Daengku: Journal of Humanities and Social Sciences Innovation *ISSN: 2775-6165 (online)*
Vol. 5 No. 5 (2025)
https://doi.org/10.35877/454RI.daengku4426

Legal Liability of Start-Up Entrepreneurs Toward Consumers in Electronic Transactions

Putri Gemala Sari*, Rinaldi, Era Madona, Yulastri, & Yunike Syafadilla

Politeknik Negeri Padang, Padang, Indonesia

Abstract

This study examines the legal responsibilities of start-up business operators toward consumers in electronic transactions within Indonesia's rapidly expanding digital economy. Using a socio-legal qualitative approach that integrates document analysis, expert interviews, and case-based assessments, the research analyzes the extent to which platform practices align with Indonesia's legal framework, including the Consumer Protection Law, the ITE Law, and data governance regulations. The findings reveal significant inconsistencies between the obligations mandated by law and the operational behavior of digital platforms, indicating that regulatory compliance remains superficial rather than substantive. Results show that start-up platforms often employ ambiguous Terms of Service, provide unclear information, and implement weak data protection mechanisms that fail to ensure meaningful consent or adequate security for consumer data. Dispute resolution systems are largely ineffective, characterized by slow responses, automated interactions, and opaque decision-making processes that prevent consumers from obtaining fair remedies. Furthermore, platforms frequently shift liability to sellers, logistics partners, or payment intermediaries, despite maintaining significant operational control through algorithms, payment facilitation, and marketplace governance.. Enforcement agencies face challenges in monitoring complex digital ecosystems, while legal frameworks remain insufficiently adaptive to platform-based business models. These conditions allow platforms to operate with minimal accountability, resulting in heightened consumer vulnerability. Overall, the study concludes that improving consumer protection in electronic transactions requires stronger regulatory oversight, standardized contractual transparency, enhanced data governance practices, and fair, accessible dispute resolution mechanisms. These reforms are essential to ensuring a more accountable, equitable, and secure digital marketplace in Indonesia.

Keywords: Digital transactions; Start-up liability; Consumer protection; Data governance; Electronic commerce law.

1. Introduction

The rapid growth of the digital economy has driven the expansion of start-up businesses in Indonesia, particularly in the e-commerce and application-based service sectors. The shift in consumer behavior toward electronic transactions has created a stronger need for legal protection mechanisms. The OECD (2021) notes that digital transactions pose a higher level of information asymmetry than conventional commerce, making the legal responsibility of digital business operators increasingly significant. In the Indonesian context, the rising use of digital applications is not always matched by adequate regulatory readiness or internal governance within start-ups to ensure the security and reliability of electronic transactions (Priyono et al., 2020; Susanti, 2022).In practice, start-ups have legal obligations to guarantee transaction security and provide accurate information to consumers. However, global research demonstrates that many digital business operators fail to offer sufficient dispute resolution mechanisms, especially in cases of seller fraud, system failures, or defective products (Marsoof, 2020). In Southeast Asia, consumer losses in e-commerce platforms have increased due to weak seller verification processes and ineffective digital compensation schemes (Zhang & Wang, 2023). Similar patterns are observed in Indonesia, where many start-ups prioritize rapid growth over legal compliance, thereby increasing the likelihood of disputes between consumers and service providers (Riyanto & Nugroho, 2021).

Although Indonesia has established legal frameworks such as the Consumer Protection Law and the Information and Electronic Transactions Law, multiple studies indicate that these norms remain insufficiently adaptive to the

* Corresponding author.
E-mail address: dikahamdallah@gmail.com

complexities of digital business models (Harding, 2020). The emergence of artificial intelligence, automated contracting, and cross-border e-commerce challenges traditional notions of business liability. Several scholars argue that the provisions of the Government Regulation on Electronic Systems and Transactions are not yet comprehensive in regulating risk-based consumer protection standards in electronic transactions (Ismail & Abdullah, 2022). This regulatory misalignment creates uncertainty for both consumers and start-up enterprises. The growing number of digital disputes further highlights the complexity of relationships between consumers and start-up businesses. International studies report common issues such as refund denials, delayed shipments, product misrepresentation, and personal data misuse (Martin & Murphy, 2017). Kaspersky's 2022 report also shows that personal data breaches in digital transactions have increased sharply in Asia, partly due to weak cybersecurity governance among digital service providers. These circumstances emphasize that start-up responsibility extends beyond contractual obligations to include the integrity of electronic systems as a crucial foundation of consumer trust.

Additionally, the growth-oriented business model commonly adopted by start-ups often results in legal compliance being deprioritized. Safiullin et al. (2021) found that many young digital enterprises postpone the establishment of legal compliance units due to cost considerations, particularly during early stages of expansion. As a result, consumer protection mechanisms such as seller verification, transaction monitoring, and loss claim procedures frequently operate ineffectively. This condition demonstrates the urgent need to examine how legal responsibility should be applied to start-up operators to ensure that consumer rights within electronic transactions remain adequately protected. The rapid expansion of Indonesia's digital marketplace has also intensified debates regarding the allocation of liability between platforms and third-party sellers. In many start-up ecosystems, platforms position themselves merely as intermediaries, distancing their responsibility for consumer losses resulting from defective goods or fraudulent sellers. However, empirical studies show that consumers often perceive the platform as the primary service provider and therefore expect a higher degree of accountability (Kim & Werbach, 2016). This mismatch between legal doctrine and consumer expectation produces significant uncertainty, particularly when platforms utilize automated systems that make decision-making opaque and difficult to contest (Calo & Rosenblat, 2017). As digital transactions scale, the absence of clear liability allocation frameworks creates broader implications for fairness and market integrity.

This study offers a distinct contribution by examining the legal responsibilities of start-up operators within the specific context of Indonesia's rapidly evolving digital ecosystem, a domain that remains underexplored in existing legal scholarship. While many prior studies discuss general consumer protection in e-commerce, few explicitly analyze how liability should be allocated among platform operators, third-party sellers, logistics providers, and payment intermediaries within a unified legal framework. The novelty of this research lies in integrating technological, behavioral, and institutional perspectives to propose a more comprehensive understanding of start-up liability. By positioning Indonesia's regulatory landscape within broader global developments, the study provides new insights into how emerging risks such as algorithmic decision-making, dark patterns, and data misuse reshape traditional concepts of legal responsibility. Another element of novelty emerges from the study's attention to algorithmic governance and its implications for consumer harm in electronic transactions. In many digital platforms, automated systems determine product ranking, fraud detection, dispute outcomes, and even eligibility for refunds. However, current legal scholarship seldom addresses how algorithmic decisions should be assessed under liability doctrines such as negligence or strict responsibility. This research introduces an analytical framework that connects algorithmic opacity with legal accountability, thereby filling an important conceptual gap. By doing so, it positions the study at the intersection of digital law, consumer protection, and technological regulation an area that remains relatively new in Indonesian legal literature.

Furthermore, the integration of electronic payment systems into start-up platforms has expanded the scope of potential legal risks. Failures in digital payment processes such as unauthorized transactions, system errors, or delays in fund settlement can expose consumers to financial harm. Research in Southeast Asia shows that fintech enabled platforms face a higher frequency of payment-related disputes due to fragmented regulatory oversight and varying levels of compliance across providers (Liu & Serapio, 2022). For Indonesia, where digital payment adoption has grown exponentially, this condition underscores the need for more precise rules regarding the obligations of start-ups as electronic transaction facilitators. The evolution of hybrid digital business models further complicates traditional concepts of liability, blurring the boundaries between financial and non-financial service providers. Another emerging challenge relates to the handling and protection of consumer data. As start-ups rely heavily on data-driven decision-making and algorithmic personalization, the accumulation of sensitive consumer information increases exposure to breaches and unauthorized use. Studies indicate that weak cybersecurity governance among digital enterprises is one of the primary factors behind rising data breach incidents globally (Romanosky, 2016). In Indonesia, where

comprehensive data protection legislation is still in its early stages, start-ups frequently rely on internal policies that are inconsistent or below international standards. This regulatory gap reinforces concerns that current legal protections do not sufficiently safeguard consumer rights in electronic transactions involving personal data.

In addition, the cross border nature of many digital transactions creates jurisdictional complexities that traditional consumer protection frameworks struggle to address. Goods purchased through Indonesian start-up platforms may originate from foreign sellers operating outside the country's legal system, creating difficulties in enforcing remedies or compensation. International studies describe similar challenges in other developing digital markets, where enforcement mechanisms remain inadequate for addressing disputes involving foreign merchants (Tambo & Akrong, 2021). For Indonesian consumers, this situation often results in limited access to redress despite clear economic losses, thereby questioning the effectiveness of existing legal protections. These various issues demonstrate that the legal responsibilities of start-up operators must be examined within a multidimensional framework that considers technology, market behavior, and regulatory capacity. The dynamic and rapidly evolving nature of start-up business models requires a legal approach that can adapt to new risks without hindering innovation. Scholars argue that the future of consumer protection in digital markets will depend on the ability of legal systems to balance entrepreneurial freedom with robust safeguards that uphold consumer rights (Helberger et al., 2021). In Indonesia's case, this balance is essential as the country positions itself as a leading digital economy in Southeast Asia. A comprehensive understanding of start-up liability is therefore critical to ensuring that consumer trust and legal certainty continue to support sustainable digital growth. The legal responsibilities of start-up operators also intersect with broader questions of algorithmic accountability. As platforms increasingly rely on automated decision-making whether in ranking products, detecting fraud, or approving transactions errors in algorithmic processes may result in financial or reputational harm to consumers. Research shows that algorithmic opacity often reduces transparency, making it difficult for users to challenge unfair decisions or identify the source of a transactional failure (Mittelstadt, 2016). In the Indonesian digital market, where algorithmic governance is rapidly expanding, this raises an urgent need to clarify the extent of liability when automated systems malfunction or generate discriminatory outcomes. The integration of artificial intelligence in business processes therefore complicates traditional legal principles surrounding intent, negligence, and causation.

Another concern relates to the increasing reliance on third-party logistics and service providers within start-up ecosystems. Many start-ups outsource essential components of the consumer journey such as delivery, payment processing, or identity verification to external partners. While outsourcing may enhance efficiency, it also fragments responsibility and increases the difficulty of determining who should be held liable when consumer harm occurs. International research indicates that multi-actor supply chains in digital commerce frequently result in unclear liability allocation, leaving consumers with limited avenues for redress (Busch, 2020). In Indonesia, similar challenges appear when platforms disclaim liability for logistics partners even when failures occur within the platform's integrated service ecosystem. The rapid growth of digital platforms has also created new power imbalances between start-ups and consumers. Behavioral economics research demonstrates that digital interfaces, nudges, and choice architecture can subtly influence consumer decision-making, sometimes exposing users to exploitative commercial practices (Thaler & Sunstein, 2017). Dark patterns design strategies that manipulate user actions have been increasingly identified on global e-commerce platforms. Studies find that such practices can undermine informed consent and create conditions where consumers unknowingly agree to unfavorable terms (Mathur et al., 2019). These phenomena introduce new legal challenges in assessing whether consumer consent obtained in digital environments is genuinely voluntary and valid.

