

LEGAL PROTECTION OF CONSUMERS IN ONLINE TRANSACTIONS: A CASE STUDY OF ONLINE FRAUD IN INDONESIA

Erfan Mukhlas Ali, Febrian Dirgantara, Didit Darmawan

Universitas Sunan Giri, Surabaya

correspondence: dr.febriandirgantara@gmail.com

Abstract - The rapid development of information technology has transformed consumer behavior, driving significant growth in online transactions in Indonesia. However, this progress is shadowed by the increasing prevalence of online fraud cases, highlighting the urgent need for robust legal consumer protection. This study examines the effectiveness of current legal frameworks, particularly the Consumer Protection Law (Law No. 8 of 1999) and the Electronic Information and Transactions Law (Law No. 11 of 2008), in safeguarding consumers against online fraud. Despite these regulations, significant challenges persist, including weak enforcement mechanisms, limited digital literacy, and insufficient regulation of platform accountability. Additionally, gaps in evidence validation and ambiguities in existing laws exacerbate consumer vulnerability. Using a normative-empirical approach, this research analyzes relevant legislation and real-world fraud cases to identify weaknesses and propose enhancements. The findings emphasize the necessity of revising and harmonizing existing regulations, strengthening institutional capacities, and fostering collaboration among stakeholders to build a secure digital ecosystem. The study concludes that a comprehensive, adaptive, and integrative legal framework is imperative to bolster consumer trust and sustain the growth of Indonesia's digital economy.

Keywords: consumer protection, online fraud, legal framework, e-commerce, digital transactions, Indonesia, regulatory challenges.

INTRODUCTION

The consumption patterns of society in the digital era have undergone profound transformation as a result of the increasingly widespread penetration of information technology. Today, communities are progressively driven towards digitalization in every economic activity, especially regarding shopping and transactions. The development of information technology has significantly altered public consumption behavior. In Indonesia, online transactions have experienced exponential growth alongside increasing internet accessibility and the evolution of e-commerce platforms (Wahyudi et al., 2021). However, this phenomenon has also given rise to new challenges in the form of a surge in online fraud cases (Amin et al., 2023). Fraud in online transactions frequently inflicts both material and immaterial losses on consumers, thereby creating an urgent need for adequate legal protection.

Consumer resilience within the digital market is critically dependent upon the ability to access and effectively utilize information regarding digital products and services (Fajar et al., 2024). Unfortunately, the lack of transparency from business actors often undermines the bargaining position of consumers, rendering their rights vulnerable. Consumers are frequently at a disadvantage due to the lack of access to accurate information concerning goods or services being offered, despite Article 4 of Law No. 8 of 1999 on Consumer Protection guaranteeing the right to clear, accurate, and honest information. In practice, information provided on digital platforms is often inaccurate or misleading, thereby facilitating fraud and harming consumers. On the other hand, technological innovations such as e-wallets, peer-to-peer lending, and marketplaces have provided considerable transactional convenience (Oriento et al., 2021; Sahid et al., 2023; Irfan & Negara, 2023), but have also introduced new risks, particularly concerning money laundering activities and the misuse of personal data (Rusianto et al., 2023; Baraja et al., 2023; Fikri et al., 2023). In this context, the protection of privacy rights as an integral part of human rights has become increasingly crucial (Issalillah & Hardyansah, 2024), demanding optimal supervision and implementation of data protection laws to safeguard all parties from digital losses (Baraja et al., 2023).

Legal protection in the digital era now extends to consumers, business actors, platform workers, and even online community groups such as social gatherings (arisan) and ride-hailing services (Wahyudi et al., 2023; Negara & Darmawan, 2023). Regulations concerning consumer protection in e-commerce systems, return mechanisms in cash-on-delivery (COD) transactions, and consumer protection in digital lending services have laid a tangible foundation for safeguarding society against potential digital losses (Anugroh et al., 2023; Irfan & Negara, 2023; Faridi et al., 2023). Harmonizing interests through active collaboration among the government, business actors, and the public is crucial in fostering a digital ecosystem that is secure, equitable, and adaptive to technological advancement. Responsively implemented legal protection thus becomes a fundamental pillar in realizing justice and growing public trust in digital goods and services in Indonesia (Baraja et al., 2023; Issalillah & Hardyansah, 2024).

Regulatory challenges in the digital realm arise not only in implementation but also in the availability of supervisory systems that are adaptive to technological change. Minimal oversight can create gaps that enable the proliferation of fraudulent practices in cyberspace. Cases of online fraud reveal a significant weakness in the supervisory system over digital platforms. Despite existing regulations, such as the Ministry of Trade Regulation No. 50 of 2020 concerning Licensing, Supervision, and Guidance for Business Actors in Electronic Trading (PMSE), oversight of online transactional activities remains insufficiently effective, creating scope for unscrupulous business actors to engage in conduct detrimental to consumers.

An effective legal system should not only protect but also facilitate consumers in obtaining justice swiftly and efficiently. Procedural complexity in legal processes poses a real risk of discouraging victims from reporting instances of fraud, perpetuating the recurrence of similar cases. The principal challenge to consumer protection in digital transactions is the weakness in law enforcement mechanisms in handling online fraud cases. Many victims are reluctant to report fraud out of perception that legal proceedings are excessively complex, prolonged, and frequently fail to guarantee adequate resolution. Saragih et al. (2023) affirm that despite the existence of regulations governing online transactions, their practical implementation remains far from ideal. Victims commonly feel deprived of justice due to the lack of effective legal support.

Law enforcement is often hampered by the insufficient availability of valid digital evidence. Perdana (2021) explains that evidence management in online fraud cases presents a major challenge in the absence of systems that assure the validity of transactions or business actor identities. This considerably impedes legal proceedings, especially within e-commerce, which often involves a multiplicity of parties.

The lack of juridical provisions supporting consumer protection in online transactions has further exacerbated the situation. According to Saragih et al. (2023), this deficiency creates legal loopholes that hinder consumers from obtaining proper protection. This circumstance underscores the urgent need for regulatory reforms, including the incorporation of more robust digital evidence, expedited judicial processes, and enhanced mechanisms to safeguard consumers in the digital era. Absent such measures, consumer trust in online transactions will continue to erode, posing a significant barrier to the growth of Indonesia's digital economy.

Inadequate consumer awareness of their rights within online transactions constitutes a fundamental issue in contemporary consumer protection. This lack of understanding results in many victims of fraud being either unwilling or unaware of the available complaint mechanisms and legal remedies. In fact, Article 62 of Law No. 8 of 1999 on Consumer Protection expressly stipulates criminal sanctions for business actors violating consumer protection provisions, including acts of fraud or the dissemination of false information. Nevertheless, without sufficient knowledge regarding their rights and applicable legal procedures, consumers often choose to passively bear their losses, thereby fostering a culture of permissiveness toward digital violations.

