Research Horizon

ISSN: 2808-0696 (p), 2807-9531 (e)

Research Horizon
Volume: 05
Issue: 02
Year: 2025
Page: 119-128

Citation:
Supriyanto, S., Rahardjo, T. M. S., Sumiyati, S., Noerdjaja, H., Pambudi, G. E., & Prabowo, M. S. (2025). Consumer protection legal frameworks in Indonesia: The challenges of e-commerce and data privacy. *Research Horizon*, *5*(2), 119–128.

Consumer Protection Legal Frameworks in Indonesia: The Challenges of E-Commerce and Data Privacy

Supriyanto[1*], Tanti Malaka Sari Rahardjo[1], Sumiyati[1], Himawan Noerdjaja[1], Gumilang Eka Pambudi[1], M. Shidqon Prabowo[1]

[1] Universitas Wahid Hasyim, Semarang, Indonesia

[*] *Corresponding author: Supriyanto (mhsmhunwahas1@gmail.com)*

Abstract

Consumer protection law in Indonesia, primarily governed by Law No. 8 of 1999, aims to safeguard consumer rights amidst the complexities of a growing economy. While this law has helped address power imbalances between consumers and businesses, it faces limitations in dealing with challenges arising from the digital economy, particularly in the realms of e-commerce and data privacy. The main objective of this study is to evaluate the effectiveness of Indonesia's consumer protection framework in the context of these modern challenges. Using a juridical-normative approach, the research analyzes relevant legal provisions through qualitative techniques, focusing on the applicability of existing laws to digital transactions. The study reveals significant gaps, particularly in the protection of personal data, cybersecurity, and privacy in e-commerce. Although various regulations, such as the Electronic Information and Transactions Law and the Trade Law, provide some safeguards, they remain insufficient in fully addressing the risks posed by rapid technological advancements. The enforcement mechanisms are also weak, leaving consumers vulnerable to issues like fraud and data breaches. The study concludes that Indonesia's consumer protection laws must be revised to address these new challenges, with a more comprehensive and centralized framework that aligns with international standards on data protection and digital transactions.

Keywords

Consumer Protection, E-commerce, Data Privacy, Legal Framework, Indonesia.

1. Introduction

The rapid growth of e-commerce has significantly altered global markets, offering new opportunities for both businesses and consumers. In Indonesia, this transformation is especially notable, as the country has emerged as the largest e-commerce market in Asia. The proliferation of digital platforms and online transactions has fuelled economic development, expanding access to goods and services in ways previously unimaginable (Darajat, 2014). However, the swift expansion of e-commerce also brings with it a host of challenges, particularly in the areas of consumer protection, data privacy, and cybersecurity. While Indonesia's Consumer Protection Law, established under Law No. 8 of 1999, was designed to address the power imbalances between consumers and businesses in traditional markets, it is ill-equipped to deal with the complexities of the digital economy (Arifin et al., 2021). As such, the protection of consumer rights in online transactions remains an unresolved issue.

The Consumer Protection Law was originally introduced to safeguard consumer rights amidst a rapidly growing economy. It laid the foundation for regulating consumer-business relationships by specifying the rights and responsibilities of both consumers and businesses. This framework helped to ensure fair transactions, providing a mechanism for addressing disputes and promoting transparency in the marketplace (Widijowati, 2023). However, as e-commerce expanded, it became evident that the law's provisions were inadequate in addressing the unique risks presented by digital transactions. The law, which primarily focuses on traditional business models, fails to account for issues such as data protection, digital privacy, and the intricacies of online fraud. As a result, consumers engaging in electronic transactions are left vulnerable to various forms of exploitation, including the unauthorized use of personal data, identity theft, and financial fraud (Rahmanto et al., 2019; Arifin et al., 2021).

The inadequacy of the Consumer Protection Law in the digital context has prompted lawmakers and regulators to develop additional legal frameworks to address emerging challenges (Prayuti, 2024). For instance, the Electronic Information and Transactions Law (ITE Law) and the Trade Law were introduced to regulate online transactions, offering a degree of protection for consumers engaging in e-commerce (Kurniawan & Setyawan, 2024). These regulations aim to ensure that online transactions are conducted in a transparent and fair manner, providing consumers with certain protections, such as the recognition of electronic evidence and digital signatures. The ITE Law also seeks to balance the interests of businesses and consumers by enforcing the principles of fairness in electronic contracts and preventing fraudulent Law invitees in the digital space. However, despite these efforts, the existing legal provisions remain fragmented and insufficient to fully address the complexity of the digital marketplace (Muslim et al., 2025). The lack of a unified legal framework, coupled with overlapping regulations, has made enforcement difficult, leaving consumers exposed to significant risks.

One of the most pressing challenges in consumer protection is the issue of data privacy (Kerber, 2016). In the digital economy, personal data has become a valuable commodity, often traded or misused by businesses for various purposes, including targeted marketing and profiling (Corones & Davis, 2017). While the ITE Law and other regulations provide some safeguards, they fail to comprehensively address the growing concerns surrounding data protection in e-commerce. The rapid expansion of cyberspace has introduced numerous risks, including cybercrimes that can compromise the confidentiality and integrity of consumer data (Elifneh et al., 2024). Indonesia's current legal framework lacks a centralized law to safeguard personal data, with existing regulations scattered across more than 30 different laws and policies. This fragmented approach not only complicates enforcement but also leaves

significant gaps in consumer protection. Consumers, who often lack awareness of their rights in the digital space, are particularly vulnerable to these risks (Saragih & Bagaskara, 2023).