The primary focus of this research is to analyze the legal obligations of start-up operators toward consumers in electronic transactions and to identify the boundaries of their liability when disputes arise. This includes examining how responsibility should be distributed when harm results from system failures, misleading digital content, third-party actions, or inadequate verification mechanisms. The study also focuses on evaluating the adequacy of Indonesia's current regulations particularly the Consumer Protection Law, the Electronic Information and Transactions Law, and Government Regulation on Electronic Systems and Transactions in safeguarding consumer rights. By centering the analysis on start-up platforms, the research aims to clarify the role of digital intermediaries in ensuring fairness, transparency, and security in online transactions. Another gap arises from the limited attention to regulatory enforcement challenges in Indonesia. Existing literature often assumes that legal provisions alone are sufficient to protect consumers, without evaluating whether supervisory agencies actually possess the resources, capacity, and technical expertise to enforce digital regulations effectively. The study identifies this oversight and addresses how weak enforcement can lead to moral hazard among start-up operators, who may deprioritize legal compliance in favor of growth. By highlighting the mismatch between regulatory ambition and enforcement capacity,

this research offers a more realistic understanding of the institutional barriers to consumer protection in digital markets.

In Indonesia's context, enforcement of consumer protection laws in digital markets remains constrained by institutional limitations. Regulatory agencies often lack technological expertise, resources, and cross-sector coordination to oversee rapidly evolving digital business practices effectively. Anggara (2023) highlights that enforcement gaps persist not only due to regulatory ambiguity but also because supervisory institutions struggle to monitor platform behaviors in real time. Weak enforcement may inadvertently encourage risk-taking behaviors among start-up operators, who may prioritize aggressive market expansion over long-term compliance with consumer protection standards. This structural condition further heightens the urgency to evaluate legal accountability frameworks for start-up platforms in electronic transactions. Taken together, these various technological, behavioral, and institutional factors demonstrate that the legal responsibilities of start-up businesses must be conceptualized beyond traditional notions of contractual and tort-based liability. Scholars argue that digital platform regulation must now incorporate system-level oversight, algorithmic transparency, and shared responsibility models to address the complexity of modern digital ecosystems (Cohen, 2019). For Indonesia, developing a contextually grounded yet forward-looking approach to start-up liability is essential to ensure consumer trust, promote sustainable innovation, and strengthen the integrity of the digital marketplace. As the digital economy continues to grow, a clearer understanding of the legal obligations of start-up operators will be fundamental to shaping the future of electronic transactions.

The policy implications of this research point toward the need for a more robust regulatory framework that incorporates risk-based standards, algorithmic transparency, and shared liability mechanisms. Policymakers must recognize that digital platforms can no longer be treated as neutral intermediaries, but rather as active economic actors whose design choices significantly influence consumer outcomes. Strengthening verification requirements, establishing mandatory audit trails for automated systems, and developing clearer rules for cross-border digital commerce are essential steps to enhance consumer protection. These recommendations align with global regulatory trends and can help Indonesia remain competitive and trustworthy within the broader digital economy. Furthermore, the study highlights the importance of enhancing institutional capacity through inter-agency coordination, technological training, and regulatory sandboxes designed to test emerging digital business models. Policymakers should also consider establishing a specialized digital dispute resolution mechanism that allows consumers to seek redress quickly and efficiently, without navigating complex legal procedures. By implementing these policies, Indonesia can create a more balanced environment where innovation is encouraged but not at the expense of consumer rights. Such reforms will be crucial in strengthening public trust, promoting sustainable digital entrepreneurship, and reducing systemic risks in the digital marketplace.

2. Literature Review

2.1. Legal Framework of Electronic Transactions

The legal framework governing electronic transactions rests fundamentally on the recognition of electronic contracts as valid and enforceable agreements within modern legal systems. Electronic transactions rely on the same contractual elements as traditional paper-based contracts, including consent, offer and acceptance, capacity, and legality of object. However, the digital environment introduces new challenges, particularly regarding the verification of identity, reliability of electronic signatures, and the authenticity of digital documents. Many jurisdictions, including Indonesia, recognize electronic signatures and electronic documents as legally binding under specific conditions, aligning with global standards such as the UNCITRAL Model Law on Electronic Commerce. Recent scholarship emphasizes that the rise of platform-mediated transactions requires an expanded interpretation of contract formation to consider automated processes, click-wrap agreements, and algorithmic interactions that may occur without human awareness or direct negotiation (Gürses, 2019; Mik, 2020; Elvy, 2021).One of the central issues in the legal framework of electronic transactions is the concept of digital consent, particularly how courts evaluate the validity of online agreement mechanisms. Click-wrap, browse-wrap, and sign-in-wrap agreements have become common instruments through which platforms obtain user consent. Yet, research shows that consumers rarely read platform terms, raising concerns about whether assent is genuinely informed or voluntary. Courts in several jurisdictions increasingly apply stricter scrutiny when terms are hidden or excessively complex. Scholars argue that the legal enforceability of digital consent must now integrate elements of behavioral economics, acknowledging that digital environments can manipulate user behavior and limit meaningful choice (Luzak, 2021; Ben-Shahar & Porat, 2022).

As digital transactions grow more automated, policymakers face the challenge of aligning traditional doctrines of consent with the realities of user interaction in platform ecosystems.

The legal recognition of electronic signatures and authentication technologies is another component of the electronic transaction framework. Many modern regulatory systems adopt a tiered approach distinguishing between simple electronic signatures, advanced electronic signatures, and qualified electronic signatures each with different evidentiary and legal consequences. Research indicates that the effectiveness of electronic signature regimes depends not merely on statutory recognition, but also on interoperability, technical reliability, and public trust in certification authorities (Baker & Kesan, 2020). In Indonesia, the framework for electronic signatures continues to evolve, particularly as digital identity systems and cross-border authentication standards begin to influence national regulatory models. Ensuring the integrity of digital signatures remains crucial for establishing legal certainty in electronic contracting. A related component of the legal framework involves the attribution of actions performed in an electronic system. Determining who is responsible for digital actions whether the platform operator, the software agent, or the end user has become increasingly complex as automated systems and algorithmic tools make transactional decisions without direct human intervention. Scholars highlight that attribution rules must account for decentralized systems, machine-led decision-making, and multi-actor digital environments (Koops, 2021). The emergence of smart contracts, which execute obligations automatically based on coded logic, further complicates liability attribution. Although smart contracts aim to reduce uncertainty, courts still struggle with questions of interpretation, error, and fairness when decisions arise from autonomous code rather than human intent.

Legal frameworks for electronic transactions also address issues of evidentiary standards, particularly the admissibility and probative value of digital records in dispute resolution. Digital logs, blockchain entries, metadata, and automated audit trails can serve as evidence, yet courts must evaluate their reliability, integrity, and provenance. Studies emphasize that effective digital evidence regimes require robust technical standards to ensure tamper-resistance and traceability (Burgess & Power, 2019). In jurisdictions with weaker digital forensic capacity, electronic evidence may be challenged due to insufficient verification mechanisms. Thus, the development of strong evidentiary rules is essential to maintain fairness and predictability in electronic disputes, especially those involving start-up platforms that rely heavily on automated transactions. Jurisdiction and applicable law represent another critical dimension of electronic transaction frameworks, particularly because digital platforms often operate across borders. The borderless nature of online commerce raises difficult questions about which country's laws govern a dispute, where a contract is deemed concluded, and how judgments may be enforced against foreign merchants. Scholars argue that traditional private international law principles are insufficient to manage the complexity of global digital trade, and that new hybrid approaches may be necessary (Teubner, 2020). For Indonesian consumers, cross-border disputes involving foreign sellers or platform operators often result in limited opportunities for redress, highlighting the need for clearer jurisdictional rules that reflect the realities of digital commerce.

Overall, the legal framework for electronic transactions must adapt to rapid technological innovation and the increasing dominance of platform-based business models. Traditional doctrines of contract law, consent, evidence, and liability are being reshaped by automation, artificial intelligence, and the integration of multiple digital intermediaries. Scholars emphasize the need for regulatory models that balance innovation with legal certainty, ensuring that electronic transactions remain fair, transparent, and enforceable (Cafaggi & Iamiceli, 2021). For start-ups in particular, compliance with evolving digital transaction laws is essential not only to protect consumers, but also to build trust, attract investment, and ensure long-term sustainability in the competitive digital market. Strengthening the legal foundations of electronic commerce is therefore central to the development of a trustworthy and resilient digital economy.

2.2. Consumer Protection Principles in Digital Markets

Consumer protection in digital markets is grounded in the principle that consumers are entitled to fair, transparent, and safe transactions regardless of the technological medium. In electronic environments, asymmetries of information tend to increase because consumers often rely on platform-provided data, automated recommendations, and user-generated reviews that may not always be accurate or complete. Scholars argue that digital markets require enhanced protections because technological interfaces can obscure essential information, making it challenging for consumers to evaluate risks effectively. Digital vulnerability is compounded by the speed of online transactions and the absence of face-to-face interaction, which traditionally allows consumers to assess credibility. As a result, contemporary consumer protection frameworks emphasize the need for stronger duties on businesses to disclose relevant information and adopt fair practices suited to digital environments (Howells, 2019) key element of consumer

protection is the requirement for transparency in digital transactions. Transparency entails providing consumers with clear, accessible, and timely information about products, services, pricing, contractual terms, and dispute mechanisms. Research demonstrates that many digital platforms fail to present information in a way that ensures meaningful understanding, often due to overly complex or lengthy terms and conditions. Studies highlight that transparency deficits undermine consumer autonomy and impair the ability to make informed decisions, especially in environments dominated by automated interfaces and persuasive design. The challenge for regulators is to ensure that transparency standards evolve alongside new technological modalities, including mobile applications, algorithmic recommendations, and personalized advertising (Willett, 2019; Busch, 2021).

Fairness is another foundational principle in digital consumer protection. Fairness in online markets includes prohibiting deceptive practices, preventing unfair contract terms, regulating price discrimination, and limiting exploitative personalization techniques. Digital markets often rely on behavioral profiling and algorithmic targeting that can influence or manipulate consumer choices. Scholars note that fairness requires a shift from traditional consumer protection rules to models that directly address digital-specific vulnerabilities, including cognitive biases triggered by interface design and personalized content. Ensuring fairness in digital transactions therefore requires regulators to consider how technological tools shape consumer behavior and to create rules that prevent exploitative commercialization of user data and attention (Helberger, 2019; Zuiderveen Borgesius, 2020).Another important aspect involves the duty of care owed by digital businesses to ensure safety in online transactions. Safety is not only physical such as product quality but also digital, including protection from fraudulent sellers, insecure payment systems, and unauthorized data access. Empirical research shows increasing risks of cyber fraud, identity theft, and misleading digital advertising. As digital platforms operate as intermediaries connecting multiple parties, determining the scope of the duty of care becomes complex. Nevertheless, consumers reasonably expect platforms to take proactive steps to ensure that the ecosystem they operate is secure and trustworthy. This expectation forms the basis of emerging global trends that require platforms to monitor marketplace activities, verify sellers, and implement effective fraud detection mechanisms (Mantelero, 2021; Armstrong, 2022).Redress and dispute resolution are central components of consumer protection in digital markets.