Furthermore, the limited dissemination and socialization of consumer protection laws by both government officials and business actors aggravates this situation. Consumers who are unaware of the existence or substance of Article 62 tend not to report fraud cases to relevant authorities, sometimes perceiving the legal process as too complicated, costly, or being skeptical of its effectiveness. Consequently, violators are not subjected to proportionate sanctions, failing to create a deterrent effect. Low rates of complaints and legal action in cases of online fraud reflect the relative weakness of consumer protection instruments in Indonesia and highlight the need for enhanced educational strategies and institutional strengthening to secure optimal legal remedies for digital consumers.

Digital platforms serving as intermediaries in transactions hold a strategic role in preventing and addressing fraud. However, the legal responsibilities of such platforms are not yet explicitly regulated within Indonesian law, resulting in legal gaps frequently exploited by these entities to evade accountability when consumers incur losses due to fraud. Sidobalok (2014) emphasizes that the lack of explicit regulation on the liability of digital platforms substantially undermines consumer protection within the e-commerce ecosystem.

At the international level, several jurisdictions have adopted more advanced legislation to protect consumers in online transactions. Kirillova et al. (2016) demonstrate that adaptive regulation to technological developments—such as digital oversight mechanisms and statutory obligations imposed on platforms—has proven effective in increasing consumer trust. Indonesia could draw from these practices to develop a legal framework better suited to the challenges posed by the digital age.

The phenomenon of online fraud not only harms consumers but also negatively impacts Indonesia's digital economic growth. Erin Ann (2005) asserts that consumer trust in e-commerce platforms is a critical factor supporting the expansion of the digital sector. Therefore, failure to strengthen consumer protection regulations risks hampering digital economic development due to declining consumer confidence.

Makarim (2008) contends that the rapid advancement of technology necessitates more flexible and dynamic regulation. Indonesia's delay in adapting its regulatory regime to technological change will only exacerbate existing legal gaps and reduce the credibility of digital platforms in the eyes of consumers.

Syawali and Imaniyati (2000), in their work on Consumer Protection Law, highlight the need for regulations that not only focus on safeguarding consumers but also impose obligations on platforms to ensure transparency in digital

transactions. In the absence of such provisions, risks faced by consumers in online transactions will continue to escalate, presenting increasingly complex challenges in the digital economy sector.

Existing regulations remain sectoral and insufficiently integrated to address the complexities of online fraud. The absence of synergy among the Consumer Protection Law, the Electronic Information and Transactions Law, and other relevant regulations generates legal ambiguity to the detriment of consumers. Accordingly, an appropriate approach is needed to consolidate these various regulations within a unified and comprehensive legal framework.

Ultimately, these phenomena indicate the necessity for a more proactive approach from the government, business actors, and society at large to prevent online fraud. Collaboration between these three parties is essential to create a safe, transparent, and sustainable digital ecosystem for consumers.

Legal scholarship on consumer protection in Indonesia still largely focuses on conventional transactions and has yet to specifically address online transactions. Existing studies tend to emphasize oversight and the liability of business actors but have not extensively analyzed the role of regulation in addressing online fraud. This study aims to fill that gap by offering a more comprehensive perspective on the phenomenon.

This research is intended to analyze the effectiveness of legal protection for consumers in online transactions in Indonesia, particularly in cases of fraud. It also seeks to identify weaknesses and challenges in the implementation of current regulations and to provide recommendations for future regulatory development.

RESEARCH METHODS

The type of research employed in this study is normative-empirical legal research. A normative approach is utilized to analyze existing regulations, including Law No. 8 of 1999 on Consumer Protection and Law No. 11 of 2008 on Electronic Information and Transactions (ITE), as well as other relevant sectoral regulations. The empirical approach is applied to examine the practical realities and actual cases of online fraud in Indonesia, encompassing the responses of consumers, business actors, and regulators.

The data sources used comprise secondary data, including literature reviews of legal documents, academic journals, and case reports related to online fraud. Data collection is conducted through the techniques of observation and document study.

The data obtained from various sources are compared and analyzed to ensure consistency and accuracy. The validity of the research is further reinforced by involving regulators with competencies in consumer protection and online transactions.

The data analysis technique employed is descriptive-analytical. Descriptive analysis is used to illustrate the phenomenon of online fraud and the existing legal framework. Meanwhile, normative analysis is applied to assess the alignment of regulations with practices in the field. This analysis further aims to identify weaknesses in law enforcement and the potential for regulatory improvement.

RESULTS AND DISCUSSIONS

The Effectiveness of Legal Protection for Consumers in Cases of Online Fraud in Indonesia

Consumer protection in online transactions has become a critical issue amidst the rapid development of the digital economy. The complexity and dynamism of electronic transactions demand regulatory frameworks that are more adaptive and responsive to emerging challenges. Legal protection for consumers in online transactions is regulated through several statutes, notably Law No. 8 of 1999 on Consumer Protection (the Consumer Protection Act/UUPK) and Law No. 11 of 2008 on Electronic Information and Transactions (the ITE Law). However, the actual implementation of these regulations often falls short of expectations. One of the principal reasons is the inability of existing regulations to anticipate the complexities of online transactions involving multiple actors, ranging from digital platforms to providers of goods and services.

Despite the existence of statutory provisions governing consumer protection in online transactions under the UUPK and the ITE Law, their practical application frequently encounters significant obstacles, as current regulations are insufficient to address the intricacies and evolving nature of digital commerce. Contemporary online transactions entail a range of stakeholders with interdependent roles and responsibilities, such as marketplace platforms, sellers, courier services, and digital payment providers. This reality complicates the determination of liable parties in the event of disputes or consumer losses, especially when business actors operate outside Indonesia's jurisdiction or leverage cross-border business models. Furthermore, prevailing regulations often fail to promptly respond to technological advancements and new digital business models, resulting in legal loopholes exploitable by unscrupulous actors. Accordingly, it is imperative to harmonize existing regulations, establish clearer implementation guidelines, and enhance synergy between the government, business actors, and digital platforms so that consumer protection remains effective and adaptive to the rapidly developing landscape of online commerce.

The core challenge for consumer protection stems from the lack of regulatory adaptation to the unique and rapidly changing characteristics of digital transactions. Various forms of online fraud frequently escape oversight and sanction due to the limited reach of existing legal provisions. The effectiveness of the Consumer Protection Act in addressing online fraud remains low, as the Act does not specifically regulate the nuances of digital transactions. Article 4 of the UUPK, which guarantees consumers' rights to clear, accurate, and honest information, is often inapplicable to instances of online fraud. Many online business actors disseminate misleading information about their products, including images that do not correspond with actual goods received by consumers.

In addition to the prevalence of misleading information, another major concern is the lack of oversight and verification mechanisms within the digital transaction ecosystem. Marketplace platforms or social media, which commonly act as intermediaries between business actors and consumers, often lack rigorous procedures for verifying the accuracy of published product information. Consequently, consumers find themselves in a vulnerable position, susceptible to deception, while unscrupulous business actors can easily switch identities or create new accounts after violating consumers' rights. This situation highlights a significant gap between the statutory guarantee of consumer rights under Article 4 of the UUPK and the practical realities of consumer protection in the highly dynamic digital space.

