refer to interface designs that can manipulate or steer users toward decisions that may not reflect their preferences, such as making cancellation difficult, emphasizing certain purchasing options, concealing additional costs, creating artificial urgency, or repeatedly prompting consumers to accept particular terms. The OECD has identified dark commercial patterns as a significant emerging consumer-protection concern because digital interfaces can exploit behavioral biases and make informed decision-making more difficult (OECD, 2022). Mathur et al. (2019) demonstrated that deceptive interface designs are widespread across digital environments, while Luguri and Strahilevitz (2021) showed experimentally that certain dark patterns can significantly influence user choices. Nouwens et al. (2020) further demonstrated how interface design can affect users' ability to make meaningful choices concerning privacy and consent. These studies suggest that the concept of consumer autonomy must be expanded from the traditional right to receive information toward the right to make decisions in a digital environment that is not deliberately manipulative.

The development of algorithmic commerce adds another layer to this issue. AI and algorithmic systems can personalize advertisements, recommend products, predict consumer preferences, determine product visibility, and optimize pricing and marketing strategies. While algorithmic personalization can improve

efficiency and consumer convenience, it can also create opacity concerning how commercial decisions are generated. Consumers may not know why particular products are recommended, why certain advertisements are displayed, or whether their behavior has been used to influence subsequent commercial offers. This creates a tension between personalization and transparency. Recent research on AI governance emphasizes that algorithmic transparency, accountability, human oversight, and risk assessment are increasingly important where automated systems have significant effects on individuals (UNESCO, 2021; OECD, 2024). In the context of digital commerce, these principles can be translated into consumer rights to meaningful information, fair treatment, and appropriate mechanisms for challenging harmful automated decisions.

Personal data protection represents another major dimension of consumer protection in digital markets. Digital transactions generate substantial quantities of personal and behavioral data, including identity information, contact details, transaction histories, payment information, browsing patterns, location data, and consumer preferences. Indonesia's Law No. 27 of 2022 concerning Personal Data Protection establishes a comprehensive legal framework concerning the rights of data subjects and obligations of data controllers and processors. The relationship between consumer protection and data protection is therefore increasingly inseparable. Consumers may suffer harm not only from defective products or unfair contractual terms but also from unauthorized data processing, excessive collection, profiling, data breaches, or secondary use of information.

The literature on privacy and consumer protection increasingly rejects the idea that privacy should be treated solely as an individual data-security issue. Acquisti et al. (2015) explain that privacy decisions are shaped by information asymmetry, behavioral biases, and contextual factors, while OECD (2024) emphasizes the convergence between AI governance, data governance, and privacy protection. In digital commerce, this convergence is particularly important because consumer data can be used to personalize advertisements, recommend products, segment consumers, and predict purchasing behavior. The Indonesian PDP Law therefore provides an important legal foundation, but effective consumer protection requires coordination between personal data regulation and consumer law so that consumers can exercise both their economic rights and data-subject rights.

Cross-border commerce presents an additional challenge. Digital platforms allow Indonesian consumers to purchase goods and services from foreign businesses with limited physical presence in Indonesia. This creates potential conflicts concerning applicable law, jurisdiction, enforcement, product standards, taxation, refunds, and dispute resolution. The literature on international e-commerce emphasizes that traditional territorial approaches to consumer protection become more difficult when transactions involve multiple jurisdictions and intermediaries. Indonesian PMSE regulation has addressed aspects of cross-border electronic commerce, but enforcement remains dependent on the ability of domestic authorities to identify foreign business actors, obtain relevant information, and coordinate with external jurisdictions. Consequently, effective consumer protection in digital commerce requires not only substantive rights but also practical mechanisms for cross-border enforcement.

Dispute resolution is consequently a central component of digital consumer protection. Conventional litigation may be costly and time-consuming relative to the value of many online transactions. Digital platforms therefore increasingly provide internal complaint and dispute-resolution mechanisms. Although these mechanisms can improve efficiency, they may also create concerns regarding neutrality, transparency, and procedural fairness when the platform itself is involved in the dispute. Alternative dispute resolution and online dispute resolution (ODR) have consequently received increasing attention as mechanisms for resolving digital consumer disputes. Effective ODR should provide accessibility, transparency, procedural fairness, timely resolution, and meaningful remedies. In the Indonesian context, these mechanisms should be integrated with the consumer dispute-resolution framework and should not undermine consumers' statutory rights to seek remedies through formal legal institutions.

Another relevant issue in the literature is the effectiveness of consumer enforcement. Formal legal rights do not necessarily translate into effective protection if consumers lack awareness, evidence, affordable dispute mechanisms, or access to competent authorities. Digital transactions can create evidentiary difficulties because relevant information may be stored electronically by platforms, payment providers, or sellers. Consumers may also encounter difficulties when an account is suspended or transaction records become inaccessible. Platform-controlled evidence therefore creates an imbalance that may affect the consumer's ability to establish a claim. Effective enforcement requires mechanisms for preserving electronic evidence, requiring appropriate disclosure, strengthening

institutional coordination, and ensuring that platforms maintain accessible transaction records.