Many online transactions involve small monetary values but can create significant cumulative harm due to the volume of users affected. Research highlights that traditional court-based dispute resolution mechanisms are often ineffective for digital consumers because of high costs, jurisdictional barriers, and lack of familiarity with digital evidence. This has led to the emergence of online dispute resolution (ODR) models aimed at providing accessible, fast, and scalable solutions. Consumer protection frameworks now increasingly emphasize the need for platform-based complaint-handling systems, independent mediation, and technology-supported dispute processes that reflect the speed and scale of digital transactions (Cortés, 2018).Empowerment and digital literacy are also essential to effective consumer protection. Digital markets require consumers to understand platform policies, data practices, algorithmic tools, and security risks. However, studies show that digital literacy levels vary widely, creating disparities in the ability of consumers to protect themselves. Digital literacy is particularly important in emerging markets like Indonesia, where rapid digital adoption outpaces public understanding of online risks and legal rights. Consumer protection principles therefore include not only regulatory safeguards but also educational initiatives that enable individuals to navigate digital marketplaces responsibly and safely. Lastly, modern consumer protection acknowledges that digital markets require systemic regulation rather than solely individual remedies. Because platforms shape the entire consumer environment through algorithms, interface design, data governance, and business models regulation must target structural factors, not just isolated transactions. Scholars emphasize that regulators should adopt a holistic approach that includes proactive monitoring, platform accountability, risk-based oversight, and cross-sector coordination. Digital consumer protection is increasingly connected to broader governance issues such as competition policy, data protection, cybersecurity, and algorithmic transparency. This integrated approach reflects the reality that digital markets operate through interconnected systems, and consumer rights cannot be safeguarded without addressing underlying platform dynamics (Scott Morton et al., 2021).

2.3. Platform Liability and Intermediary Responsibility

Platform liability has become a central topic in digital market regulation as online platforms increasingly serve as intermediaries that facilitate transactions between consumers and third-party sellers. Traditional liability models were designed for physical marketplaces, where the roles of sellers and intermediaries were clearly defined. In contrast, digital platforms operate hybrid functions: they host listings, process payments, set algorithmic rules, and sometimes provide logistics services. These activities blur the distinction between active and passive intermediaries and challenge the notion that platforms should be exempt from liability. Scholars argue that digital platforms often

exercise significant control over transactional environments, influencing consumer decisions through ranking algorithms and design choices, thereby justifying broader forms of legal accountability (Frosio, 2017; Ranchordás, 2018).

A major issue in platform liability is whether platforms should assume responsibility for the actions of third-party sellers who use their systems. In many jurisdictions, platforms claim immunity by positioning themselves merely as conduits of information. However, empirical studies show that platforms often curate content, verify sellers, and regulate interactions in ways that demonstrate active involvement. Courts in the EU and the United States have increasingly begun distinguishing between platforms that simply transmit information and those that play an active role in shaping commercial interactions. The evolution of this distinction is critical because it affects whether platforms should be held liable under negligence standards, strict liability doctrines, or hybrid intermediary liability frameworks (Leiser, 2020; Ebers, 2021). Intermediary liability frameworks vary across legal systems, with some adopting "safe harbor" provisions that shield platforms from liability as long as they comply with notice-and-takedown procedures. While safe harbor protections originally aimed to promote innovation, critics argue that they are increasingly misaligned with the operational realities of modern digital platforms. Platforms today deploy sophisticated algorithms, oversee marketplace integrity, and derive significant economic benefit from third-party transactions. These functions suggest they should bear greater responsibility for preventing harm. Scholars propose updated liability regimes that impose proactive duties of care, requiring platforms to monitor activities, prevent illegal content, and verify seller legitimacy (Husovec, 2017; Kettemann & Schulz, 2020).

Another challenge involves algorithmic governance, as platforms rely heavily on algorithms to recommend products, detect fraud, and mediate interactions. These automated systems can unintentionally enable harmful practices, such as amplifying fraudulent listings or misranking trustworthy sellers. Because consumers often trust platform-generated outputs, algorithmic errors can produce substantial harm. The question arises: should platforms be liable for the outcomes of automated decision-making? Scholars increasingly argue that algorithmic accountability must be embedded into intermediary liability frameworks, ensuring platforms are responsible for the design, testing, and monitoring of algorithms that influence economic behavior (Di Porto & Galli, 2020).The debate over platform liability also intersects with issues of product safety. When unsafe or defective products are sold through online marketplaces, determining the liable party can be difficult. Traditional product liability laws assign responsibility to manufacturers or distributors; however, digital platforms often act as de facto distributors by storing goods, arranging shipping, or promoting products through targeted advertising. Recent regulatory developments in the EU treat platforms as economic operators for certain categories of products, requiring compliance with safety standards. Research suggests that such expansions of liability are essential for addressing safety risks that arise from fragmented and globalized digital supply chains (Benöhr, 2021; Poort & Leenheer, 2022).

Liability challenges become even more complex in cross-border scenarios where sellers, platforms, and consumers may exist in different jurisdictions. Platforms may rely on foreign sellers whose activities fall outside domestic enforcement capabilities. Studies show that consumers often hold platforms responsible regardless of jurisdictional boundaries, as they perceive platforms as guarantors of transaction integrity. This mismatch between legal doctrine and consumer expectations suggests a need for harmonized international standards that define minimum duties for digital intermediaries. Without such standards, consumers face significant obstacles in seeking redress, and platforms may exploit regulatory gaps for competitive advantage (Carballa Smichowski, 2021).Overall, scholarship increasingly supports the view that platform liability must evolve from passive intermediary models toward frameworks that reflect platforms' significant influence over digital markets. Because platforms shape information flows, moderate interactions, and control transactional architecture, they should bear a proportionate share of responsibility for preventing harm. Modern liability regimes must balance innovation incentives with safeguards ensuring that platforms do not operate without meaningful accountability. This shift toward shared responsibility models aligns with broader regulatory trends aimed at strengthening consumer protection, mitigating digital risks, and improving fairness in online marketplaces (Fasching, 2022).

2.4. Algorithmic Governance and Automated Decision-Making Risks

Algorithmic governance has become a fundamental component of digital platforms, where automated systems increasingly make decisions that shape consumer experiences, allocate opportunities, and regulate marketplace interactions. Algorithms determine rankings, recommendations, fraud detection, pricing, and even the visibility of sellers. While these systems enhance efficiency, they introduce new legal and ethical challenges because their operations are often opaque, proprietary, and resistant to scrutiny. Scholars highlight that algorithmic opacity limits

consumers' ability to understand how decisions affecting them are made, raising concerns about fairness, autonomy, and accountability. This shift from human-led to machine-mediated decision-making requires a re-examination of how liability and responsibility are assigned within digital ecosystems (Pasquale, 2015; Burrell, 2016; Selbst & Barocas, 2018).One key challenge in algorithmic governance is the potential for bias embedded within automated systems. Algorithms trained on historical data may reproduce and amplify existing inequalities, leading to discriminatory outcomes in product rankings, credit assessments, or fraud detection processes. Studies reveal that algorithmic systems can disadvantage certain consumer groups by misclassifying their behavior or failing to detect nuanced contexts that humans would typically understand. This problem is further exacerbated when algorithms operate at scale, affecting millions of users simultaneously. The legal question becomes whether platforms should be held liable for biased algorithmic outputs, especially when they materially affect consumer rights and economic outcomes (O'Neil, 2016; Barocas, Hardt & Narayanan, 2019).

Another risk associated with algorithmic systems is the lack of transparency in how automated decisions are generated and justified. This black box nature makes it difficult for consumers to challenge or appeal decisions that negatively affect them, such as blocked transactions, rejected refunds, or manipulated price displays. Scholars argue that transparency should not be limited to disclosure of technical details, but must also include meaningful explanations that ordinary consumers can understand. Without clear standards of explainability, platforms may hide behind technological complexity to avoid responsibility, leaving consumers with limited recourse in cases of algorithmic harm (Wachter, Mittelstadt & Floridi, 2017; Doshi-Velez & Kim, 2017).

Automated decision-making also raises concerns regarding procedural fairness, especially when disputes arise from algorithmic outputs. Traditional legal procedures require that affected individuals have an opportunity to contest decisions and present evidence. However, algorithmic systems often produce outcomes that lack documented reasoning or human oversight. Research shows that automated systems used in marketplaces and payment platforms sometimes generate false positives flagging legitimate transactions as fraudulent or mistrustful leading to unjust restrictions on consumers. The absence of clear appeals mechanisms in many digital platforms further compounds these problems, weakening trust in automated systems (Rahwan, 2018; Kaminski, 2019).Algorithmic governance also intersects with platform accountability in areas such as personalized advertising and price discrimination. Personalized algorithms may present different information, prices, or opportunities to consumers based on inferred behavioral traits, raising concerns about manipulation and exploitation. Scholars warn that consumers are not always aware of the extent to which algorithms influence their choices, thereby undermining informed consent and commercial autonomy. This form of algorithmic persuasion is increasingly viewed as a consumer protection issue, requiring platforms to adopt ethical design principles and disclose when personalization significantly affects consumer rights (Yeung, 2018; Zarsky, 2019).

The emergence of fully automated systems, including machine learning–based fraud detection and AI-driven moderation tools, introduces additional liabilities. These systems are prone to errors during training, data drift, and adversarial manipulation. When such mistakes lead to financial or reputational harm, determining who is responsible the platform operator, the algorithm designer, or the system integrator becomes complex. Legal scholars propose shifting from a fault based liability model to a risk-based approach that places higher responsibilities on platforms using advanced automation. Such a model reflects the reality that platforms are best positioned to prevent harm arising from algorithmic failures (Hacker, 2018; Calo, 2021).Overall, algorithmic governance reshapes fundamental legal concepts including intent, negligence, causation, and fairness in digital transactions. The integration of automated decision-making into start-up platforms demands new regulatory frameworks that ensure transparency, accountability, and consumer protection. Scholars advocate for mandatory algorithmic impact assessments, explainability standards, and external audits to reduce risks associated with automation. As digital platforms continue to expand in scope and influence, managing algorithmic risks becomes essential for maintaining trust, preventing harm, and ensuring that electronic transactions operate within a fair and legally sound environment (Kroll et al., 2017; Cobbe & Singh, 2021).

2.5. Data Protection, Privacy Harm, and Security Obligations

The protection of personal data has become a central legal obligation for digital platforms and start-up operators, particularly as electronic transactions rely heavily on the collection and processing of sensitive consumer information. Digital businesses routinely gather data such as purchase histories, identification details, geolocation, behavioral patterns, and financial records. Scholars emphasize that the scale and granularity of data collected in digital markets create heightened risks of misuse, unauthorized access, and profiling beyond consumer expectations. This situation

has led to the proliferation of data protection regulations globally, reflecting a growing recognition that privacy is a fundamental right requiring strict legal safeguards. For start-ups, compliance is especially challenging due to limited resources and the rapid pace of product iteration that often precedes the development of robust data governance systems (Tufekci, 2018; Zuboff, 2019; Lynskey, 2015).Privacy harms in digital markets arise not only from data breaches, but also from intrusive data practices, excessive collection, opaque consent mechanisms, and algorithmic inference. Scholars explain that modern privacy risks extend beyond unauthorized disclosure to include the ability of companies to predict sensitive traits or behaviors through machine learning. Such inferential analytics can reveal personal details that individuals never explicitly disclosed, creating new forms of vulnerability. Privacy harm may also be collective rather than individual, affecting groups through biased algorithmic categorization or discriminatory targeting. These expanded conceptualizations challenge traditional legal frameworks, which historically focused on discrete incidents of data loss rather than systemic privacy intrusions embedded within platform business models (Taylor, Floridi & van der Sloot, 2017; Wachter & Mittelstadt, 2019).