Moreover, the resolution of consumer disputes arising from online fraud remains problematic, including difficulties in identifying perpetrators and collecting legally valid electronic evidence. Existing regulations have yet to comprehensively regulate consumer protection procedures in digital transactions, particularly regarding the liability of platforms as supervisory entities. Therefore, a regulatory renewal is needed, introducing special provisions governing online transactions, including the reinforcement of business actor verification systems, improvements in product information transparency, and the imposition of stringent sanctions against business actors proven to provide false or misleading information to consumers.

This phenomenon illustrates the low level of compliance among certain online business actors with the principles of transparency and honesty in product information disclosure. Consumers are often attracted by enticing promotions or visually appealing product displays, but the goods they receive frequently fall short of expectations. This not only causes economic loss but also erodes public trust in digital transactions. Furthermore, such misleading conduct may be categorized as a violation of consumer rights, contravening provisions of the Consumer Protection Act. For consumer protection to become more effective, stricter regulatory oversight, utilization of verification technologies on digital platforms, and comprehensive public education—encouraging consumers to be more critical and prudent in their transactions—are essential. The active involvement of all stakeholders is crucial to fostering a healthy, competitive digital trading ecosystem in Indonesia that prioritizes integrity and the safeguarding of consumer rights.

In the digital era, legal protection also necessitates adaptation to the rapid advancement of information technology. The urgent demand to establish a more responsive legal ecosystem to meet digital challenges is becoming increasingly prominent. The Electronic Information and Transactions Law (ITE Law), which is intended to support consumer protection within the digital realm, also faces numerous challenges. Article 28(1) of the ITE Law prohibits the dissemination of misleading information or acts detrimental to consumers. However, enforcement often encounters obstacles due to the lack of valid digital evidence, such as records of transactions or electronic communications. In addition, law enforcement officers frequently lack the technical capacity to handle digital evidence appropriately.

Difficulties in proving violations of Article 28(1) of the ITE Law reveal major weaknesses in the enforcement of the law against cases involving the dissemination of misleading or harmful information to consumers in digital environments. The reliance on digital evidence, including conversation histories, transaction records, and other electronic data, underscores the necessity of a stringent and standardized system for the collection and preservation of such evidence. Unfortunately, many reported cases are not supported by authentic or relevant digital evidence, complicating verification processes at both the investigation and trial stages. Moreover, limited competency among law enforcement personnel in tracing, verifying, and analyzing digital data leads to further delays and, in many instances, cases that cannot proceed. This highlights the critical need to enhance the technical capacity of law enforcement through intensive training and the procurement of advanced digital forensic tools, as well as to educate both the public and business actors regarding the importance of documenting digital evidence in every transaction. These measures are necessary to ensure the effectiveness of the ITE Law in maximizing consumer protection.

The role of digital platforms as central parties in online transactions is pivotal in determining the level of security and consumer protection. However, the current position of platforms as mere intermediaries results in less than optimal consumer protection. As facilitators of online transactions, digital platforms bear significant responsibilities in safeguarding consumers, especially as e-commerce continues to increase. Yet, the legal liability of these platforms remains largely unregulated. Zaini (2024) notes that in numerous online fraud cases, e-commerce platforms often act only as intermediaries and do not accept liability for losses incurred by consumers, consequently placing consumers in a vulnerable position without adequate legal protection.

The lack of explicit regulation further weakens the consumer position, particularly when tracking and resolving disputes is highly challenging. The obligations of platforms to ensure data and transaction security must be emphasized in more comprehensive and detailed regulations. Cases of online fraud recurrently illustrate consumers' difficulties in

obtaining fair redress due to the absence of mechanisms governing the platform's responsibilities regarding the transactions they facilitate. Yuniarti (2019) also emphasizes that platforms bear an obligation to protect consumers' personal data, though practical implementation remains weak. This erodes consumer trust in digital platform services, especially when legal issues related to data security and fraud are left unresolved.

Another principal challenge is the existence of legal loopholes stemming from the absence of specific regulation on platform liability. Consumers become principal victims as regulations fail to guarantee effective protection in cyberspace. The absence of explicit rules delineating platform liability for consumer protection creates legal gaps to the detriment of consumers. In the absence of clear regulation, platforms tend to eschew responsibility, leaving consumers unprotected in the event of losses. This underscores the urgency of reinforcing regulation and oversight of digital platforms to create a safe and equitable online transactional ecosystem.

Efforts at oversight and law enforcement within the digital trade sector are further hampered by both policy-level and operational weaknesses. The role of supervisory institutions remains suboptimal, adding complexity to the overall framework of consumer protection. Oversight bodies such as the Ministry of Trade and the Financial Services Authority (OJK) have yet to optimize their preventive and remedial roles regarding online fraud. Although Minister of Trade Regulation No. 50 of 2020 provides a basic supervisory framework for electronic trading (PMSE), its practical implementation remains weak. Many online business operators are unregistered or lack appropriate business licenses, complicating the tracing of perpetrators in fraud cases.

The shortcomings in the implementation of Minister of Trade Regulation No. 50 of 2020 are reflected in the continued existence of online business operators operating without official authorization or registration within government oversight systems. This situation poses substantial challenges for authorities in enforcing consumer protection and eradicating detrimental trade practices such as fraud and product counterfeiting. In instances of fraud, it is difficult for consumers to claim accountability as the identities and the legal status of the business actors are often ambiguous or anonymous. Weak oversight also fosters the proliferation of illegal businesses that disregard ethical standards and legal requirements, thereby increasing risks for consumers. Strengthening business registration and monitoring systems must thus become a principal priority, implemented through stricter law enforcement, inter-agency data integration, and the advancement of digital literacy among both business operators and consumers. These efforts are essential to establish a healthy, transparent, and trustworthy electronic commerce ecosystem.

Consumer education issues further diminish the effectiveness of legal protection in the digital domain. It is widely recognized that many consumers lack knowledge about their rights and available complaint mechanisms, which allows unscrupulous business actors to commit fraud with relative impunity. Another factor influencing the effectiveness of legal protection is the general unawareness among consumers regarding their entitlements. Many do not know the procedures for filing complaints, or refrain from reporting fraud out of concern that legal proceedings will be overly complex and time-consuming. This creates a permissive culture in which business actors feel emboldened to engage in fraudulent practices.

The lack of synergy among various regulations also complicates the implementation of legal protection for online consumers. Fragmentary rule-making often leads to confusion among both law enforcement authorities and the public regarding dispute resolution pathways. Regulatory inconsistencies pose a major obstacle. The Consumer Protection Law (UUPK), the ITE Law, and other laws frequently lack coordination, resulting in legal ambiguities. For instance, regarding the liability of business actors for consumer losses, existing regulations do not clearly define the extent and boundaries of such responsibility.

Regulatory disharmony is indeed a serious impediment to digital consumer protection, especially when there are overlaps or regulatory gaps among legal frameworks such as the UUPK, the ITE Law, and other sectoral regulations. This condition leads to confusion both for business actors and law enforcement officers in interpreting and applying rules related to liability for consumer losses. As a result, dispute resolution is often protracted, due to the absence of clear reference points regarding who bears liability, the extent of such liability, and appropriate compensation mechanisms. Such legal ambiguities can also be exploited by business actors to evade their obligations, thereby putting consumers at a disadvantage. Therefore, harmonization of regulations and the development of more specific and comprehensive guidelines are essential to ensure that digital consumer protection is not hindered by divergent legal interpretations and that genuine protection is realized in practice.