The literature also suggests that consumer protection should increasingly be viewed as a form of digital governance. Traditional consumer law focuses primarily on the bilateral relationship between consumer and business actor, whereas platform markets involve networks of businesses, intermediaries, technology providers, payment systems, logistics providers, advertisers, and regulators. This multi-actor structure requires a governance approach capable of allocating responsibility according to the degree of control and benefit exercised by each actor. Such an approach is consistent with contemporary developments in platform governance, AI governance, and data governance, where accountability is distributed across technological and institutional ecosystems rather than assigned exclusively to individual sellers.

International regulatory developments provide useful comparative perspectives for Indonesia. The European Union's Digital Services Act establishes obligations for online platforms concerning transparency, advertising, recommender systems, trader traceability, and consumer protection, while the EU Artificial Intelligence Act establishes a risk-based framework for AI systems. The General Data Protection Regulation also provides extensive protections concerning personal data processing and individual rights. These instruments demonstrate a broader regulatory trend toward combining consumer protection, platform accountability, transparency, and data governance. However, comparative models should not be transplanted mechanically into Indonesia because differences exist in legal institutions, enforcement capacity, market structures, and regulatory traditions.

Taken together, the literature demonstrates that digital consumer protection is multidimensional. It encompasses traditional consumer rights, electronic contracts, platform responsibility, algorithmic transparency, protection against manipulative interface design, personal data protection, cross-border commerce, and accessible dispute resolution. Existing Indonesian regulations have progressively addressed several of these dimensions, particularly through the UUPK, PMSE regulations, the PDP Law, and the emerging 2026 PMSE framework. Nevertheless, the rapid development of platform-based markets means that regulatory categories continue to evolve faster than conventional legal frameworks.

The principal research gap lies in the limited integration of these legal dimensions into a single analytical framework for Indonesia. Existing studies frequently examine consumer protection, electronic contracts, personal data, e-commerce, or platform liability separately. Less attention has been given to how these areas interact within contemporary platform-based markets, particularly following the introduction of Minister of Trade Regulation No. 19 of 2026 and the increasing use of AI-driven commercial practices. This study therefore approaches digital consumer protection as an integrated legal-governance problem, examining the interaction between consumer rights, platform responsibilities, data protection, algorithmic and interface-based commercial practices, cross-border transactions, and dispute resolution. The analysis is intended to identify whether the existing Indonesian regulatory framework provides sufficient protection for consumers and to formulate legal directions for a more coherent, adaptive, and enforceable framework for digital commerce.

III. RESEARCH METHOD

This study employs a normative juridical legal research approach to examine the legal challenges of consumer protection in digital commerce and platform-based markets in Indonesia. Normative legal research is appropriate because the study focuses on analyzing legal norms, regulatory coherence, rights and obligations of relevant actors, and the adequacy of existing legal instruments in addressing emerging forms of digital commerce. The analysis focuses particularly on consumer rights, electronic transactions, platform responsibilities, personal data protection, digital advertising, algorithmic practices, cross-border commerce, and consumer dispute resolution.

The research uses three complementary legal approaches: the statutory approach, conceptual approach, and comparative approach. The statutory approach examines relevant Indonesian legal instruments, including Law No. 8 of 1999 concerning Consumer Protection, Government Regulation No. 71 of 2019 concerning the Operation of Electronic Systems and Transactions, Government Regulation No. 80 of 2019 concerning Trading Through Electronic Systems, Law No. 27 of 2022 concerning Personal Data Protection, Presidential Regulation No. 49 of 2024 concerning the National Consumer Protection Strategy, and Minister of Trade Regulation No. 19 of 2026 concerning the Implementation of Trading Through Electronic Systems. The conceptual approach is used to examine the concepts of consumer protection, platform responsibility, information asymmetry,

contractual fairness, digital consumer autonomy, algorithmic transparency, personal data protection, and effective legal redress. The comparative approach considers selected international regulatory developments, particularly the European Union's Digital Services Act, General Data Protection Regulation, and Artificial Intelligence Act, to identify regulatory principles that may provide relevant lessons for Indonesia.

The legal materials consist of primary, secondary, and tertiary legal materials. Primary legal materials include legislation, government regulations, ministerial regulations, and other authoritative legal instruments governing consumer protection, electronic commerce, digital platforms, and personal data. Secondary legal materials include peer-reviewed journal articles, books, scholarly publications, institutional reports, policy documents, and authoritative analyses concerning digital consumer protection and platform governance. Tertiary materials, including legal dictionaries and relevant reference sources, are used to clarify terminology and support the interpretation of legal concepts.

Data are collected through library research and systematic document analysis. Relevant legal materials are identified based on their relationship to the research questions and subsequently classified according to the principal legal issues examined in the study. The analysis focuses on five interconnected dimensions: (1) consumer rights and electronic contractual relationships; (2) legal responsibility of digital platforms and business actors; (3) personal data protection and algorithmic commercial practices; (4) cross-border digital transactions and enforcement; and (5) dispute resolution and consumer redress.