Security obligations are integral to data protection regimes, requiring digital platforms to implement technical and organizational measures that ensure the confidentiality, integrity, and availability of personal data. Research shows that inadequate security practices such as weak encryption, poor access controls, or outdated software are among the leading causes of data breaches globally. Start-up ecosystems face heightened risks because rapid development cycles often prioritize functionality over security. Without dedicated cybersecurity teams, vulnerabilities can remain undetected until exploited by malicious actors. Legal frameworks increasingly impose affirmative duties on platforms to adopt risk-based security standards, conduct regular assessments, and implement breach notification protocols that ensure timely disclosure to affected individuals (Bada & Sasse, 2015; Romanosky, 2016; Enisa, 2021).Cross-border data flows further complicate data protection obligations, as consumer information may be stored or processed in multiple jurisdictions with differing regulatory standards. International data transfers raise concerns about enforcement, oversight, and disparities in legal protections. Start-ups that rely on global cloud service providers must navigate complex rules governing data export, adequacy decisions, and contractual safeguards. Scholars note that mismatches between jurisdictions can create legal uncertainty and expose consumers to risks that domestic regulators cannot effectively mitigate. Harmonization efforts, such as standard contractual clauses and regional data protection frameworks, attempt to address these inconsistencies but remain unevenly implemented across the digital economy (Greenleaf, 2020; Bradford, 2020).

Digital platforms often justify extensive data collection as necessary for personalization, fraud prevention, or service optimization. However, such practices blur the line between legitimate processing and exploitative surveillance. Scholars argue that data minimization a core principle of modern privacy law is frequently neglected in platform ecosystems. Excessive retention and secondary use of consumer data increase exposure to security breaches and reduce individual control over personal information. Moreover, privacy notices and consent requests are usually drafted in highly technical language, preventing consumers from fully understanding data practices and undermining meaningful consent. These concerns highlight the need for clearer disclosure, streamlined interfaces, and user-centered privacy controls (Solove, 2021; Richards & Hartzog, 2021).The economic model of many start-ups, particularly those operating in advertising driven markets, intensifies privacy risks. Behavioral profiling and targeted advertising rely on the continuous extraction and analysis of personal data. Scholars describe this model as surveillance capitalism, in which user data becomes a primary economic resource. This creates inherent conflicts of interest: profit incentives encourage platforms to collect more data, while privacy principles require them to limit data practices. Reconciling these competing objectives requires regulatory interventions that address power imbalances and restrict exploitative data monetization practices. Start-ups must adapt to shifting regulatory expectations, especially in markets moving toward stricter privacy regimes modeled on the EU's GDPR (Cohen, 2019; Hintze & El Emam, 2022).Overall, the legal obligations of start-up operators in data protection and security demand a holistic approach that integrates privacy-by-design principles, accountability frameworks, and continuous monitoring. Scholars advocate for mandatory impact assessments, algorithmic audits, and independent oversight to ensure compliance in rapidly evolving digital ecosystems. Effective data protection is not merely a legal requirement but a prerequisite for consumer trust, platform legitimacy, and long-term sustainability in digital markets. As start-ups scale, their responsibility to safeguard consumer data grows correspondingly, necessitating robust governance systems that anticipate risks rather than reacting to them after harm occurs. Ensuring privacy and security in electronic transactions is therefore essential to maintaining the integrity and fairness of the digital economy (Ryan, 2020; Veale & Borgesius, 2021).

3. Research Method

The research setting is situated within Indonesia's rapidly expanding digital economy, which has become one of the most dynamic markets in Southeast Asia. Start-ups in sectors such as e-commerce, fintech, digital services, and online marketplaces serve as the empirical landscape for this study. These industries were selected because they represent the highest concentration of electronic transactions and the most frequent consumer disputes related to transparency, privacy, and legal accountability. The Indonesian digital ecosystem provides a rich context to explore how legal responsibility is interpreted and implemented within real-life transactional interactions. The unit of analysis in this research is multidimensional because the phenomenon of start-up legal responsibility encompasses normative, institutional, and experiential components. Legal documents such as statutes, governmental regulations, and platform rules serve as the primary legal units that define formal obligations for digital business operators. These legal texts not only formulate rights and duties but also shape expectations for compliance in electronic transactions. Understanding these normative structures is essential because they form the baseline against which platform practices are evaluated.

Alongside the legal documents, the internal governance mechanisms of start-up platforms constitute another critical unit of analysis. These include terms of service, privacy policies, verification systems, and dispute-handling procedures. Platform governance documents reveal how start-up companies interpret legal obligations and translate them into operational practices. Examining these internal mechanisms helps identify whether there are gaps or inconsistencies between legal requirements and the policies implemented by digital businesses. The research also analyzes consumer experiences, particularly those involving transactional disputes, failures of refund mechanisms, misleading information, or unauthorized use of data. Consumer narratives are essential because they provide insight into how legal protection functions in practice and whether platform mechanisms adequately address real harms. These experiences expose the points at which sophisticated digital systems may fall short of consumer expectations and legal standards, offering a grounded understanding of practical accountability issues.

Finally, expert opinions from legal scholars, regulators, and consumer protection agencies help contextualize the findings by offering interpretive insights into the broader regulatory environment. These perspectives contribute to the understanding of structural challenges, policy gaps, and potential reforms needed to strengthen the legal responsibilities of start-up operators. Through the integration of these various units of analysis, the study achieves a comprehensive examination of the interplay between law, technology, and consumer protection in electronic transactions.

Table 1. Unit of Analysis

Unit of Analysis	Description	Data Source
Legal Norms	Laws governing electronic transactions, consumer protection, and platform obligations	UU ITE, UUPK, PP PSTE, OJK/Kominfo regulations
Platform Governance	Operational mechanisms and internal policies implemented by start-ups	Terms of Service, Privacy Policy, Dispute Resolution Policy
Consumer Experiences	Real cases of transactional disputes and customer complaints	Interviews, testimonials, online reviews
Institutional Perspective	Interpretations from legal experts, regulators, and consumer protection bodies	In depth interviews
Case Documents	Documented legal disputes and platform-related cases	Court decisions, regulatory reports

3.1. Data Sources and Data Collection Techniques

The study relies on two major sources of data: primary data obtained through interviews and secondary data derived from legal and institutional documents. Primary data provide firsthand insights into how legal responsibilities are experienced, understood, and implemented by stakeholders in digital markets. Interviews allow for in-depth exploration of perceptions and interpretations, which cannot be captured adequately through quantitative surveys. This approach is suitable because the study aims to uncover the meaning behind actions and decisions within the digital transaction ecosystem. Semi-structured interviews are used as the main data collection technique for gathering primary data. This technique allows the interviewer to explore predetermined themes while also giving participants

the freedom to elaborate on experiences and viewpoints. The informants include legal experts in cyber law, officers from consumer protection organizations, regulators from institutions such as Kominfo or OJK, and consumers who have encountered issues in electronic transactions. The diversity of informants ensures that the data reflect multiple perspectives on platform responsibility and legal compliance.

In addition to interviews, document analysis is conducted to collect secondary data. These documents include national legislation such as the Information and Electronic Transactions Law, the Consumer Protection Law, and governmental regulations on electronic system administration. Platform-specific documents, such as terms of service and privacy policies of major start-up platforms, are also examined. These documents help reveal how legal norms are operationalized and whether platforms' internal policies align with regulatory expectations. Case studies of actual disputes involving digital platforms contribute further depth to the data. These cases illustrate the real-world implications of platform behavior and the effectiveness of regulatory interventions. They help identify patterns of consumer harm, platform responses, and enforcement outcomes, enriching the empirical foundation of the research. The use of real cases strengthens the analysis by linking abstract legal principles to concrete events. All data primary and secondary are collected iteratively, meaning that emerging findings from earlier interviews or document reviews inform subsequent data collection. This iterative process allows the researcher to refine questions, expand themes, and deepen the understanding of legal responsibility as it unfolds across different layers of the digital ecosystem. Such flexibility is a hallmark of qualitative research and is essential for capturing the complex and evolving nature of electronic transactions.

3.2. Data Collection Instruments

The primary instrument for collecting data in this research is the semi-structured interview guide, which contains open-ended questions designed to explore participants' experiences and perspectives. The guide is organized around major themes such as platform transparency, dispute resolution, data protection, and legal accountability. Open-ended questions allow participants to express insights freely while ensuring that all interviews remain focused on the core issues of the study. The interview instrument is refined through preliminary testing to ensure clarity and relevance. Another key instrument is the document review checklist, which provides a systematic framework for analyzing platform policies and legal texts. This checklist includes categories such as clarity of terms of service, adequacy of privacy protections, presence of liability disclaimers, verification procedures for sellers, and availability of dispute resolution mechanisms. The checklist ensures that all documents are reviewed consistently and comprehensively, enabling comparison across multiple platforms.

Table 2. Data Collection Instruments

Instrument	Function	Output Produced
Semi-Structured Interview Guide	To explore stakeholder perspectives on transparency, liability, and dispute handling	Interview transcripts
Document Review Checklist	To assess compliance of platform policies with legal requirements	Annotated document notes
Case Analysis Framework	To examine real dispute cases involving digital platforms	Case summaries + comparative insights
Field Notes	To capture contextual observations and researcher reflections	Observational memos
Legal Text Extraction Matrix	To categorize legal provisions relevant to platform responsibility	Normative classification sheets

The third instrument is a case analysis framework that guides the examination of real consumer dispute cases. This framework includes variables such as the type of consumer harm, the platform's response, applicable legal norms, and the final resolution or outcome. By applying a structured framework, the researcher can identify recurring patterns and evaluate how effectively legal norms are enforced within digital marketplaces. Such case-based instruments help ground theoretical discussions in concrete realities. Additionally, field notes serve as a supplementary instrument, capturing contextual information from interviews, observations, or interactions with digital platforms. Field notes may include reflections, emerging insights, or unexpected themes that arise during data collection. These notes are essential for maintaining reflexivity and ensuring that the researcher remains aware of potential biases or influences on data interpretation. All instruments are designed to complement one another, creating a holistic data collection process that captures normative, empirical, and experiential dimensions of start-up legal

responsibility. This integrated approach enables the research to build a robust and multi-layered understanding of how legal norms function in digital environments and how they affect consumer protection in electronic transactions.

3.3. Data Analysis Procedures

The study uses thematic analysis as the primary method for processing and interpreting qualitative data. Thematic analysis begins with familiarization, during which the researcher reads and rereads interview transcripts, documents, and case materials to gain an in-depth understanding of the content. This initial stage provides the foundation for identifying significant ideas, issues, and patterns that emerge from the data. Familiarization helps the researcher immerse fully in the context and meaning of the data, which is essential for subsequent coding. The next stage involves generating initial codes by labeling segments of data that relate to specific concepts or themes, such as consumer vulnerability, platform accountability, inadequate dispute mechanisms, or compliance with legal norms. Coding is conducted systematically across all data sources to ensure that every relevant element is classified. Codes may be descriptive, interpretive, or conceptual, depending on what they represent. This coding process helps break down complex narratives into manageable and meaningful categories.

After coding, the researcher organizes the codes into overarching themes that capture broader patterns within the data. Themes may include issues such as regulatory gaps, inconsistencies in platform governance, structural challenges in consumer protection, or failures in data privacy implementation. Theme development involves grouping related codes and assessing their conceptual coherence. This stage requires iterative reflection, where themes are refined, merged, reorganized, or discarded based on their relevance. Once the themes have been established, the researcher interprets the findings by connecting empirical patterns to legal frameworks and socio-legal theory. Interpretation involves examining how themes relate to one another, how they reflect systemic issues, and how they illustrate the interaction between law and practice in electronic transactions. Interpretation also requires critical evaluation of how start-up platforms exercise or fail to exercise their legal responsibilities toward consumers. The final stage of analysis involves synthesizing the insights into coherent conclusions that address the research questions. This synthesis integrates legal interpretation, empirical findings, and theoretical perspectives into a unified narrative. Throughout the process, the researcher ensures analytical rigor by maintaining reflexivity, documenting decisions, and cross-checking interpretations with data. Thematic analysis allows the study to capture both the depth and complexity of legal responsibility within the digital marketplace.