Studying international practices may serve as a significant reference for strengthening the framework of digital consumer protection in Indonesia. The adaptation of more advanced global regulations is required to ensure that Indonesian consumers are prepared to face the numerous challenges posed by modern e-commerce. From an international standpoint, numerous jurisdictions have developed specific regulations focusing on online transactions to provide enhanced consumer protection. Indonesia, with its rapidly growing e-commerce sector, must adopt a similar approach to ensure optimal protection for its consumers. Janitra et al. (2021) assert that regulations that are adaptive to technological advancements are crucial in maintaining consumer trust in digital systems, particularly in internet-based transactions.

Regulatory change and adaptation are essential so that the law can keep pace with dynamic and complex technological developments. Without responsive regulation, consumer trust in digital transactions will continue to erode,

potentially hindering digital economic growth. The inability of national regulations to keep pace with technological advancements has exacerbated the situation, creating legal gaps that undermine consumer trust in online transactions. Nasution (1995) emphasizes that, absent relevant regulatory updates, consumers remain vulnerable in the face of increasingly complex digital transactions.

The dispute resolution process in the digital environment requires mechanisms that are more efficient and accessible for all segments of society. Limitations of legal infrastructure are a primary factor hindering rapid and affordable consumer dispute resolution. Moreover, the absence of inexpensive and expeditious dispute settlement mechanisms is a significant impediment. Krisharyanto and Setyowati (2019) state that courts are frequently inefficient for handling online disputes due to lengthy proceedings and high costs. This is further compounded by the fact that many consumers lack access to appropriate legal services, as highlighted by Subekti (2000) in his work on Contract Law.

The efficacy of consumer protection is highly dependent on the effectiveness of mechanisms for addressing online fraud cases. The lack of efficient resolution systems enables business actors to evade liability and perpetuates consumer loss. Unresolved cases of online fraud negatively impact consumer confidence. Zaini (2024) notes that ineffective dispute resolution mechanisms frequently discourage consumers from reporting their cases, resulting in many business actors remaining unaccountable for consumer losses.

Personal data security issues constitute a primary concern in online transactions, given the high risk of data breaches and misuse. The absence of clear legal foundations amplifies the potential threats for consumers and undermines public trust in digital platforms. On the other hand, personal data protection also remains a pressing challenge in online transactions. Yuniarti (2019) observes that without a robust legal framework, consumer data is vulnerable to misuse. This further erodes consumer confidence in the security of digital transactions.

A balanced scheme of legal protection must ensure benefits not only for consumers but also for business actors, particularly small enterprises. Regulatory barriers and limited access to legal remedies may impede small businesses from growing within the digital ecosystem. In addition to consumer protection, Yuliana (2022) stresses that legal safeguards should also encompass small business operators, who are often hampered by regulatory complexity and limited access to legal resources. Such imbalances create additional challenges in ensuring a fair digital ecosystem.

Equitable and sustainable digital transformation requires collaboration and synergy among the government, the private sector, and civil society to reinforce comprehensive legal protection. The importance of adaptive regulation for safeguarding other digital rights has grown alongside the increasing complexity of the digital ecosystem. Jaman et al. (2021) recommend that efforts to reinforce consumer protection regulation must proceed in parallel with the protection of other digital rights, thereby creating an inclusive and sustainable digital environment. Without these efforts, the growth of Indonesia's digital economy risks being stunted by persistent low levels of public trust in online transactions.

Enhancement of the quality of legal protection must be realized through ongoing education, regulatory strengthening, and capacity building within legal institutions. Synergy among various stakeholders is expected to minimize online fraud cases and support national digital economic growth. Effective legal protection requires a comprehensive approach, including consumer education, regulatory reinforcement, and institutional capacity building within law enforcement agencies. Absent these measures, online fraud incidents will continue to rise, to the detriment of consumers and the overall digital economy in Indonesia.

Weaknesses and Challenges in the Implementation of Regulatory Frameworks Governing Online Fraud Cases in Indonesia

The rapid pace of digital transformation necessitates that all regulatory frameworks dynamically adapt to remain relevant and effective. A regulatory lag behind technological advancements inevitably results in the law's incapacity to provide optimal consumer protection. The first weakness in regulatory application lies in the lack of adaptation to technological evolutions. Most existing regulations—for instance, Law No. 8 of 1999 concerning Consumer Protection (UUPK)—were designed for conventional transactions and do not account for the complexities inherent in digital transactions. As a result, these regulations are difficult to implement regarding online fraud cases involving digital platforms or emerging technologies such as cryptocurrency.

Furthermore, the distinct characteristics between conventional and digital transactions create interpretative challenges for the application of the UUPK. Digital transactions frequently involve parties across jurisdictions, the use of anonymous identities, and payment instruments that are difficult to trace, such as crypto assets. These issues complicate national law enforcement and open loopholes for perpetrators to perpetrate transnational fraud. The absence of explicit legal norms regulating the supervision and enforcement of such practices leaves digital consumers vulnerable and inadequately protected.

Moreover, the complexities faced by law enforcement agencies in distinguishing legitimate digital transactions from fraudulent activities are compounded by low technological literacy and limited technical resources. Identifying perpetrators, collecting electronic evidence, and recovering consumer losses are often hindered by ambiguous standards of proof in the digital domain. Consequently, regulatory reforms are required to accommodate legal needs in the era of digital transformation, including expanding the scope of consumer protection, strengthening oversight mechanisms, and adapting to technological advances such as blockchain and cryptocurrency.

Supervision of digital business actors is a critical aspect in creating a healthy transactional ecosystem. Without effective oversight, fraudulent and deceptive practices proliferate. The second regulatory weakness is the inadequacy of oversight over online business operators. Although regulations on Electronic Systems and Transactions (PMSE) require digital businesses to register, many platforms and individuals continue to operate without official authorization. The government's inability to monitor all online commercial activities creates regulatory gaps that allow unscrupulous business actors to commit fraud.

The level of digital literacy among the public significantly influences the effectiveness of legal protection in the online sphere. A lack of awareness and education about digital risks further exposes consumers to harm. Another major challenge is the low rate of digital literacy within society, with many consumers unaware of how to ensure the security of online transactions or verify the legitimacy of sellers. This leaves them susceptible to fraud, especially in transactions conducted through social media platforms that are unregulated by PMSE.

Law enforcement in online transactions is profoundly influenced by the quality and procedural management of digital evidence. Ambiguity in the validation of digital evidence creates opportunities for perpetrators to evade responsibility. The enforcement of law in online fraud cases faces significant challenges, especially in terms of collecting and verifying digital evidence. Evidence in the form of screenshots or electronic transaction records, although frequently relied upon in dispute resolution, is easily manipulated and often contested in court. Isnaeni et al. (2023) indicate that weaknesses in the standard procedures for digital evidence collection often result in cases failing to achieve adequate legal resolution.