The collected legal materials are analyzed qualitatively through legal interpretation, legal comparison, and regulatory gap analysis. First, relevant provisions are interpreted to identify the rights, obligations, prohibitions, responsibilities, and enforcement mechanisms established by Indonesian law. Second, the Indonesian framework is compared with selected international regulatory approaches to identify similarities, differences, and potentially relevant regulatory principles. Third, regulatory gaps are identified by comparing existing legal provisions with emerging risks associated with platform-based commerce, including manipulative interface practices, algorithmic personalization, data-intensive business models, cross-border transactions, and platform-mediated disputes.

The analysis follows a sequential process consisting of identification of legal problems, collection and classification of legal materials, interpretation of relevant

legal provisions, conceptual and comparative analysis, identification of regulatory gaps, and formulation of legal recommendations. The findings are then synthesized to assess whether the existing Indonesian consumer protection framework provides adequate legal protection in contemporary digital commerce. The study ultimately seeks to formulate a more coherent and adaptive legal framework that balances consumer rights, platform innovation, business interests, technological development, and effective regulatory enforcement.

IV. RESULTS AND DISCUSSION

Results

The normative analysis indicates that Indonesia has developed a relatively broad legal foundation for consumer protection in digital commerce, but the regulatory framework remains fragmented across consumer protection, electronic commerce, personal data protection, and platform governance instruments. The principal framework consists of Law No. 8 of 1999 concerning Consumer Protection, Government Regulation No. 71 of 2019 concerning the Operation of Electronic Systems and Transactions, Government Regulation No. 80 of 2019 concerning Trading Through Electronic Systems, Law No. 27 of 2022 concerning Personal Data Protection, Presidential Regulation No. 49 of 2024 concerning the National Consumer Protection Strategy, and Minister of Trade Regulation No. 19 of 2026 concerning the Implementation of Trading Through Electronic Systems. The analysis demonstrates that these instruments collectively provide substantial normative foundations, but they do not yet constitute a fully integrated legal framework specifically designed for the complex relationships generated by platform-based digital commerce.

The first finding concerns the continuing relevance but limited digital specificity of the conventional consumer protection framework. The UUPK provides fundamental rights relating to safety, accurate information, choice, compensation, and dispute resolution. These rights remain applicable to online transactions. However, the law was enacted in 1999, before the emergence of contemporary marketplaces, social commerce, algorithmic recommendation systems, and AI-based commercial practices. Consequently, several contemporary forms of consumer vulnerability cannot be addressed explicitly through the original regulatory architecture. The legal issue is therefore not the absence of

consumer rights but the extent to which existing rights can effectively respond to new technological and commercial structures.

The second finding is the increasing regulatory recognition of digital platforms and PPMSE actors. PP No. 80 of 2019 established the basic legal framework for electronic commerce, while Permendag No. 19 of 2026 significantly develops the regulatory framework by addressing PPMSE business models, electronic advertising, cross-border trade, artificial intelligence, supervision, and administrative sanctions. This development demonstrates a shift from regulating electronic transactions primarily as technological transactions toward regulating the broader digital commercial ecosystem. Nevertheless, platform responsibility remains a complex issue because platforms may simultaneously function as marketplaces, advertising intermediaries, payment facilitators, data processors, and providers of technological infrastructure.

A third finding concerns the difficulty of allocating legal responsibility among multiple actors. In platform-based transactions, consumers may interact with sellers, marketplace operators, payment providers, logistics providers, advertisers, and other intermediaries within a single transaction. Where consumers experience defective products, misleading information, payment failures, delivery problems, or difficulties obtaining refunds, identifying the legally responsible party may therefore become complicated. The existing framework recognizes responsibilities for business actors and PPMSE providers, but the allocation of responsibility may become less clear when consumer harm results from interactions among several actors. This creates a need for a responsibility framework based not only on formal contractual relationships but also on the degree of control, benefit, and involvement of each actor in the transaction.

The fourth finding relates to information asymmetry and transparency in digital commercial practices. Digital platforms control significant amounts of information concerning products, consumer behavior, advertising, seller performance, recommendation systems, and transaction histories. Consumers generally have less information about how products are ranked, recommended, advertised, or personalized. This creates a structural asymmetry that may affect consumer autonomy. Existing consumer protection principles concerning truthful information provide a normative basis for addressing misleading information, but

they do not comprehensively regulate algorithmic ranking, personalized recommendations, sponsored listings, or other technologically mediated forms of commercial influence.

The fifth finding is the emergence of dark patterns and manipulative digital interfaces as a consumer protection issue. Traditional consumer law generally focuses on misleading information or unfair contractual terms, whereas digital platforms can influence consumer behavior through interface architecture. Practices such as hidden costs, difficult cancellation procedures, default selections, artificial urgency, repeated prompts, or complicated consent mechanisms can potentially reduce consumers' ability to make autonomous decisions. Although Indonesian regulatory developments increasingly recognize manipulative digital practices as a concern, the current framework requires further clarification concerning definitions, prohibited practices, evidentiary standards, supervisory responsibilities, and available remedies.

The sixth finding concerns personal data protection as an integral component of digital consumer protection. The PDP Law provides important rights and obligations concerning personal data processing, but the analysis indicates that data protection and consumer protection operate through partially separate regulatory frameworks. Digital commerce combines both dimensions because consumers provide personal information as part of commercial transactions and because such information can subsequently be used for profiling, targeted advertising, personalization, and behavioral analysis. Consequently, consumer protection cannot be limited to the protection of economic interests. It must also encompass protection against unlawful or excessive processing of personal data and inappropriate use of consumer information.