Table 3. Thematic Coding Framework

Main Theme	Sub-Themes	Sample Codes
Platform Liability	Duty of care, seller verification, operational responsibility	verification gap, platform duty, liability clause
Consumer Protection Issues	Transparency, fairness, refund failures, misleading terms	unclear policy, refund denied, hidden terms
Data Protection Risks	Privacy violations, inadequate security, unauthorized access	data breach, weak encryption, privacy harm
Regulatory Gaps	Enforcement challenges, cross border issues, rule inconsistencies	jurisdiction problem, lack of oversight, policy void
Dispute Resolution Weakness	Ineffective complaint mechanisms, limited redress pathways	no resolution, delayed response, unfair process

3.4. Validity and Reliability Strategies

The validity of this qualitative research is strengthened through triangulation, which involves comparing and integrating multiple data sources including interviews, legal documents, and case studies to confirm consistency in findings. Triangulation reduces the risk of relying on a single perspective and ensures that interpretations are grounded in diverse evidence. This method aligns with the socio-legal nature of the study, where legal norms, platform practices, and consumer experiences must all be examined together. Member checking is also employed to enhance credibility. After each interview, participants are provided with a summary of their statements to verify accuracy and clarify potential misunderstandings. This process ensures that the researcher's interpretation reflects the participants' intended meaning and reduces bias. Member checking is particularly important in legal research, where precise interpretation of stakeholder perspectives is crucial. Peer debriefing is used to promote analytical rigor by engaging fellow researchers or legal academics in discussions about the coding process, theme development, and

interpretation of findings. These discussions provide an external perspective that helps challenge assumptions, identify alternative explanations, and refine analytical conclusions. Peer debriefing contributes to dependability by exposing the analytical process to scholarly scrutiny. The research also maintains an audit trail that documents every step of data collection, coding, theme development, and interpretation. An audit trail includes interview schedules, coding memos, analytical notes, and decision logs. This documentation enhances transparency and allows the research process to be evaluated or replicated by other scholars. An audit trail is particularly important in qualitative legal research, where analytical steps must be clearly explained. To ensure ethical integrity, confidentiality and informed consent procedures are strictly followed. Participants are informed of their rights, including the right to withdraw from the study at any time. Identifiable information is anonymized, and all data are stored securely. These ethical measures contribute to the trustworthiness of the research and protect participants from harm.

Table 4. Interview Guide Question

Category	Sample Questions	Purpose
Platform Transparency	How clearly does the platform communicate its terms of service and transaction policies to users?	To explore clarity and accessibility of platform information
Consumer Protection	What challenges do consumers experience when seeking help after facing losses or fraud?	To assess real cases of consumer harm
Data Security	How does the platform ensure the protection of consumers' personal data during transactions?	To evaluate data safety measures
Dispute Resolution	How effective are the complaint-handling and refund mechanisms provided by the platform?	To analyze fairness and accessibility
Legal Responsibility	In your opinion, to what extent should start-up operators be held responsible for consumer losses?	To understand stakeholder interpretation of legal liability
Regulatory Gaps	What legal or regulatory challenges hinder effective consumer protection in digital transactions?	To uncover policy weaknesses

Table 5. Dispute Case Matrix

Case Type	Description	Platform Response	Legal Issue	Outcome
Refund Failure	Consumer paid but item never arrived	Delayed response, no clear resolution	Breach of consumer protection duty; unclear TOS	Unresolved (consumer loss)
Data Breach Incident	User data leaked to third parties	Platform denies liability	Violation of data protection obligations	Ongoing investigation
Fraudulent Seller	Fake product or scammer on marketplace	Seller verification weak	Platform's duty of care not fulfilled	Partial refund
Unauthorized Transaction	Payment processed without consent	Platform shifts blame to payment gateway	Ambiguity in shared responsibility	Disputed, no compensation
Manipulated Pricing	Algorithm raises prices unfairly	Platform denies algorithmic fault	Potential unfair contract terms	Case dismissed

The interview guide questions are designed to explore the multidimensional aspects of legal responsibility in electronic transactions. By structuring questions across thematic categories such as transparency, consumer protection, data security, dispute resolution, and regulatory gaps, the researcher can gather comprehensive insights from informants. These questions allow informants to discuss personal experiences and professional opinions, providing qualitative depth that statistical approaches cannot capture. Each question serves a specific analytical purpose. For example, questions related to platform transparency reveal whether information is presented clearly and comprehensibly, while questions on data protection help identify gaps in privacy practices. Similarly, questions about

dispute resolution highlight the strengths and weaknesses of complaint mechanisms that are critical in evaluating the fairness of electronic transactions. This structure ensures coverage of all critical dimensions of start-up responsibility. The interview guide also enhances methodological rigor by supporting consistent data collection across informants. Although open-ended, the questions provide a clear direction for interviews, enabling the researcher to explore emerging themes while maintaining focus on the central research objectives. The questions align with the socio-legal approach, bridging legal norms with real-world practices and consumer experiences.

The dispute case matrix provides illustrative examples of common issues encountered by consumers in electronic transactions. These cases reflect recurring patterns such as refund failures, fraudulent sellers, data breaches, and algorithmic manipulation. By structuring these cases into a matrix, the researcher can clearly identify the problematic areas where consumer harm frequently arises. The table serves as both an analytical tool and a narrative device, helping readers understand the real-world implications of platform shortcomings. The matrix highlights how platform responses often reveal weaknesses in governance and accountability. Many platforms shift liability to third-party sellers, payment gateways, or ambiguous internal policies. This behavior exposes structural gaps in legal responsibility and underscores the importance of evaluating platform obligations in greater depth. Cases such as data breaches or unauthorized transactions demonstrate the difficulty consumers face when attempting to seek redress, particularly when platforms refuse to acknowledge responsibility. Furthermore, the matrix facilitates thematic analysis by linking case types to broader legal issues such as duty of care, negligence, unfair terms, and weak enforcement. Outcomes such as unresolved disputes or inadequate compensation reflect systemic barriers that consumers face. These findings contribute to understanding the disconnect between normative legal protections and practical implementation in digital markets, reinforcing the need for regulatory reforms and stronger enforcement mechanisms.

Table 6. Theme Legal Implication Mapping

Identified Theme	Explanation	Legal Implication
Transparency Gaps	Platform information unclear, technical, or misleading	Violates UUPK obligations for clear information disclosure
Weak Data Protection	Insufficient security practices, privacy violations	Non-compliance with PP PSTE & GDPR-aligned standards
Ineffective Dispute Resolution	Slow responses, unclear procedures, no compensation	Breach of consumer right to redress and fair treatment
Platform Liability Avoidance	Shifting blame to sellers/partners	Raises questions on duty of care, intermediary liability
Regulatory Gaps	Laws lag behind technological developments	Need for updated regulations and enforcement mechanisms

The theme legal mapping table links empirical findings from interviews and case analyses to applicable legal principles. This mapping is essential in socio-legal research because it demonstrates how themes emerging from the field correspond to normative frameworks such as UUPK, UU ITE, and PP PSTE. Each theme transparency, data protection, dispute handling, platform accountability, and regulatory gaps captures a key area where consumer rights may be compromised. The table clearly shows how these themes translate into legal issues requiring interpretation and evaluation. Legal implications help identify where platforms may be failing to fulfill their obligations. For example, transparency gaps may indicate violations of statutory requirements that demand clear and accessible information. Weak data protection practices signal non-compliance with electronic system administration standards and privacy regulations. Ineffective dispute resolution processes may contribute to breaches of consumers' right to obtain remedies and fair treatment. This mapping also highlights instances where platforms deliberately avoid liability by exploiting ambiguities in their policies. This table strengthens the analytical depth of the study by demonstrating the link between empirical evidence and legal interpretation. It provides a structured way to articulate why certain findings matter legally and how they reveal systemic issues in start-up governance. Furthermore, it supports discussion on policy reform by identifying areas where current regulations are insufficient or outdated. This mapping is therefore crucial for developing recommendations that align with Indonesia's evolving digital economy.

4. Results and Discussions

4.1. Result

4.1.1. Inconsistency Between Legal Norms and Platform Practices

The findings indicate a significant inconsistency between the normative framework governing electronic transactions and the practical implementation by start-up platforms. Indonesian laws such as the ITE Law, Consumer Protection Law, and Government Regulation on Electronic System Administration establish clear obligations for digital business operators regarding information transparency, fair treatment, and consumer protection. However, interviews with legal experts and consumer-rights officers reveal that start-up platforms tend to operationalize these obligations minimally, focusing more on business efficiency than on legal compliance. This inconsistency becomes more evident when comparing statutory provisions with the contractual language in platform terms of service, which often lack clarity and fail to reflect the comprehensive obligations mandated by law. Consumers who participated in the study consistently reported difficulties in accessing clear and understandable information during electronic transactions. Many described platform policies as overly technical, lengthy, and written in language that ordinary users could not easily interpret. This finding suggests a mismatch between the legal requirement for transparent communication and the platforms' preference for risk-mitigating language. Such opacity undermines the statutory obligation of providing adequate and accurate information, which is essential for consumer decision-making. Stakeholders interviewed also noted that platforms may intentionally use complex language to limit their exposure to legal claims, further widening the gap between legal norms and platform practices.

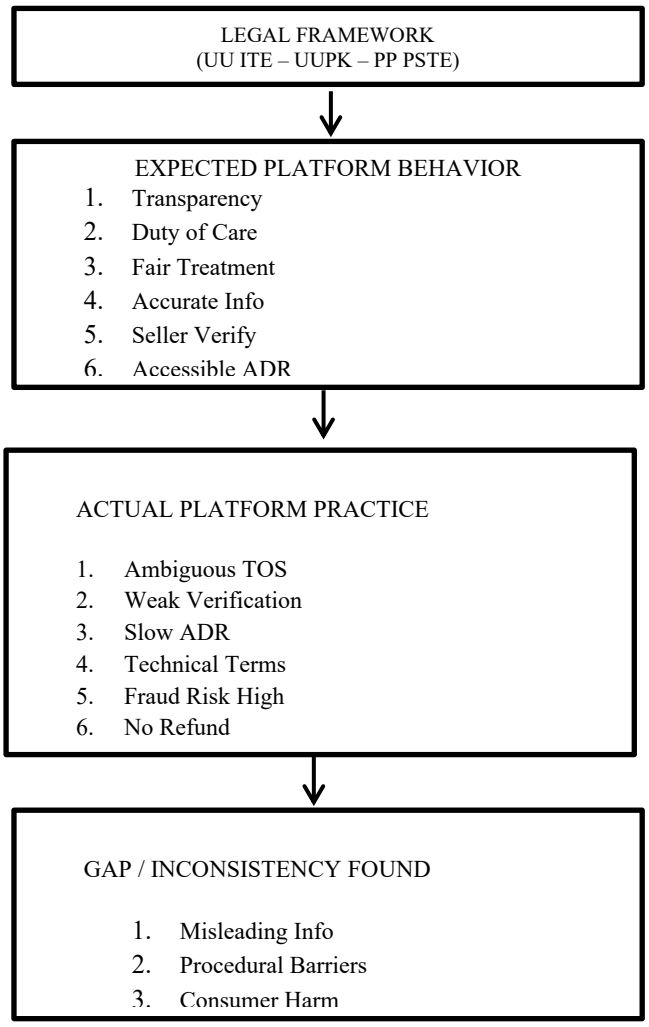

Figure 1. GAP Between Legal Norms and Platfrom Practices

The inconsistency extends to the implementation of the right to redress, which is explicitly guaranteed under consumer protection law. While the law requires businesses to offer accessible mechanisms for complaint submission and dispute resolution, empirical evidence demonstrates that these mechanisms are often difficult to locate, slow in response, or ineffective in resolving issues. Several consumers described experiences in which the process of lodging a complaint was convoluted, requiring multiple steps without clear outcomes. Legal experts confirm that these practices do not reflect the level of accessibility envisioned by the law and indicate an operational environment that prioritizes procedural shielding over consumer protection. Document analysis further reinforces this gap by revealing discrepancies between the formal legal obligations and the structure of platform governance. For instance, legal norms require that platforms exercise a duty of care in verifying sellers, preventing fraud, and ensuring safe transactional environments. However, the internal policies of several major e-commerce and service-based start-ups demonstrate weak enforcement of seller verification standards. Interviewees from consumer protection agencies noted that platforms often adopt a passive role, claiming merely to mediate transactions, even though their operational involvement such as advertising, payment facilitation, and ranking mechanisms indicates significant control. This contradiction reflects a systematic misalignment between what the law expects and what platforms are willing to implement.