Such procedural weaknesses in the collection of digital evidence—as highlighted by Isnaeni et al. (2023)—constitute a significant barrier to legal enforcement in the digital age. Many legal cases, particularly those involving online transactions, digital fraud, or data breaches, do not achieve just outcomes because the digital evidence submitted fails to meet technical and legal standards. Errors or lack of diligence at the stages of collection, storage, and authenticity testing often raise questions about the validity of such evidence in court. In addition, insufficient expertise among law enforcement personnel and related authorities exacerbates the situation, increasing the potential for evidence manipulation or loss. To address these issues, it is essential to establish clear standard operating procedures as well as specialized training for law enforcement officials in handling digital evidence, ensuring that every case is processed fairly and transparently and that legal violations in the digital sphere carry a deterrent effect.

The obligation of digital platforms to protect consumers remains limited due to the lack of binding regulation. In the absence of regulatory compulsion, platforms often evade responsibility when issues arise. Furthermore, the liability of digital platforms as intermediaries in online transactions remains an unregulated area. Zaini (2024) observes that platforms often disclaim liability in the event of fraud, claiming to act solely as facilitators. Without clear and stringent regulations compelling platforms to offer enhanced consumer protections, such situations continually disadvantage consumers.

The practice of digital platforms disclaiming responsibility by asserting their role as mere facilitators highlights the weakness of legal protection for consumers in online transactions. In fraud cases, consumers are placed in a precarious position, struggling to obtain accountability or equitable remedies from platforms. The absence of explicit regulation provides little incentive for platforms to enhance protection mechanisms, such as seller verification, fraud detection systems, and effective complaint handling and loss recovery systems. Consequently, consumers tend to bear the risks and losses resulting from third-party conduct on the platform. Thus, clear and robust regulation is imperative so that digital platforms are required to contribute to the creation of a safe, transparent, and consumer-oriented transactional ecosystem. Such regulatory measures are not only expected to increase consumer trust, but also to stimulate fair and sustainable growth within the digital economy.

A proactive legal strategy is imperative amidst the rapid advancement of digital technology innovation. Reactive regulatory approaches have resulted in legal oversight and protection lagging behind the evolving practices of online commerce. Such reactive legal responses further aggravate the situation. As Wahyudi et al. (2021) observe, the majority of regulations are formulated only in response to emerging issues, thereby perpetually trailing behind technological innovation and societal practices. This approach not only renders regulation less effective but also creates gaps in legal protection for consumers.

From the consumer perspective, barriers to access in dispute resolution mechanisms hamper the realization of justice, particularly in cases involving nominal transaction values. It is essential for regulations to promote alternative mechanisms that are more expedient and efficient to suit the needs of a digital society. Access to swift and affordable dispute resolution remains a primary obstacle for consumers. Zaini (2024) highlights that traditional court litigation is often perceived as inefficient for disputes involving minor financial losses. Alternatives such as online arbitration or digital mediation, as recommended by Yuniarti (2019), offer promising solutions to enhance the efficiency and accessibility of the dispute resolution process.

Personal data protection is an inseparable component of the security of modern digital transactions. Without robust endeavours to protect such data, consumer trust in platforms will continue to decline. Beyond challenges in regulatory frameworks and dispute resolution mechanisms, personal data protection stands as a pivotal issue. Issalillah

and Hardyansah (2024) explain that consumer confidence in digital platforms is frequently undermined by inadequate personal data safeguards. Data security, therefore, is a fundamental element that must be strengthened to foster greater consumer trust in online transactions.

The lack of adequate personal data protection has become a principal factor in diminishing consumer trust in digital platforms. Consumers are increasingly aware of the risks associated with data breaches and potential misuse, which can adversely affect both their privacy and financial security. Within a fast-paced and dynamic online transaction ecosystem, the protection of personal data must become a paramount concern for all digital platforms to ensure a secure experience for their users. Strengthening these efforts may include implementing encryption technologies, multi-layer verification, and privacy policies that are both transparent and easily comprehensible. Regular education initiatives aimed at consumers, to increase their awareness regarding data protection measures, are also essential in fostering prudent data-sharing practices. With robust data protection in place, consumer trust in digital platforms will grow, thereby promoting the sustainable and healthy development of the digital economy.

Enhancing digital literacy should be a priority agenda for both regulatory authorities and industry stakeholders. Consumer education is not merely a form of individual protection but also serves as an investment in cultivating a healthy digital ecosystem. Insufficient digital literacy among consumers exacerbates the complexity of these issues. Platforms and regulators must collaborate to deliver educational programs that inform consumers of their rights in digital transactions. Such efforts are crucial so that consumers may assess fraud risks more critically and understand the available legal protection mechanisms.

Regulatory fragmentation and lack of integration result in inconsistent and confusing protection for both businesses and consumers. Therefore, the harmonization of regulations should be a primary concern to fortify the legal regime for online consumer protection. Sectoral and non-integrated regulations create obstacles to effective implementation. The absence of harmonization among the Consumer Protection Law, the Electronic Information and Transactions Law, and the Regulation on Electronic Systems and Transactions has resulted in legal overlaps and vacuums that disadvantage consumers. Additionally, this regulatory disharmony complicates the duties of law enforcement in determining the appropriate legal basis for addressing online fraud cases.

Human resource and infrastructure limitations within law enforcement agencies also impede efforts to address digital crime. Training for officials and investment in monitoring technology are critically required to enhance law enforcement capacity in the digital era. The scarcity of trained personnel capable of handling technologically complex cases, coupled with inadequate funding for supporting technologies, remains a major barrier to improving oversight and effective legal enforcement.

Addressing online fraud requires cross-sectoral and innovative solutions—regulatory, educational, and infrastructural. Collaboration among all stakeholders will reinforce a secure and conducive digital transaction ecosystem for national economic growth. In sum, the challenges in enforcing laws against online fraud in Indonesia demand innovative strategies to improve regulatory frameworks, strengthen dispute resolution mechanisms, and enhance consumer digital literacy. These measures are vital not only to protect consumers but also to promote a sustainable digital economy. Overcoming these weaknesses and challenges requires more strategic and comprehensive action. A flexible and adaptive regulatory approach, responsive to technological developments, should be prioritized to establish effective legal protection for consumers in online transactions.

Legal Aspects of Personal Data Protection in Mobile Applications

The protection of personal data has emerged as a central issue within contemporary legal discourse in the digital age. The significance of data protection has heightened alongside the rapid expansion of the mobile application ecosystem. Issues regarding personal data protection have become increasingly prominent in line with the massive adoption of mobile applications in Indonesia. Every digital transaction executed via mobile applications almost invariably entails the submission of sensitive data, such as identity information, geolocation, banking details, and online behavioral records. Existing regulations—primarily Article 26 of the Electronic Information and Transactions Law (ITE Law) and Minister of Communication and Informatics Regulation No. 20 of 2016—seek to govern the protection of personal data; however, in practice, many application developers have yet to comply with the standards mandated by law (Permata Rizki et al., 2022).