The seventh finding concerns algorithmic and AI-driven commerce. The inclusion of AI-related provisions in the 2026 PMSE framework demonstrates that Indonesian regulation has begun to respond to technological developments beyond conventional e-commerce. AI can be used to recommend products, personalize advertisements, detect fraudulent behavior, optimize pricing, and analyze consumer preferences. These applications may generate efficiency benefits but can also create risks involving opacity, discrimination, inaccurate recommendations, and automated decision-making. The existing framework provides an emerging regulatory basis, but more detailed obligations concerning algorithmic transparency, documentation, human oversight, auditing, and

consumer contestability remain necessary, particularly for AI applications capable of producing significant effects on consumers.

The eighth finding concerns cross-border digital commerce and enforcement. Indonesian consumers can access products and services from foreign sellers and platforms with limited physical presence in Indonesia. Although PMSE regulations establish requirements for cross-border electronic commerce, practical enforcement can be complicated by questions of jurisdiction, applicable law, seller identification, evidence, and execution of remedies against foreign entities. The analysis indicates that formal recognition of consumer rights is insufficient when consumers face difficulties enforcing those rights against businesses operating outside the effective reach of domestic institutions.

The ninth finding concerns consumer dispute resolution and access to remedies. Digital commerce generates disputes involving product quality, product-description discrepancies, delivery, payment, refunds, warranties, account restrictions, and transaction cancellation. Platform-based complaint mechanisms can provide rapid and relatively accessible solutions, but their effectiveness depends on transparency, procedural fairness, accessibility, and the independence of the dispute-resolution process. Where the platform itself is involved in the disputed transaction, reliance exclusively on internal mechanisms may create concerns regarding neutrality. Effective consumer protection therefore requires coordination between platform-based complaint systems, alternative dispute resolution, consumer dispute-resolution institutions, and judicial remedies.

The tenth finding concerns the continuing gap between regulatory development and the changing nature of digital consumer risks. The regulatory trajectory from the UUPK to PMSE regulation, the PDP Law, the National Consumer Protection Strategy, and the 2026 PMSE regulation demonstrates substantial institutional development. However, technological innovation continues to introduce new forms of consumer vulnerability. The legal framework must therefore be capable of adapting to AI-based commerce, platform concentration, behavioral advertising, dark patterns, cross-border transactions, and data-driven personalization without creating excessive regulatory uncertainty for legitimate digital business activities. The principal results of the normative analysis can be summarized as follows:

Legal Dimension	Existing Regulatory Foundation	Principal Finding	Remaining Legal Challenge
Consumer rights	UUPK No. 8/1999	Fundamental consumer rights remain applicable to online transactions	The framework lacks sufficient digital-specific provisions
Electronic commerce	PP No. 80/2019; Permendag No. 19/2026	Digital commerce and PPMSE activities are increasingly regulated	Rapid technological change creates new regulatory gaps
Platform responsibility	PMSE framework	PPMSE actors are increasingly subject to regulatory obligations	Responsibility among platforms, sellers, and intermediaries requires clearer allocation
Electronic advertising	PMSE regulation	Digital advertising is increasingly incorporated into commerce regulation	Algorithmic targeting and manipulative advertising require further clarification
Personal data	UU No. 27/2022	Consumers have strengthened rights as data subjects	Integration between consumer protection and data protection remains necessary
AI and algorithms	Permendag No. 19/2026 and emerging AI governance	Indonesian regulation has begun addressing AI-related commerce	Detailed transparency, accountability, auditing, and human-oversight

			requirements remain under development
Dark patterns	Consumer-protection policy development	Manipulative interface practices have emerged as a recognized concern	Definitions, prohibited practices, evidence, and sanctions require clearer regulation
Cross-border commerce	PP No. 80/2019; Permendag No. 19/2026	Cross-border digital trade is formally recognized	Jurisdiction and enforcement remain difficult
Dispute resolution	UUPK and related mechanisms	Consumers have formal avenues for complaints and remedies	Platform-based resolution requires stronger fairness and accountability safeguards
Regulatory governance	Perpres No. 49/2024 and related action planning	Consumer protection increasingly adopts a coordinated governance approach	Institutional coordination and enforcement capacity remain important challenges

Discussion

The findings of this study demonstrate that consumer protection in Indonesian digital commerce has developed significantly but remains characterized by regulatory fragmentation, particularly where conventional consumer law intersects with electronic commerce, platform governance, personal data protection, algorithmic systems, and emerging forms of digital manipulation. This finding is consistent with recent Indonesian legal scholarship, which generally identifies a gap between the rapid development of digital commerce and the capacity of existing legal instruments to address emerging forms of consumer

vulnerability. Subagyono et al. (2024), for example, argue that Indonesia's existing consumer protection framework faces difficulties in addressing the complexity of contemporary electronic transactions and that regulatory reform is necessary to accommodate developments in e-commerce. Similarly, Rosidah and Karjoko (2025) find that although the Consumer Protection Law, ITE Law, PMSE regulation, and related instruments provide a basic legal foundation, consumers continue to face difficulties in obtaining effective recovery for losses arising from electronic transactions.