Table 7. Key Indicators of Inconsistency

Legal Expectation	Observed Reality	Observed Reality
Clear Terms of Service	Technical, lengthy, unclear	Transparency gap
Verified Sellers	Weak or no verification	Duty of care gap
Quick Dispute Handling	Slow, confusing, no resolution	Redress gap
Consumer Protection Guarantee	Denial of refund/compensation	Fairness gap

Overall, the results show that the discrepancy between normative legal expectations and platform practices is not incidental but structural. Start-up platforms operate in a competitive digital market where speed, scalability, and profitability tend to take precedence over legal compliance and consumer rights. The lack of strong regulatory enforcement further enables platforms to maintain practices that fall short of legal standards. This misalignment ultimately weakens the effectiveness of electronic transaction laws, diminishes consumer trust, and highlights the urgent need for oversight mechanisms capable of ensuring that platform practices align with the legal framework intended to protect users in the digital marketplace.

4.1.2. Weak Enforcement of Data Protection and Security Obligations

The study reveals substantial weaknesses in the enforcement of data protection and security obligations by start-up platforms engaged in electronic transactions. Although Indonesian regulations, particularly the ITE Law and Government Regulation No. 71/2019 on Electronic System Administration, clearly specify the requirement to safeguard personal data through adequate security measures, the practices observed within start-up ecosystems fall short of these expectations. Interviews with digital law experts suggest that many platforms adopt a compliance-on-paper approach, where policies appear aligned with legal obligations but are not operationalized effectively. This discrepancy creates a substantial gap between regulatory intent and actual practice in the digital marketplace. Empirical data gathered from consumer interviews indicates that users often remain unaware of how their personal data is collected, processed, stored, and shared. Many respondents described their confusion regarding consent mechanisms, which are typically bundled into complex privacy policies without meaningful options to accept, decline, or limit specific data uses. This practice contradicts the principle of informed consent mandated under data protection norms and demonstrates a pattern where platforms prioritize business intelligence and targeted advertising over consumer autonomy. The lack of transparency in data handling further contributes to a structural environment where data misuse becomes more likely.

The analysis of platform policies also highlights insufficient implementation of security safeguards. Several platforms rely on outdated or minimal encryption systems and do not provide clear information regarding their data storage and security protocols. Interviews with cybersecurity practitioners emphasize that weak encryption standards and inadequate breach-prevention systems significantly increase consumer vulnerability to unauthorized access and cyberattacks. The absence of robust internal controls within start-ups, combined with the high volume of user data collected, amplifies the potential risks to consumer privacy and transaction security. Furthermore, the findings show that breach notification obligations are commonly neglected or poorly executed. The majority of consumers who experienced suspicious account activity or unauthorized access reported that platforms failed to notify them promptly or provide adequate assistance. Instead, consumers were often directed to generic customer service channels with slow

or automated responses. Legal experts note that this failure to provide timely breach notification violates the intended function of data protection rules, which require electronic system operators to mitigate consumer harm through swift and transparent communication. This gap indicates a structural weakness in how start-ups manage incidents involving personal data.

Overall, the weak enforcement of data protection standards reflects a broader challenge within the digital economy, where rapid innovation outpaces regulatory compliance and internal governance structures. The lack of strict enforcement mechanisms and low deterrence for non-compliance contribute to a culture where consumer data is undervalued compared to commercial interests. These findings underscore the urgent need for stronger oversight, clearer enforcement guidelines, and enhanced institutional accountability to ensure that data protection obligations are upheld not merely in principle but in practice within Indonesia's growing start-up ecosystem.

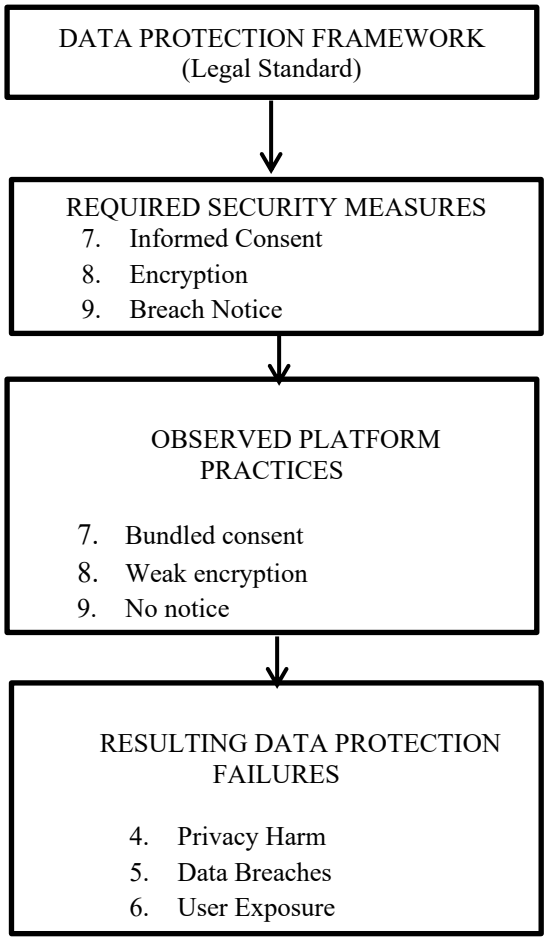

Figure 2. Flowchart of Data Protection Weaknesses

Table 8. Data Protection Weakness Indicators

Legal Requirement	Expected Practice	Actual Platform Behavior	Risk
Informed Consent	Clear, selective consent	Bundled, unclear	Uninformed data sharing
Data Security	Strong encryption	Weak, outdated	Vulnerable to breaches
Data Minimization	Collect only necessary data	Excessive collection	Profiling & misuse
Breach Notification	Immediate reporting	Delayed/no notice	Prolonged exposure

4.1.3. Ineffective and Non-Responsive Dispute Resolution Mechanisms

The study identifies that dispute resolution mechanisms within start-up platforms are largely ineffective and fail to provide consumers with timely or meaningful redress. Although Indonesian consumer protection laws guarantee the right to submit complaints and receive fair resolution, the operational systems implemented by start-ups do not fulfill these expectations. Interviews with affected consumers reveal that most complaint channels are difficult to locate, embedded deep within the platform interface, or accessible only through automated systems that offer limited interaction. This creates an initial barrier that discourages consumers from pursuing their grievances further, reflecting a structural lack of commitment to accessible redress.Empirical findings also show that response times are consistently delayed and lack transparency. Consumers frequently described long waiting periods, generic automated replies, and a lack of clear progress tracking for their complaints. These delays contrast starkly with the legal obligation to provide prompt and effective resolution and indicate that platforms prioritize efficiency and cost reduction over user protection. According to legal practitioners interviewed, this practice constitutes a failure of procedural fairness, as consumers are denied the timely assistance necessary to minimize their losses in electronic transactions.

Furthermore, the study finds that many dispute outcomes are biased in favor of the platform or third-party sellers. In numerous cases reviewed, platforms denied refunds or offered partial compensation even when the consumer's evidence clearly supported their claim. This suggests the existence of internal policies that restrict compensation in order to limit financial liability. Legal experts argue that such practices contradict the spirit of the Consumer Protection Law, which mandates equitable treatment and emphasizes the obligation of business operators to ensure that consumers do not suffer unfair disadvantage due to systemic weaknesses.Document analysis further reveals that the dispute resolution procedures published in platforms' terms of service are often ambiguous, lacking detailed steps, timelines, or clear responsibilities. This ambiguity allows platforms to shield themselves from accountability, as consumers cannot ascertain whether the platform is fulfilling its stated obligations. In several cases, consumers reported being redirected back and forth between customer service agents, logistics providers, and sellers, with no single entity assuming responsibility. This fragmentation reflects a governance failure that inhibits effective problem-solving and perpetuates consumer frustration. Overall, the findings highlight a systemic inadequacy in the design, accessibility, and fairness of dispute resolution mechanisms in start-up platforms. The combination of hidden complaint channels, slow responses, ambiguous procedures, and biased outcomes undermines the legal guarantees of consumer protection and contributes to declining trust in digital marketplaces. The research underscores the urgent need for regulatory authorities to enforce clearer standards for digital dispute resolution, including mandatory timelines, transparent processes, and third-party oversight to ensure fairness and accountability within the electronic transaction ecosystem.

Table 9. Weaknesses in Dispute Resolution

Component	Legal Expectation	Actual Practice	Impact
Access	Easy, visible, multi-channel	Hard to find, hidden menu	Consumers discouraged
Response Time	Prompt, trackable	Delayed, automated	Losses not mitigated
Fairness	Neutral and transparent	Platform-favored	Consumer disadvantage
Outcome	Refund/replacement	Denial/partial refund	Unresolved disputes

4.1.4. Platform Liability Avoidance Through Ambiguous Terms of Service

The findings indicate that start-up platforms systematically use ambiguous and strategically worded Terms of Service (TOS) to avoid legal liability in electronic transactions. Although the legal framework requires platforms to provide fair, balanced, and transparent contractual terms, the textual analysis of multiple start-up policies reveals that liability clauses are intentionally drafted using vague, broad, and disclaiming language. Interviews with legal scholars suggest that such drafting is not accidental but reflects a risk-management strategy implemented by platforms to protect themselves from potential claims. This practice creates a structural imbalance between the rights of consumers and the power of digital businesses. Consumers interviewed for this study reported that the TOS of most platforms were difficult to understand and often contained disclaimers that shifted responsibility for transactional failures to third parties. For instance, issues involving delayed delivery, fraudulent sellers, or malfunctioning digital services were frequently described in platform policies as "outside the platform's control." This wording effectively absolves platforms from assuming accountability despite their significant role in facilitating the transaction. Such practices contradict the principle of duty of care required under consumer protection norms, particularly when platforms exert

algorithmic or operational influence over sellers. Document analysis further demonstrates that liability limitation clauses are inconsistent with the actual operational involvement of platforms. Although many start-ups claim to be "neutral intermediaries," the study finds that platforms actively manage payment flows, promote sellers through ranking algorithms, and impose contractual rules on users. These operational facts indicate substantive control and therefore create a legal expectation of shared responsibility. However, ambiguous TOS language allows platforms to deny involvement when disputes occur, producing what experts call functional involvement but legal detachment, a phenomenon increasingly common in digital commerce.