Regulatory oversight of mobile applications in Indonesia is still considered suboptimal. The absence of stringent sanctions allows business actors to operate beyond established legal boundaries. Weak supervision and a lack of effective penalties have resulted in numerous applications overtly requesting access to data beyond what is necessary for core service provision. Frequently, applications collect and process additional data without transparent disclosure regarding the purpose and duration of data retention. Such practices violate the principles of fairness and legal certainty for consumers as data subjects, who rightfully possess the entitlements to proportional treatment, including the right to provide consent and to withdraw such consent at any time (Efimtseva & Shadrin, 2020).

Cyberattacks and negligence on the part of application operators constitute distinct challenges for guaranteeing data security. Numerous data breach incidents attest to the inadequacy of data protection systems at the level of application producers. The potential for consumer data leaks represents a tangible threat within the mobile application ecosystem,

arising either from cyberattacks or lapses in the maintenance of secure systems by application providers. Incidents involving data theft or the sale of user data to third parties remain prevalent and can result in financial loss, reputational damage, or even extortion of consumers. However, the enforcement of data breach cases remains hampered by complex evidentiary requirements and frequent conflicts of cross-border jurisdiction (Nasrudin & Latumahina, 2022).

Low legal awareness within society further exacerbates the risk of data misuse by application providers. Public education regarding user rights and obligations remains limited amidst ongoing digitalization. Deficiencies in education and digital literacy amplify consumers' vulnerability to the misuse of personal data. A significant portion of users does not fully comprehend the implications of agreeing to privacy policies or End-User License Agreements (EULA) in the applications they use. This gap is often exploited by application providers, who draft one-sided agreements that minimize their legal liabilities and shift the entire burden of loss or data theft onto consumers (Azhari & Soetopo, 2022).

Legal certainty and consumer protection are heavily influenced by the existence of specific regulations. The absence of a principal legal framework has led to a legal vacuum concerning personal data protection in the mobile sector. From a substantive legal perspective, the lack of a dedicated statute governing data protection creates uncertainty regarding the rights and obligations of all parties. Although Indonesia has initiated deliberations on the Personal Data Protection Bill (PDP Bill), both its passage and effective enforcement remain in progress. Consequently, consumer protection remains contingent upon interpretation and implementation of overlapping sectoral regulations, which tend to be inconsistent and open to multiple interpretations.

This regulatory fragmentation undermines the efficacy of consumer protection in Indonesia, as overlapping and ambiguous sectoral regulations create considerable legal uncertainty. Such disharmony impedes the enforcement of consumer rights, as ambiguities and poor coordination among authorities often force consumers into protracted and complicated dispute resolution processes due solely to interpretive differences among institutions. To address these challenges, regulatory harmonization, the formulation of integrated consumer protection standards, and the strengthening of supervisory authorities are of paramount importance to ensure justice and legal certainty throughout the digital economic ecosystem.

The globalization of digital markets calls for the development of cross-border legal enforcement mechanisms. Many mobile applications are designed and operated by foreign legal entities beyond the reach of domestic law. This global dimension complicates regulatory governance, as numerous application providers are based overseas while their users reside in Indonesia. The enforcement of privacy and data protection violations is frequently hindered by jurisdictional barriers and the lack of mutual legal assistance mechanisms among countries. Consequently, foreign application providers often escape legal proceedings, leaving domestic consumers with limited avenues for redress (Qureshi et al., 2023).

Internal corporate policies within application providers do not always prioritize the protection of consumers' rights. Frequently, personal data is retained or managed without clear data deletion timelines. Legal analysis reveals a prevalent tendency among developers to retain consumer data without specifying retention periods. Indonesian regulation does, in fact, require the deletion of consumer data upon request, but practical implementation remains far from ideal. Failure to completely delete such data may result in ongoing exposure to misuse, even after consumers have ceased using the application's services (Guamán et al., 2023).

The obligation to erase consumer data upon request represents a critical measure in the protection of privacy and individual rights in the digital era. The lack of effective implementation, however, reveals gaps in Indonesia's regulatory enforcement and oversight mechanisms. Many digital service providers lack adequate internal procedures for accommodating data deletion requests or for transparently disclosing the storage and processing of consumer data. As a result, consumer data may persist within systems, be archived across multiple servers, or be transmitted to third parties, thereby maintaining the potential for further misuse—including identity theft, fraud, and unauthorized marketing. These conditions highlight the need for not only comprehensive regulations but also technical capacity-building, supervisory enhancements, and business actor education to ensure that data erasure rights are consistently enforced, thus guaranteeing consumer security and trust within Indonesia's digital landscape (Prastyanti et al., 2022).

The principle of strict liability must be actualized within the legal practice of data protection to prioritize consumer rights in cases of data breaches or misuse. Within the realm of liability, the adoption of strict liability should form the bedrock of legal protection for users of mobile applications. Producers ought to be held accountable for any loss or damage sustained by consumers as a result of negligence or failures in data protection systems, regardless of whether fault is established. The implementation of strict liability will incentivize providers to adopt proactive security standards and undertake regular audits (Azhari, 2021).

The application of strict liability demands that producers not only meet minimum compliance standards but also proactively safeguard the security of their products in the marketplace. In this way, producers can no longer invoke ignorance or third-party misconduct as defenses in the event of consumer harm resulting from their products. This approach will compel providers to engage in ongoing evaluations and conduct regular audits, proactively identify programming or system risks, and adopt new technological innovations to improve product quality and security. In addition, the implementation of strict liability will foster regulatory compliance and heighten industry awareness of the

importance of consumer protection. Ultimately, consumers will benefit from enhanced safeguards, while businesses will be incentivized to maintain their reputation and competitiveness by delivering safe and high-quality products (Chen et al., 2021).

Strengthening oversight mechanisms for digital applications is imperative. At the macro level, the establishment of an independent authority with comprehensive powers of supervision and law enforcement is necessary. Independent monitoring and auditing mechanisms for all mobile applications in circulation are also essential. Institutions such as the Ministry of Communication and Informatics or a national data authority must be mandated to undertake verification, certification, and continuous oversight, as well as provide accessible complaint channels for consumers who have suffered harm due to data breaches. These efforts will foster public trust and enhance the commitment of application producers to legal compliance (Tjin Tai, 2018).

A just and equitable digital transformation must be founded on the principles of personal data protection. All stakeholders are duty-bound to promote a progressive and inclusive digital legal culture. In conclusion, the protection of personal data within mobile applications must be recognised as a digital fundamental right, guaranteed by the state. Effective collaboration among regulatory authorities, application producers, supervisory institutions, and civil society is imperative to give rise to a safe and healthy digital ecosystem. The harmonization of Indonesia's legal framework with international standards, such as the General Data Protection Regulation (GDPR), should serve as a reference point in strengthening the system of legal protection for application consumers in Indonesia.