The persistence of these challenges indicates that the principal problem is not the complete absence of consumer protection norms but the limited digital specificity and integration of existing regulations. Law No. 8 of 1999 concerning Consumer Protection (UUPK) continues to provide fundamental rights concerning safety, information, choice, compensation, and dispute resolution. However, the law was enacted before the emergence of contemporary marketplace platforms, social commerce, algorithmic recommendations, personalized advertising, and AI-mediated transactions. Subagyono et al. (2024) similarly identify ambiguity concerning the application of the consumer concept and dispute-resolution framework in online transactions. Their findings suggest that the traditional distinction between consumers, business actors, and intermediaries becomes increasingly difficult to maintain in digitally mediated transactions.

This problem is reinforced by Rosidah and Karjoko (2025), who argue that the legal framework governing electronic transactions provides formal protection but that the recovery of consumer losses is not necessarily straightforward. They propose stronger validation of business actors before products are offered and more effective compensation mechanisms involving Electronic System Trading Providers (PPMSE). The implication is that consumer protection should move beyond the recognition of abstract rights toward mechanisms that enable those rights to be exercised effectively. In digital commerce, therefore, the effectiveness of consumer law should be evaluated not only by the existence of substantive rights but also by the accessibility of compensation, complaint mechanisms, evidence, and enforcement.

The second major issue concerns the legal responsibility of digital platforms. Platform-based commerce differs fundamentally from conventional transactions because a marketplace can perform multiple functions simultaneously. A platform may provide the technological infrastructure,

organize product listings, facilitate payments, operate advertising systems, manage ratings and reviews, collect personal data, determine product visibility, and administer dispute mechanisms. Consequently, the platform may exercise considerable influence over the transaction even where it does not formally sell the product. Recent research by Zulfah et al. (2025) demonstrates that Indonesia currently adopts a knowledge-based and conditional approach to platform responsibility, while the European Union applies a more risk-based and proportional model emphasizing systemic risks and transparency. The study recommends clearer risk-assessment standards, enhanced transparency, and stronger compensation mechanisms for users.

This finding is important because it challenges a purely contractual approach to platform responsibility. If responsibility is determined exclusively by the formal contractual relationship between consumer and seller, the platform may avoid responsibility even when its technological architecture substantially contributes to consumer harm. The appropriate legal question should therefore include the platform's degree of control, knowledge, economic benefit, and capacity to prevent or mitigate harm. Such an approach would be consistent with contemporary platform-governance literature, which conceptualizes platforms not merely as passive intermediaries but as private regulators capable of structuring the conditions under which users and businesses interact.

The importance of this issue can also be seen in recent Indonesian research on consumer remedies. Manggala and Susanti (2025), examining consumer remedies concerning damaged goods and protection fees on Shopee, find that consumers may rely on both contractual mechanisms within the platform and external legal protection under consumer and insurance law. Their study emphasizes that dispute resolution may proceed through non-litigation mechanisms, including mediation through the Consumer Dispute Resolution Agency (BPSK), or litigation where appropriate. This illustrates that platform-based mechanisms and state-based legal remedies should not be treated as mutually exclusive. Instead, platform complaint systems should function as an accessible first layer of protection without eliminating consumers' statutory rights to seek external remedies.

The third issue concerns information asymmetry and digital transparency. Conventional consumer protection assumes that consumers require adequate

information concerning products and services to make rational choices. In digital commerce, however, the problem is more complex because platforms do not merely provide information; they determine which information consumers see and in what order. Product rankings, reviews, sponsored listings, recommendation algorithms, discount displays, and personalized advertisements can shape consumer decisions before the consumer interacts directly with the seller.

Recent empirical research confirms the importance of these mechanisms. Lase (2025), studying TikTok Shop consumers in Gunungsitoli, found that product quality, digital marketing, and online reviews significantly influenced purchasing decisions, with product quality having the strongest influence among the variables examined. Eriyani and Amalia (2025), meanwhile, found that digital marketing and online reviews significantly influenced Generation Z purchase intention on Shopee, while pricing also significantly affected purchase intention. Their model explained 68% of the variance in purchase intention. These studies are important for consumer law because they demonstrate that digital marketing and platform-generated information are not peripheral features of e-commerce; they are central mechanisms influencing consumer decision-making. The legal significance of online reviews and digital marketing is therefore closely connected to the principle of informed choice. If reviews are manipulated, advertisements are disguised as neutral recommendations, or product rankings are influenced by commercial relationships without adequate disclosure, consumers may make decisions based on information that does not accurately reflect market conditions. The issue consequently extends beyond traditional false advertising toward the broader governance of digital information environments.