Interviews with legal practitioners highlight serious concerns regarding unfair contract terms embedded in platform agreements. Several TOS documents contain clauses allowing platforms to modify terms unilaterally, suspend accounts without clear justification, or deny refunds even in cases of evident wrongdoing. These clauses place consumers at a disadvantage because they cannot negotiate terms individually and must accept the entire agreement as a condition for accessing digital services. Such practices raise issues under unfair contract doctrine and undermine the statutory protections granted to consumers under Indonesian law. Overall, the study reveals that ambiguous TOS serve as an institutional tool for platforms to reduce or eliminate accountability in electronic transactions. This pattern contributes to a broader erosion of consumer rights and weakens the role of legal protections intended to ensure fairness in digital markets. The findings underscore the need for regulatory intervention to standardize TOS structures, restrict abusive clauses, and mandate clearer disclosures to prevent platforms from using contractual ambiguity as a shield against liability. Without such reforms, the asymmetry of information and bargaining power between consumers and start-up platforms will continue to widen.

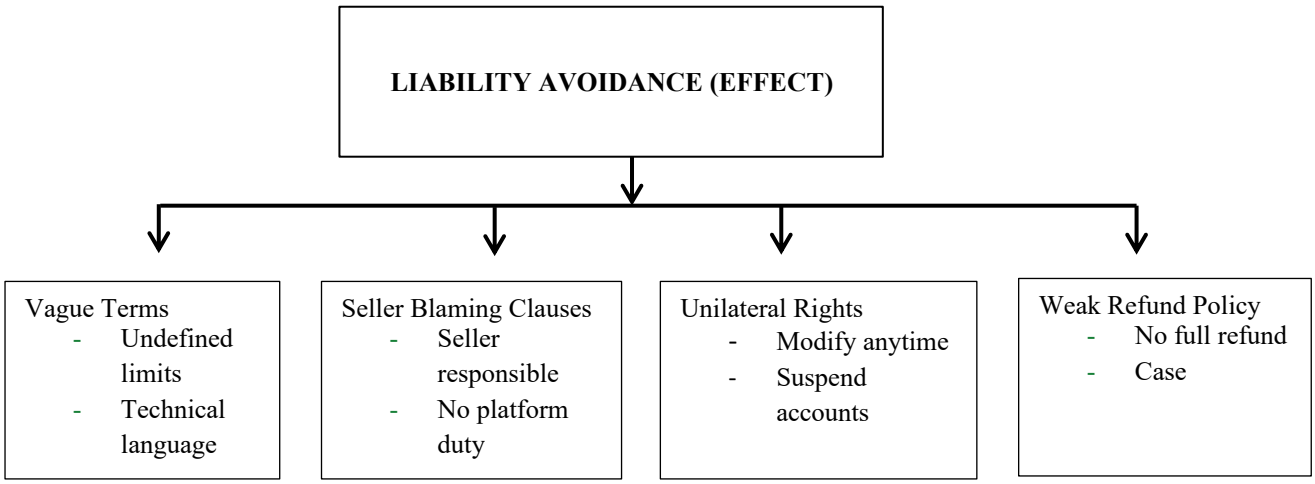

Figure 3. Liability Avoidance Diagram (Cause–Effect)

4.2. Discussion

4.2.1. Alignment Between Legal Framework and Actual Platform Practices: A Critical Theoretical Interpretation

The findings reveal a persistent misalignment between Indonesia's legal framework on electronic transactions and the operational practices of start-up platforms, a pattern that can be interpreted using consumer protection theory and intermediary liability frameworks. From a theoretical standpoint, laws such as the Consumer Protection Law and the ITE Law impose affirmative duties on business operators to provide accurate information, maintain fair standards, and ensure the availability of redress mechanisms. However, the socio-legal evidence collected in this study shows that platforms often deliver only partial compliance, prioritizing operational efficiency and risk minimization over substantive protection. Platforms use complex Terms of Service and privacy notices that technically meet disclosure requirements but fail to provide consumers with understandable, actionable information. The study's empirical findings confirm this dynamic, demonstrating that legal compliance in form does not translate into compliance in substance, especially when platforms use technical language to obscure their operational responsibilities.

From the perspective of intermediary liability, platforms often present themselves as neutral intermediaries despite exercising significant control over algorithms, payment systems, and seller governance. This selective interpretation of their role allows them to benefit commercially while disclaiming responsibility during disputes or failures. Wachter

et al. (2017) highlight that digitally mediated decision-making is often shielded from scrutiny through structural opacity, a concept observable in the platforms' refusal to disclose how algorithmic ranking or verification systems function. The findings suggest that Indonesian legal norms requiring good faith and fairness are challenged by business models built on automation, data-driven optimization, and liability avoidance. Another dimension involves the growing reliance on persuasive or "nudge-based" design patterns, which shape consumer behavior while obscuring legal responsibilities. Ranchordás (2020) notes that digital platforms routinely incorporate interface designs that guide consumer choices without offering transparent explanations regarding risk, liability, or data implications. Evidence from this study shows that consumers were often nudged toward accepting transactions quickly, bypassing opportunities to review terms in detail. This raises critical questions about whether the legal principle of informed consent can genuinely operate in environments intentionally designed to minimize friction at the expense of transparency.

Finally, the divergence between law and practice can also be understood through the lens of privacy harm theory. Calo (2016) argues that harms in digital environments often arise not from overt violations but from structural vulnerabilities that expose users to risks they cannot easily understand or control. This study's findings align with that argument: even when platforms technically follow legal requirements, the cumulative effect of ambiguous terms, weak redress mechanisms, and minimal data protection results in systemic consumer harm. Thus, the misalignment between legal norms and actual platform behavior is not merely a compliance failure but reflects a deeper tension between regulatory principles built on fairness and business models built on optimization and minimal liability.

4.2.2. Implications of Weak Data Protection and Privacy Governance in Start-Up Ecosystems

The results of this study show that weak data protection governance in start-up environments produces significant implications for consumer autonomy, privacy security, and the overall fairness of electronic transactions. The growing dependence of start-ups on data-driven business models increases the likelihood of over-collection, profiling, and opaque data-processing activities. Koops et al. (2017) argue that privacy functions across multiple dimensions informational, decisional, and accessibility which means that failures in governance often cascade across multiple harm categories simultaneously. The evidence from this research confirms that start-up platforms frequently overlook these dimensions, resulting in structural vulnerabilities that place consumers at a systemic disadvantage. Key privacy risks stem from the imbalance of power in data flows, where platforms exercise extensive control over data extraction and analysis, while consumers are left with limited knowledge or ability to negotiate consent. The phenomenon aligns with Tufekci's (2018) analysis of computational power asymmetry, which explains how digital entities leverage big data and opaque algorithms to influence user behaviors without offering meaningful control mechanisms. In this study, consumers reported having little awareness of how start-ups repurposed their data beyond the immediate transaction. The weak enforcement of consent requirements shows that the legal principle of informed consent is ineffective when platforms deliberately employ design structures that obscure data practices.

Moreover, the inadequate handling of personal data by start-up platforms reveals a more fundamental issue: the failure to recognize privacy as an essential consumer right rather than a legal formality. Solove (2015) emphasizes that privacy harms often emerge not from overt breaches, but from structured environments that expose individuals to risks through aggregation, data persistence, and secondary use. The findings support this framework, showing that start-up platforms routinely accumulate data beyond what is necessary for transactions, increasing exposure to future misuse, leaks, or unauthorized access. Weak internal monitoring and lack of independent audits further exacerbate these risks. The study also finds strong evidence that the start-up ecosystem mirrors patterns described in Zuboff's (2019) "surveillance capitalism," where consumer data becomes commodified through mechanisms that remain invisible to users. Interviews with cybersecurity experts highlight that data protection policies adopted by start-ups tend to follow minimal compliance strategies, serving more as legal shields than substantive safeguards. This arrangement benefits platforms by enabling data monetization while externalizing the risks onto consumers. The regulatory framework, though present, lacks active enforcement, allowing start-ups to accumulate data with limited accountability or transparency. Finally, the results reveal that weak data protection practices undermine the legal promise of consumer control over personal data. van Ooijen and Vrabec (2019) argue that even strong data protection regulations fail to restore control unless supported by operational mechanisms that enable users to access, correct, and restrict data processing. This study shows that such mechanisms are underdeveloped or absent in many start-up platforms. As a result, consumers remain highly exposed to privacy harms with minimal recourse. The implications are profound: without significant improvements in enforcement, governance, and platform accountability, the digital ecosystem risks evolving into a space where consumer rights exist nominally but remain practically inaccessible.

4.2.3. Structural Challenges in Digital Dispute Resolution and Asymmetrical Bargaining Power

The findings of this study show that dispute resolution in digital start-up ecosystems is hindered by structural barriers that reflect the asymmetrical bargaining power between consumers and platforms. Despite legal guarantees for fair and accessible redress, platforms often design dispute mechanisms that are difficult to navigate, rely heavily on automated systems, and lack transparency. Mantelero (2022) emphasizes that fairness and accountability in digital environments require proactive governance, yet the evidence here demonstrates that platforms adopt minimalist approaches that prioritize efficiency over consumer needs. This mismatch weakens procedural justice and undermines the legal framework's intention to provide meaningful remedies for consumers engaged in electronic transactions. The asymmetry of information further amplifies difficulties in dispute resolution. Platforms control the flow of data, determine access to communication channels, and set the terms of engagement, leaving consumers with little leverage when disputes arise. Mittelstadt, B. (2016) explain that digital businesses frequently exploit this informational imbalance to maintain strategic control while limiting their exposure to legal claims. The study's participants reported that they often lacked clarity on what evidence was required, how long the process would take, or whether their complaints would be assessed impartially. As a result, many consumers abandoned the dispute process entirely, indicating a systemic breakdown in the promise of accessible digital justice.

Algorithmic mediation also contributes to structural weaknesses in dispute resolution. The use of automated decision-making systems in initial complaint filtering means many disputes are responded to without human evaluation. Wachter et al. (2017) argue that such algorithmic opacity makes it difficult for individuals to understand how decisions are made and to contest unfair outcomes. In this study, consumers frequently received generic automated responses that neither addressed the substance of their complaints nor provided avenues for escalation. This reliance on automation not only delays meaningful resolution but also reinforces the imbalance between platforms—who control the technological infrastructure—and users who depend on it. Design practices adopted by platforms further disadvantage consumers during dispute processes. Ranchordás (2020) notes that "nudge-based" interface designs can subtly direct user behavior, often in ways that limit access to rights or procedural pathways. Evidence from interviews indicates that key dispute features—such as complaint forms or refund request buttons—were often placed in concealed menus or required multiple steps to reach, creating friction that discourages consumers from pursuing claims. These design choices reflect an intentional prioritization of platform protection over consumer empowerment, contradicting legal principles that emphasize transparency and fairness in business-to-consumer transactions. Beyond procedural barriers, the study's findings suggest that dispute resolution failures contribute to deeper harms that extend beyond the transaction itself. Calo (2016) argues that digital harms often arise from systemic vulnerabilities that expose individuals to repeated risks. When dispute mechanisms fail, consumers not only endure financial loss but also experience diminished trust in digital markets and increased vulnerability to future exploitation. The persistence of unresolved disputes indicates that platforms have little incentive to reform their systems without regulatory intervention. Thus, the asymmetrical bargaining power embedded within platform architecture results in a dispute environment where consumer rights exist formally but remain largely inaccessible in practice.