CONCLUSIONS

Legal protection for consumers involved in online transactions in Indonesia, particularly in cases of fraud, continues to encounter various obstacles. Law No. 8 of 1999 concerning Consumer Protection and Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law) provide the legal foundation, yet they have not been fully effective in addressing the complexities inherent in digital transactions. Numerous fraud cases remain unresolved due to weak law enforcement, limited capacity of relevant institutions, and low levels of digital literacy among consumers. The difficulty of verifying digital evidence and the absence of comprehensive regulations regarding the liability of digital platforms further exacerbate the situation.

Regulatory shortcomings, such as the lack of harmonization between the Consumer Protection Law, the ITE Law, and regulations on Electronic Commerce (PMSE), have created legal loopholes exploited by perpetrators of fraud. Suboptimal oversight of digital commerce activities often places consumers in a disadvantaged position. These challenges are compounded by consumers' limited awareness of their rights and the available avenues for lodging complaints.

Nevertheless, opportunities to enhance consumer protection remain open. Through regulatory reform, the improvement of digital literacy, and the strengthening of institutional law enforcement capacities, consumer protection can be significantly increased. An appropriate and collaborative approach among government, business actors, digital platforms, and the public is key to fostering a secure and trustworthy digital ecosystem.

Regulations such as the Consumer Protection Law, the ITE Law, and PMSE must be revised and harmonized to more effectively address cases of online fraud. Specific provisions concerning the liability of digital platforms to protect consumers should be implemented promptly to close existing legal gaps.

E-commerce platforms must be mandated to adopt robust consumer protection measures, including seller verification, escrow systems, and stringent supervision of transactions. Government oversight of compliance by these platforms must also be enhanced.

Enhanced collaboration among government authorities, business actors, digital platforms, and society is necessary to establish a safer digital ecosystem. Business actors and platforms can play an active role in consumer education and in ensuring transparent and fair commercial practices.

REFERENCES

- Alamin, S. R. L., D. Nurmalasari, D. Darmawan, & S. Arifin (2021). Comprehensive Relational Value Marketing Framework, *Journal of Social Science Studies*, 1(1), 299 – 304.
- Amin, M. N., A. Herisasono, Mujito, R. K. Khayru, & M. Zakki. (2023). Legal Protection of Consumers in Online Transactions for Counterfeit Halal Products on E-Commerce Platforms, *Journal of Social Science Studies*, 3(1), 53 – 58.
- Anugroh, Y. G., R. Hardyansah D. Darmawan, R. K. Khayru, & A. R Putra. (2023). Consumer Protection and Responsibilities of E-commerce Platforms in Ensuring the Smooth Process of Returning Goods in COD Transactions, *Journal of Social Science Studies* 3(2), 89 – 94.
- Azhari, A. (2021). Legal review of consumer law protection on personal data on digital platform. <https://doi.org/10.25041/IPLR.V2I1.2189>
- Azhari, T. M. A. R., & Soetopo, M. G. S. (2022). Protection of Personal Data in Transactions Using ECommerce in the Perspective of Indonesian Law (An Overview). *International Journal of Research and Innovation in Social Science*. <https://doi.org/10.47772/ijriss.2022.61222>
- Aziz, A., D. Darmawan, R. K. Khayru, A. S. Wibowo, & Mujito. (2023). Effectiveness of Personal Data Protection Regulation in Indonesia's Fintech Sector, *Journal of Social Science Studies*, 3(1), 23 – 28.
- Baraja, M. U., R. Saputra, P. Saktiawan, F. Dirgantara, S. Waskito. (2023). Implementation and Supervision of Personal Data Protection Law on Online Platforms, *Journal of Social Science Studies*, 3(1), 101 – 108.