The fourth issue is the emergence of dark patterns. This study's findings are strongly supported by recent scholarship identifying dark patterns as a significant regulatory gap in Indonesian consumer law. Hayati (2025) argues that Indonesian consumer protection law does not adequately address dark patterns because existing rules only indirectly regulate certain forms of manipulative interface design. The study recommends explicit legal restrictions against interface practices that impair consumer autonomy or exploit behavioral biases. This conclusion is reinforced by Supriyanto and Hadi (2025), who examine dark patterns specifically within Indonesian e-commerce. Their research finds that Indonesia does not yet have explicit regulation prohibiting dark patterns and that enforcement remains predominantly reactive. Through international

benchmarking, they identify the importance of ethical design guidelines and UI/UX auditing as potential instruments for improving digital-market transparency. Similarly, Az-Zahra et al. (2025) identify three principal Indonesian regulatory gaps: the absence of explicit substantive prohibitions, the absence of specialized institutional oversight, and the lack of technical guidelines for digital interface governance. Their comparative analysis of South Korea and the EU suggests that effective regulation requires a combination of substantive norms, institutional mechanisms, and technical standards.

More recent research strengthens this argument. Annisa and Hutabarat (2026) identify forms of dark patterns in Indonesian marketplace applications including false urgency, hidden costs, sneak-into-basket mechanisms, fake reviews, fake discounts, and disguised advertising. Their study demonstrates that these practices can affect consumer autonomy, fairness, and legal protection. Research published in 2026 on digital subscription services similarly identifies auto-renewals, post-trial charges without adequate notice, pre-selected paid add-ons, and deliberately complicated cancellation processes as forms of manipulative design that are insufficiently addressed by existing Indonesian consumer law.

The increasing use of AI adds a new dimension to this problem. AI-personalized commercial environments can potentially make dark patterns more adaptive because systems can use behavioral data to determine which messages, offers, or interface elements are most likely to influence a particular consumer. Hidayat and Manurung (2026), using qualitative interviews with Indonesian e-commerce consumers, found themes involving limited awareness of algorithmic influence, urgency and scarcity pressure, unequal effort between accepting and refusing choices, declining trust following perceived manipulation, and consumer strategies for restoring autonomy. This suggests that AI-enabled personalization may intensify the traditional information asymmetry between consumers and digital platforms.

The fifth issue concerns personal data protection as an integral dimension of consumer protection. Digital commerce depends on extensive processing of consumer data, including identity information, contact details, payment information, transaction histories, location data, browsing patterns, and behavioral profiles. Putra et al. (2024) identify multiple legal risks throughout the data-processing lifecycle in Indonesian e-commerce, including non-compliant

collection, insufficient transparency, excessive collection, unauthorized access, disclosure, modification, misuse, destruction, and loss of personal data. Their study also identifies ambiguities concerning consent, accountability, and enforcement under Law No. 27 of 2022.

This finding is supported by Maharani and Prakoso (2023), who examined personal data protection obligations of electronic system providers in digital transactions involving platforms such as Akulaku, Lazada, and Tokopedia. Their research emphasizes the importance of compliance with privacy policies, security measures, monitoring, and institutional mechanisms for reducing data-breach risks. Putra, Fibrianti, and Fakhrullah (2024) further argue that Data Protection Impact Assessment (DPIA) can provide an important mechanism for protecting consumer personal data on e-commerce platforms. Their study proposes indicators derived from the rights of personal data subjects and the data-processing obligations established by Law No. 27 of 2022.

More recent comparative research by Putra, Fibrianti, and Prasetya (2025) examines the liability of e-commerce service providers for consumer personal-data processing under Indonesian law and the European GDPR framework. Their analysis highlights the importance of clarifying the legal position and responsibilities of e-commerce service providers as controllers of consumer personal data. This is particularly relevant because the platform's role extends beyond facilitating transactions; it may also determine the purposes and means of processing extensive consumer information.

The relationship between data protection and consumer protection should therefore be understood as mutually reinforcing rather than institutionally separate. A consumer may experience harm through financial loss, defective products, or misleading information, but may also experience harm through profiling, unauthorized data processing, security breaches, or the use of personal data to manipulate purchasing decisions. The use of IP addresses provides a further illustration. Recent research identifies IP addresses as potentially relevant personal-data objects and emphasizes the need to limit their use for behavioral analysis, personalization, and transaction security in accordance with Indonesian law.

The sixth issue is electronic contracts and digital transaction validity. The legal validity of electronic agreements is essential because consumers commonly accept standardized platform terms without negotiation. Recent research by

Wulandari et al. (2025) examines the validity of digital signatures in internet sales transactions from the perspective of the Civil Code and Consumer Protection Law, demonstrating that digital transaction validity remains closely connected to traditional principles of contract law and consumer protection. The legal challenge therefore extends beyond recognizing electronic contracts as valid; it also concerns whether contractual terms are transparent, fair, comprehensible, and consistent with mandatory consumer-protection provisions.

The seventh issue concerns cross-border transactions. Digital commerce allows Indonesian consumers to interact with sellers and platforms located outside Indonesia, creating questions concerning applicable law, jurisdiction, evidence, seller identification, refunds, product standards, and enforcement. Comparative research on Indonesia and the European Union by Mau (2025) concludes that Indonesia's digital consumer protection framework remains more fragmented and faces challenges concerning enforcement and inter-agency coordination, while the EU has developed a more harmonized rights-based framework. This comparison does not necessarily imply that Indonesia should replicate the EU model, but it illustrates the institutional importance of regulatory coordination when consumer relationships cross multiple legal jurisdictions.