4.2.4. Ambiguous Contractual Clauses and the Erosion of Consumer Rights in Electronic Transactions

The findings of this study indicate that ambiguous contractual clauses in platform Terms of Service (TOS) play a central role in eroding consumer rights within digital transactions. Although consumer protection law mandates that contractual terms must be clear, fair, and not misleading, the TOS of many start-up platforms employ vague, technical, and overly broad language that obscures the scope of platform liability. This echoes Mantelero (2022), who argues that fairness and accountability cannot be achieved when contractual documents are drafted in a way that conceals the operational responsibilities of digital intermediaries. The ambiguity embedded in these clauses enables platforms to evade legal obligations while maintaining the façade of compliance. A recurring theme in the findings is the strategic use of linguistic complexity to shift responsibility from the platform to third-party actors.

The findings also highlight the opacity surrounding algorithmic decision-making systems that determine ranking, visibility, and access within platforms. Wachter et al. (2017) emphasize that the absence of explanation for automated decisions severely limits the ability of consumers to contest unfair outcomes or understand how contractual terms are applied in practice. Interview participants reported instances in which refund eligibility or complaint prioritization appeared arbitrary, yet the TOS provided no clarity about how such determinations were made. This algorithmic opacity reinforces the imbalance of power between platform operators and consumers and weakens the legal doctrine of good faith. Design elements in digital interfaces further aggravate the problem. Ranchordás (2020) argues that digital platforms often deploy interface-based nudges that subtly influence user decisions while disguising the legal implications of consent. This was evident in this study, where consumers described being nudged to accept TOS

through pre-ticked boxes, compressed summaries, or pop-up designs that discouraged deeper reading. These digital dark patterns not only facilitate uninformed consent but also amplify the impact of ambiguous clauses by ensuring that consumers agree to terms they do not fully understand. Such practices directly challenge the legal requirement for clear, accessible, and honest business communication.

Finally, the cumulative effect of ambiguous TOS is reflected in the structural vulnerability of consumers to digital harms. Calo (2016) argues that privacy and digital harms often emerge not from single contractual failures but from systemic arrangements designed to externalize risks onto users. The findings of this study align closely with this framework: ambiguous liability clauses, combined with opaque algorithmic practices and nudging design strategies, create an ecosystem in which consumers bear the burden of transactional risks while platforms enjoy legal insulation. This erosion of substantive consumer rights underscores the urgent need for regulatory intervention to standardize TOS language, restrict abusive clauses, and strengthen oversight mechanisms that ensure consumer protection in digital environments.

5. Conclusion

The results of this study demonstrate that the legal responsibilities of start-up platforms in electronic transactions remain misaligned with the expectations established by Indonesia's consumer protection and electronic information laws. Although the regulatory framework provides a strong foundation for fairness, transparency, and accountability, the practical implementation within digital platforms often fails to reflect these normative principles. This misalignment results in limited consumer safeguards and exposes users to various transactional and privacy-related risks. The study further concludes that the transparency gap in platform policies represents a fundamental weakness in current digital business practices. Terms of Service and privacy notices continue to be drafted using ambiguous, technical, and inaccessible language, preventing consumers from making informed decisions. These patterns reveal a systematic tension between legal obligations and operational strategies aimed at minimizing liability rather than enabling consumer empowerment. Weak data protection governance is identified as a consistent structural problem across start-up ecosystems. Despite the existence of regulatory standards requiring secure data handling, informed consent, and breach notification, platforms often adopt minimal compliance approaches that prioritize commercial data extraction. As a result, consumers face heightened risks associated with personal data misuse, unauthorized access, and privacy harms that remain largely unreported or inadequately addressed.

Dispute resolution mechanisms implemented by start-up platforms also exhibit significant limitations. While consumers are legally entitled to redress, the mechanisms provided by platforms are typically slow, non-transparent, and heavily automated. These constraints undermine the principles of procedural justice and leave many disputes unresolved, thereby reducing consumer trust in the digital marketplace. The study additionally finds that ambiguous contractual clauses play a central role in facilitating platform liability avoidance. Clauses that shift responsibility to sellers, logistics providers, or payment intermediaries undermine the substantive protections intended by law. The widespread use of such contractual strategies creates a digital environment in which consumers bear disproportionate risks, even in transactions where platforms maintain operational control. From an institutional perspective, the persistence of these challenges indicates that regulatory oversight has not kept pace with rapid technological change. Fragmented enforcement mechanisms and limited regulatory capacity allow digital platforms to operate with significant discretion, weakening the deterrent effect of existing laws. Without adaptive regulation and stronger institutional frameworks, platform non-compliance is likely to continue. Overall, this research concludes that ensuring consumer protection in digital transactions requires not only stronger regulatory enforcement but also substantive reforms in platform governance, contractual transparency, and data protection practices. A more coherent and adaptive approach to digital regulation is essential to strengthen consumer rights, enhance accountability, and create a safer and fairer digital marketplace.

References

Armstrong, T. (2022). Platform responsibility and consumer safety in digital markets. *Journal of Consumer Policy, 45*(3), 487–509. https://doi.org/10.1007/s10603-021-09502-6

Anggara, G. (2023). Digital platform regulation and the challenges of consumer protection in Indonesia. *Journal of Consumer Policy, 46*(2), 355–372. https://doi.org/10.1007/s10603-022-09518-2

Arianto, N. (2021). Digital business transformation: Challenges and opportunities. *Journal of Asian Finance, Economics and Business, 8*(5), 593–602. https://doi.org/10.13106/jafeb.2021.vol8.no5.0593

Baker, J., & Kesan, J. P. (2020). Electronic signatures and the future of digital contracting. *Journal of Law &Technology, 35*(2), 145–178. https://doi.org/10.2139/ssrn.3512451

Ben-Shahar, O., & Porat, A. (2022). Personalization and consumer law. *University of Chicago Law Review, 89*(4), 1321–1374. https://doi.org/10.2139/ssrn.4042224

Burgess, M., & Power, M. (2019). Digital evidence and the challenges of authentication in online transactions. *Digital Policy, Regulation and Governance, 21*(3), 229–243. https://doi.org/10.1108/DPRG-12-2018-0069

Busch, C. (2021). Transparency in the digital economy. *Journal of European Consumer and Market Law, 10*(1), 12–24. https://doi.org/10.2139/ssrn.3777614

Cafaggi, F., & Iamiceli, P. (2021). Contract governance in the platform economy. *Northwestern Journal of International Law & Business, 41*(3), 389–445. https://doi.org/10.2139/ssrn.3778804

Calo, R., & Rosenblat, A. (2017). The taking economy: Uber, information, and power. *Columbia Law Review, 117*(6), 1623–1690

Cortés, P. (2018). *The Law of Consumer Redress in an Evolving Digital Market*. Cambridge University Press. https://doi.org/10.1017/9781108667509

Gürses, S. (2019). Understanding the legal validity of electronic agreements. *International Review of Law, Computers & Technology, 33*(3), 233–251. https://doi.org/10.1080/13600869.2019.1622309

Harding, A. (2020). Regulating online consumer transactions: Legal challenges in digital markets. *Computer Law & Security Review, 36*, 105374. https://doi.org/10.1016/j.clsr.2020.105374

Helberger, N., Zuiderveen Borgesius, F., & Reyna, A. (2021). The perfect match? A closer look at the relationship between EU consumer law and data protection law. *Common Market Law Review, 58*(4), 1147–1180. https://doi.org/10.54648/COLA2021047

Ismail, R., & Abdullah, S. (2022). Legal protection in electronic commerce transactions: A regulatory perspective. *Information & Communications Technology Law, 31*(2), 163–181. https://doi.org/10.1080/13600834.2021.1936699

Kaspersky. (2022). *Consumer digital risk report: Asia-Pacific cyber threats*. (Official Report).

Kim, P., & Werbach, K. (2016). Trust, growth, and regulation in online platform markets. *University of Pennsylvania Journal of Business Law, 19*(1), 33–84.

Koops, B.-J. (2021). Attribution in autonomous digital transactions. *Computer Law & Security Review, 41*, 105561. https://doi.org/10.1016/j.clsr.2021.105561

Liu, X., & Serapio, M. (2022). Regulatory risks in fintech adoption across Southeast Asia. *Journal of Financial Regulation and Compliance, 30*(2), 185–200. https://doi.org/10.1108/JFRC-03-2021-0018

Luzak, J. (2021). Meaningful consent in the digital marketplace: Rethinking online contracts. *Journal of Consumer Policy, 44*(3), 345–364. https://doi.org/10.1007/s10603-020-09478-8

Marsoof, A. (2020). Consumer protection in online platforms: A comparative legal analysis. *International Journal of Law and Information Technology, 28*(3), 203–225. https://doi.org/10.1093/ijlit/EAAA011

Martin, K., & Murphy, P. (2017). The role of data privacy in consumer trust in digital transactions. *Journal of Business Ethics, 143*, 489–507. https://doi.org/10.1007/s10551-015-2769-z

Mathur, A., et al. (2019). Dark patterns at scale: Findings from a crawl of 11,000 shopping websites. *Proceedings of the ACM on Human-Computer Interaction, 3*(CSCW), 1–32. https://doi.org/10.1145/3359183

Mik, E. (2020). Smart contracts: Terminology, technical limitations, and real world complexity. *Law, Innovation and Technology, 12*(2), 269–300. https://doi.org/10.1080/17579961.2020.1815408

Mittelstadt, B. (2016). Auditing for transparency in algorithmic decision-making. *Communications of the ACM, 59*(10), 56–62. https://doi.org/10.1145/2973839

OECD. (2021). *Consumer protection in e-commerce: OECD recommendations*. Paris: OECD Publishing.

Priyono, A., Moin, A., & Putri, V. (2020). Identifying digital transformation paths in start-ups. *Journal of Open Innovation: Technology, Market, and Complexity, 6*(4), 125. https://doi.org/10.3390/joitmc6040125

Riyanto, S., & Nugroho, P. (2021). Legal compliance and operational risks in Indonesian start-ups. *International Journal of Management Studies, 28*(1), 45–59. https://doi.org/10.32890/ijms.28.1.2021.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity, 2*(2), 121–135. https://doi.org/10.1093/cybsec/tyw001

Safiullin, N., et al. (2021). Start-up governance and legal risk factors in digital markets. *Entrepreneurship and Sustainability Issues, 9*(1), 101–115. https://doi.org/10.9770/jesi.2021.9.1(7)

Susanti, D. (2022). Challenges of consumer protection in Indonesian digital markets. *Journal of Consumer Policy, 45*, 295–314. https://doi.org/10.1007/s10603-021-09504-4

Tambo, E., & Akrong, R. (2021). Cross-border e-commerce and consumer protection gaps in emerging markets. *Electronic Commerce Research, 21*, 345–367. https://doi.org/10.1007/s10660-019-09400-x

Teubner, G. (2020). Digital jurisdiction in a transnational world. *Global Constitutionalism, 9*(2), 289–313. https://doi.org/10.1017/S2045381719000375

Thaler, R. H., & Sunstein, C. R. (2017). *Nudge: Improving decisions about health, wealth, and happiness* (Updated ed.). Yale University PRESS.

Zhang, L., & Wang, Y. (2023). Cross-border e-commerce and consumer risk in Southeast Asia. *Electronic Commerce Research and Applications, 57*, 101242. https://doi.org/10.1016/j.elerap.2023.101242