- Chen, Y., Hua, X., & Maskus, K. E. (2021). International protection of consumer data. *Journal of International Economics*. <https://doi.org/10.1016/J.JINTECO.2021.103517>
- da Costa, S., D. Darmawan, & A. de Jesus Isaac. (2022). Self-Identity Formation and Social Perception of Individuals through Interaction on Social Media in a Digital World, *Journal of Social Science Studies*, 2(2), 273 – 278.
- Daud, E. Z., & Suyanto, H. (2024). The Legal Protection on Consumers of E-Commerce Transactions in Indonesia. *Law Development Journal*, 6(2), 266-278.
- Efimtseva, T., & Shadrin, S. (2020, May 27). Legal Regulation of Personal Data in the Digital Economy: Leading Problems and Prospects. <https://doi.org/10.2991/ASSEHR.K.200526.058>
- Erin Ann, O. H. (2005). Choice of Law for Internet Transactions: The Uneasy Case for Online Consumer Protection. *University of Pennsylvania Law Review*, 153(6), 1883-1950.
- Fajar, I., R. Hardyansah, & D. Darmawan. (2024). Development of Cybercrime Law in Indonesia: Challenges and Prospects. *Journal of Science, Technology and Society*, 5(1), 1-8.
- Faridi, F., D. Darmawan, R. Hardyansah, A. R. Putra, A. S. Wibowo. (2023). Legal Protection for Online-Based Lending Consumers, *International Journal of Service Science, Management, Engineering, and Technology*, 4(2), 34–38.
- Fikri, A. Z., S. F. Yulianis, D. Darmawan, S. Sudjai, & M. C. Rizky. (2023). Criminalization in Money Laundering Cases in Indonesia. *Journal of Science, Technology and Society*, 4(2), 21-30.
- Gani, A., R. K. Khayru, & D. Darmawan. (2021). Minimalism Trends in Consumption Behavior: Social Inequality and Industrial Dynamics, *Journal of Social Science Studies*, 1(1), 129 – 134.
- Guamán, D. S., del Alamo, J., & Such, J. M. (2023). Automated GDPR compliance assessment for cross-border personal data transfers in android applications. *Computers & Security*. <https://doi.org/10.1016/j.cose.2023.103262>
- Infante, A. & R. Mardikaningsih. (2022). The Potential of social media as a Means of Online Business Promotion, *Journal of Social Science Studies*, 2(2), 45-49.
- Irfan, M. & D. S. Negara. (2023). The Effectiveness of Consumer Protection Arrangements in E-Commerce Transactions on the Shopee Marketplace Platform in Indonesia, *Journal of Social Science Studies* 3(2), 115 – 120.
- Issalillah, F. & R. Hardyansah. (2022). The Impact of the Digital Divide and Misinformation on Participation and Trust in Local Communities, *Journal of Social Science Studies*, 2(2), 7 – 12.
- Issalillah, F., & Hardyansah, R. (2024). Relevance of Privacy Within the Sphere of Human Rights: A Critical Analysis of Personal Data Protection. *Bulletin of Science, Technology and Society*, 3(1), 31-39.
- Jaman, U. B., Putri, G. R., & Anzani, T. A. (2021). Urgensi Perlindungan Hukum Terhadap Hak Cipta Karya Digital. *Jurnal Rechten: Riset Hukum dan Hak Asasi Manusia*, 3(1), 9–17.
- Janitra, R. M. S., Az, M. G., & Wisnuwardhani, D. A. (2021). Asas Kebebasan Berkontrak dan Perlindungan Konsumen dalam Kontrak Baku Pada Internet Banking. *Jurnal Cakrawala Hukum*, 12(3), 334–343.
- Kementerian Perdagangan. (2020). Peraturan Kementerian Perdagangan Nomor 50 Tahun 2020 tentang Ketentuan Perizinan Berusaha, Pengawasan, dan Pembinaan Pelaku Usaha Perdagangan Melalui Sistem Elektronik. *Berita Negara Republik Indonesia Tahun 2020 Nomor 498*. Jakarta.
- Kirillova, E. A., Shergunova, E. A., Ustinovich, E. S., Nadezhin, N. N., & Sitdikova, L. B. (2016). The Principles of the Consumer Right Protection in Electronic Trade: A Comparative Law Analysis. *International Journal of Economics and Financial Issues*, 6(2), 117-122.
- Krisharyanto, E., & Setyowati, P. J. (2019). Pengendalian Pre-Project Selling Melalui Prinsip Perlindungan Konsumen Berdasarkan UU Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen. *Perspektif*, 24(2), 124–130.
- Makarim, E. (2008). *Kompilasi Hukum Telematika*. Gravindo Persada, Surabaya.
- Miru, A. (2020). *Hukum Kontrak & Perancangan Kontrak*. Raja Grafindo, Surabaya.
- Nasrudin, F. K., & Latumahina, R. E. (2022). Perlindungan hukum terhadap konsumen kartu sim yang mengalami kebocoran data akibat peretasan. *Bureaucracy Journal : Indonesia Journal of Law and Social-Political Governance*. <https://doi.org/10.53363/bureau.v2i1.137>
- Nasution, A. (1995). *Konsumen dan Hukum*. Pustaka Sinar Harapan, Jakarta.
- Negara, D.S. & D. Darmawan. (2023). Digital Empowerment: Ensuring Legal Protections for Online Arisan Engagements. *Bulletin of Science, Technology and Society*, 2(2), 13-19.
- Oriento, D.S. Negara, A.R. Putra, S. Arifin, & R. Saputra. (2021). Risks and Legal Protection in Non-Cash Financial Transactions Through E-Wallets, *Journal of Social Science Studies*, 3(1), 109 – 114.
- Permata Rizki, R. D. A., Brahmana, H., Iskandar, J., An, Y., & Susanto, H. H. S. (2022). Tinjauan Yuridis Perlindungan Hak Privasi Dalam Transaksi Elektronik Pada Era Disrupsi Teknologi. *Journal of Education, Humaniora and Social Sciences*. <https://doi.org/10.34007/jehss.v4i4.1044>
- Prastyanti, R. A., Rahayu, I., Yafi, E., Wardiono, K., & Budiono, A. (2022). Law And Personal Data: Offering Strategies For Consumer Protection In New Normal Situation In Indonesia. *Jurnal Jurisprudence*. <https://doi.org/10.23917/jurisprudence.v1i1i.14756>
- Qureshi, M. I., Nasien, D., & Adiya, M. H. (2023). Mobile-Based Applications: The Legal Challenges on Data Privacy. *International Journal of Online Engineering (Ijoe)*. <https://doi.org/10.3991/ijoe.v19i09.40915>
- Republik Indonesia. (1999). Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. *Lembaran Negara Republik Indonesia Tahun 1999 Nomor 22*. Sekretariat Negara, Jakarta.
- Republik Indonesia. (2008). Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). *Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58*. Sekretariat Negara, Jakarta.
- Romdoni, I. A. (2024). Legal Analysis of Consumer Protection in E-Commerce Transactions. *Jurnal Jendela Hukum Indonesia*, 2(1), 11- 21.
- Rusianto, R., R. Hardyansah, & D. Darmawan. (2023). Application of the Elements of Money Laundering Crime in Indonesian Jurisprudence, *Bulletin of Science, Technology and Society*, 2(3), 44-50.
- Sahid, R. R., R. Hardyansah, D. Darmawan, D.S. Negara, & R.K. Khayru. (2023). Legal Perspective of Investment Risk Mitigation on Peer-to-peer Lending Platforms, *Journal of Social Science Studies*, 3(1), 177 – 184.
- Saragih, A. E., Bagaskara, M. F., & Mulyadi. (2023). Perlindungan Hukum Terhadap Konsumen dalam Transaksi E-Commerce. *Jurnal Kajian Hukum dan Pendidikan Kewarganegaraan*, 2(2), 3-8.
- Sidobalok, J. (2014). *Hukum Perlindungan Konsumen di Indonesia*. Citra Aditya, Bandung.
- Silfiah, R. I., Suwardi, Humiati, Sulatri, K., & Ismail, Y. (2024). Legal Protection of Consumers with Online Transactions. *Journal of Law, Politic and Humanities*, 4(6), 2584-2595.
- Sinambela, E. A. & D. Darmawan. (2022). Advantages and Disadvantages of Using Electronic Money as a Substitute for Cash, *Journal of Social Science Studies*, 2(2), 56-61.
- Subekti. (2000). *Hukum Perjanjian* (7th ed.). PT. Intermasa, Bogor.
- Sulaiman, M., N. H. Pakpahan, & A. R. Putra. (2023). Analysis of the Validity and Effectiveness of Electronic Contracts in Legal Protection of Digital Transactions in Indonesia, *Journal of Social Science Studies*, 3(1), 41–46.

- Susanto, J. A., R. Hardyansah, D. Darmawan, & R. K. Khayru. (2024). Juridical analysis of consumer protection in counterfeit drug transactions in the digital era. *Legalis et Socialis Studiis*, 2(2), 1–9.
- Suwito., F. Diagantara, Mujito, R. Hardyansah & P. Saktiawan. (2022). Navigating Social Mobility Through Reintegration of Crime-Involved Individuals, *Journal of Social Science Studies*, 2(1), 157 – 160.
- Tjin Tai, E. (2018). Data Ownership and Consumer Protection. *Social Science Research Network*. <https://doi.org/10.2139/SSRN.3172725>
- Wahyudi, E., D. Darmawan, & R. Hardyansah. (2023). Legal Protection for Online Ojek Drivers Who are Victims of Fictitious Order, *Bulletin of Science, Technology and Society*, 2(2), 37-43.
- Wahyudi, W., Kabalmay, R. N. K., & Amri, M. W. (2021). Big Data and New Things in Social Life. *Studi Ilmu Sosial Indonesia*, 1(1), 1-12.
- Wulandari, W. & D. Darmawan. (2022). Salesperson Interaction Quality and Consumer Decisions in Online Transactions, *Journal of Social Science Studies*, 2(2), 91 – 98.
- Wulandari, Y. S. (2018). Perlindungan Hukum bagi Konsumen terhadap Transaksi Jual Beli E-Commerce. *Jurnal Ilmu Hukum*, 2(2), 199-210.
- Yuliana, S. (2022). Perlindungan Hukum Terhadap Usaha Kecil Menengah (UKM) Berdasarkan UU No. 8 Tahun 1999 Tentang Hukum Perlindungan Konsumen. *Justici*, 14(1), 1–14.
- Yuniarti, S. (2019). Perlindungan Hukum Data Pribadi di Indonesia. *Business Economic, Communication, and Social Sciences (BECOSS) Journal*, 1(1), 147–154.