The eighth issue concerns the effectiveness of consumer dispute resolution. Subagyono et al. (2024) identify important questions concerning the relationship between the Consumer Protection Law, ITE Law, and dispute resolution in online transactions. Their study argues that existing legal categories may generate ambiguity in determining which legal framework should govern particular online disputes. Manggala and Susanti (2025), meanwhile, demonstrate that disputes concerning damaged goods on e-commerce platforms may involve both internal contractual mechanisms and external remedies under consumer protection law. These findings indicate that digital consumer protection requires a multi-layered dispute-resolution structure rather than dependence on a single mechanism.

The platform's internal complaint mechanism should consequently be regarded as complementary to, rather than a replacement for, external legal remedies. This is particularly important where the platform controls the transaction records, payment information, communication history, and evidence needed to resolve the dispute. Procedural fairness requires consumers to have meaningful access to evidence, explanations, review mechanisms, and escalation

procedures. A platform should not effectively become the final adjudicator of disputes in which it has a direct economic or contractual interest without adequate safeguards.

V. CONCLUSION AND RECOMMENDATION

This study concludes that consumer protection in Indonesia's digital commerce ecosystem has evolved through the interaction of general consumer protection law, electronic commerce regulation, personal data protection, and platform-related governance. Law No. 8 of 1999 on Consumer Protection remains the fundamental legal basis, complemented by Government Regulation No. 80 of 2019 on Electronic Commerce and Law No. 27 of 2022 on Personal Data Protection. However, the existing framework remains fragmented and does not yet comprehensively address risks arising from platform-based markets, including algorithmic personalization, dark patterns, consumer profiling, standardized electronic contracts, targeted advertising, and cross-border transactions. Consumer vulnerability is therefore shaped not only by fraudulent sellers or defective products but also by structural features of digital platforms that can influence consumer autonomy and decision-making. Recent scholarship similarly identifies gaps in regulating manipulative interface design, data-driven practices, and platform accountability, indicating that conventional transaction-oriented consumer protection is increasingly insufficient for the complexity of digital markets. The study consequently recommends an ecosystem-oriented approach to digital consumer protection that integrates substantive consumer rights with platform accountability, personal data governance, algorithmic transparency, fair interface design, and accessible remedies. Indonesia should strengthen and modernize its consumer protection framework by clarifying the responsibilities of platforms according to their actual role, control, knowledge, and capacity to prevent consumer harm; establishing clearer standards against dark patterns and manipulative interface designs; integrating consumer protection with data and algorithmic governance; and strengthening safeguards for profiling, personalized advertising, and recommendation systems. Such reforms should also be accompanied by stronger institutional coordination among consumer-protection, trade, digital, data-protection, and competition authorities, as well as enhanced cooperation for cross-border transactions.

In addition, consumer protection should be supported by practical enforcement and accessible mechanisms for obtaining remedies. Regulatory authorities should develop clearer technical guidance and supervisory mechanisms for digital interfaces, including monitoring of hidden costs, false urgency, pre-selected options, disguised advertising, misleading consent mechanisms, and unnecessarily difficult cancellation procedures. Platforms that process consumer data or employ algorithmic systems should provide meaningful transparency and appropriate risk-management measures, while high-risk processing should be subject to strengthened data-protection impact assessment and accountability mechanisms. Cross-border consumer protection should likewise be reinforced through institutional and international cooperation to facilitate complaint handling, evidence gathering, enforcement, and compensation. For consumers, technology-supported dispute-resolution mechanisms such as online dispute resolution, standardized complaint procedures, mediation, and platform-based compensation should be expanded, particularly for low-value transactions where conventional litigation may be impractical. Future research should empirically examine consumer experiences with algorithmic recommendations, dark patterns, personalized advertising, electronic contracts, and platform complaint mechanisms across different demographic groups and digital-commerce platforms, including comparative studies with jurisdictions that have developed more specific digital consumer-protection frameworks. Overall, the findings support a shift from a predominantly transaction-oriented model toward an ecosystem-oriented model of digital consumer governance in which consumer rights, platform accountability, data protection, algorithmic transparency, fair digital design, cross-border cooperation, and effective remedies operate as interconnected components of consumer protection.

REFERENCES

Annisa, A., & Hutabarat, S. M. D. (2026). Legal protection for consumers in the context of dark patterns in Indonesian marketplace applications: A comparative study with the Netherlands. Rechtsidee, 14(1). https://doi.org/10.21070/jihr.v14i1.1149

Az-Zahra', P. N., Nurlaily, & Agustianto. (2025). Regulating dark patterns in Indonesian e-commerce: Comparative lessons from South Korea and the EU. Journal of Judicial Review, 27(2). https://doi.org/10.37253/jjr.v27i2.11304

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union.

European Union. (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services (Digital Services Act). Official Journal of the European Union.

European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union.

Hayati, A. N. (2025). The issue of dark patterns in digital platforms: The challenge for Indonesia's consumer protection law. Asian Journal of Law and Society, 11(4), 453–465. https://doi.org/10.1017/als.2024.24

Hidayat, Y. E., & Manurung, N. C. F. (2026). Protecting consumer autonomy from AI-personalized dark patterns on e-commerce platforms in Indonesia. TITAH: Journal of Law.

Indonesia. (1999). Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

Indonesia. (2019a). Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Indonesia. (2019b). Peraturan Pemerintah Republik Indonesia Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik.

Indonesia. (2022). Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Indonesia. (2024a). Peraturan Presiden Republik Indonesia Nomor 49 Tahun 2024 tentang Strategi Nasional Perlindungan Konsumen.

Indonesia. (2024b). Peraturan Menteri Perdagangan Republik Indonesia Nomor 17 Tahun 2024 tentang Rencana Aksi Strategi Nasional Perlindungan Konsumen.

Indonesia. (2026). Peraturan Menteri Perdagangan Republik Indonesia Nomor 19 Tahun 2026 tentang Perdagangan Melalui Sistem Elektronik.

Jannah, M., Mahmuda, Z., & Alankrita, A. (2025). The digital economy boom: How e-commerce is reshaping Indonesia's market. Indonesia Discourse, 2(1), 33–58. https://doi.org/10.15294/indi.v2i1.23034

Lase, A. E. (2025). An analysis of how online reviews, product quality, and digital marketing affect consumer decisions to buy on the Gunungsitoli City TikTok Shop application. Economic Education Analysis Journal, 14(2). https://doi.org/10.15294/eeaj.v14i2.25007

Maharani, R., & Prakoso, A. L. (2023). Perlindungan data pribadi konsumen oleh penyelenggara sistem elektronik dalam transaksi digital. Jurnal USM Law Review, 7(1). https://doi.org/10.26623/julr.v7i1.8705

Manggala, F. P., & Susanti, D. O. (2025). Rethinking consumer legal remedies for damaged goods under protection fees on e-commerce platforms: The Shopee case study. DiH: Jurnal Ilmu Hukum, 21(1), 20–30. https://doi.org/10.30996/dih.v0i0.11722

Mau, H. A. (2025). Consumer legal protection in the digital era: Indonesia and the European Union. SASI, 31(4), 326–343. https://doi.org/10.47268/sasi.v31i4.2802

Muhammadalfansaputra, Zakaria, R., & Yuniaristanto. (2026). Dark pattern dalam social commerce dan pengaruhnya terhadap perilaku konsumen digital di Indonesia: Sebuah systematic literature review. Pendas: Jurnal Ilmiah Pendidikan Dasar, 11(3). https://doi.org/10.23969/jp.v11i03.62184

OECD. (2024). AI, data governance and privacy: Synergies and areas of convergence. OECD Publishing. https://doi.org/10.1787/2476b1a4-en

Putra, T. I., Fakhis, A. Z. P., Tussaleha, A., Firdhausya, M. U., Aflah, M. H. N., Ezzerouali, S. A., & Banane, M. C. (2024). Legal gaps and risks in consumer data processing: An analysis of Indonesian e-commerce under the Personal Data Protection Law. Journal of Private and Commercial Law, 8(2), 199–230. https://doi.org/10.15294/jpcl.v8i2.20081

Putra, T. I., Fibrianti, N., & Fakhrullah, M. R. (2024). Data protection impact assessment indicators in protecting consumer personal data on e-commerce

platforms. The Indonesian Journal of International Clinical Legal Education, 6(1), 111–150. https://doi.org/10.15294/iccle.v6i1.2002

Putra, T. I., Fibrianti, N., & Prasetya, R. A. (2025). Liability of e-commerce service providers for processing consumer personal data: Comparative study of Indonesia & Europe. Journal of Private and Commercial Law, 9(1), 72–109. https://doi.org/10.15294/jpcl.v9i1.9370

Rosidah, Z. N., & Karjoko, L. (2025). Enhancing consumer protection in electronic transactions in Indonesia. Sriwijaya Law Review, 9(1), 194–207. https://doi.org/10.28946/slrev.Vol9.Iss1.3942.pp194-207

Subagyono, B. S. A., Romadhona, M. K., Chumaida, Z. V., Suheryadi, B., & Elkhashab, N. S. (2024). Can Indonesia's laws keep up? Protecting consumer rights in digital transactions. Journal of Law and Legal Reform, 5(3), 869–890. https://doi.org/10.15294/jllr.v5i3.4202

Supriyanto, & Hadi, M. N. (2025). Analisis mitigasi dark pattern pada e-commerce di Indonesia. Trade Policy Journal.

Triseptina, A., Rahmani, N. A. B., & Rahma, T. I. F. (2026). A protection model against side effects of cosmetic products in e-commerce: Perspectives from Islamic economics, social, and risk management. Economic Education Analysis Journal, 15(2). https://doi.org/10.15294/eeaj.v15i2.48472

Wulandari, A. S. R., Buana, A. P., Tarring, A. D., Ma'ruf, T. A., & Ikhtiari, A. (2025). The position of the validity of digital signatures in internet sales transactions: Perspectives of the Civil Code and the Consumer Protection Law. Indonesia Media Law Review, 4(1), 1–23. https://doi.org/10.15294/imrev.v4i1.21263

Zulfah, S., Hapsari, B. J. P., & Rusda, F. (2025). Legal responsibility of digital commerce platforms for seller content that violates public ethics. Indonesia Media Law Review, 4(1), 84–117. https://doi.org/10.15294/imrev.v4i1.31016