The absence of a comprehensive data protection law has led to concerns about the security of personal information in e-commerce transactions (Ciocchetti, 2007). Data breaches, identity theft, and unauthorized access to sensitive information are common issues faced by consumers, and the legal mechanisms in place to address these problems are often insufficient. Moreover, Indonesia's regulatory approach to data protection is not in line with international standards, such as the European Union's General Data Protection Regulation (GDPR), which has become a global benchmark for privacy protection. The lack of alignment with international standards further exacerbates the challenges posed by cross-border transactions, were data flows freely across national boundaries, often without adequate protection. To address these challenges, Indonesia needs to revise and strengthen its consumer protection laws to keep pace with the evolving digital landscape. Thus, this paper aims to evaluate the effectiveness of Indonesia's existing consumer protection framework in addressing the challenges posed by e-commerce and data privacy concerns, identify gaps in the current legal provisions, and offer recommendations for the development of a more comprehensive and centralized approach to consumer protection in the digital economy.

2. Methods

This study aims to evaluate the effectiveness of Indonesia's existing consumer protection framework in addressing the challenges posed by e-commerce and data privacy concerns. By employing a juridical-normative approach, this research will analyze the current legal provisions and assess their applicability to digital transactions. The study will identify the gaps in consumer protection, particularly in the areas of data protection, cybersecurity, and privacy in e-commerce. It will also examine the enforcement mechanisms in place and explore the challenges faced by regulators in ensuring compliance with consumer protection laws in the digital economy. The findings of this study will provide valuable insights into the limitations of Indonesia's current legal framework and offer recommendations for the development of a more comprehensive and centralized approach to consumer protection in the digital age.

Ultimately, this research seeks to contribute to the growing body of literature on consumer protection in the digital economy, advocating for legal reforms that align Indonesia's policies with international standards. As the digital economy continues to expand, it is crucial that Indonesia takes proactive steps to safeguard the rights of consumers in the online space. Only through a robust and comprehensive legal framework can consumers be fully protected from the risks associated with e-commerce and digital transactions.

3. Results and Discussion

3.1. Gaps in Indonesia's Consumer Protection Framework

Indonesia's consumer protection laws, primarily governed by Law No. 8 of 1999, were initially designed to regulate and preserve consumer rights amidst the complexities of traditional production and consumption. The law aimed to address power imbalances between consumers and business Lawlor's, ensuring a fair and equitable transaction process. However, as the economy shifts towards the digital realm, the existing provisions in the Consumer Protection Law have proven inadequate to address the new challenges posed by e-commerce, data protection, cybersecurity, and consumer privacy. This section examines the gaps in Indonesia's consumer protection framework, focusing on the risks and vulnerabilities associated

with digital transactions and the lack of comprehensive protection for consumers in the e-commerce environment (Arifin et al., 2021).

A significant gap in Indonesia's current legal framework is the insufficient coverage of data protection and consumer privacy in the digital space. While the Consumer Protection Law (No. 8 of 1999) outlines the rights of consumers and aims to ensure fairness in business transactions, it fails to address the growing complexities of digital transactions, particularly in terms of data privacy, encryption, and the use of personal information in e-commerce (Widiarty & Fahim, 2024). With Indonesia now being the largest e-commerce market in Asia, the importance of safeguarding personal data has become increasingly urgent. However, personal data protection is fragmented across multiple laws and regulations, with no single, unified legal framework governing how businesses must handle consumer data (Ridho et al., 2024).

Currently, Indonesia's data protection regulations are scattered across over 30 different legal provisions, none of which offer a comprehensive solution to the risks of data misuse, hacking, or fraud in the digital marketplace. Although the Information and Electronic Transactions (ITE) Law (No. 19 of 2016) provides some legal protection, it does not provide clear guidelines or enforcement mechanisms for protecting consumer data from cybercrimes such as identity theft, data breaches, and unauthorized transactions. The lack of a comprehensive data protection law leaves consumers vulnerable to exploitation, as businesses may misuse consumer data for profit, or fail to take adequate precautions to secure sensitive information.

Additionally, Indonesia's cybersecurity framework is underdeveloped, which compounds the risks consumers face in the digital economy. While there are some regulations in place, such as the ITE Law and Government Regulations No. 80 of 2019 and No. 71 of 2019, which address electronic transactions and e-commerce, they do not provide sufficient coverage or detailed cybersecurity measures (Arifin et al., 2021). The rise of cybercrimes, including phishing, hacking, and online fraud, presents an ongoing challenge to consumer protection in the digital age. Businesses often lack the necessary tools or legal obligations to implement effective cybersecurity measures to protect consumer data from cyberattacks. There is an urgent need for comprehensive cybersecurity regulations that require businesses to invest in better protection measures, implement strong encryption protocols, and offer remedies to consumers who suffer from digital fraud.

The current regulatory framework also suffers from fragmented enforcement and overlapping authority among different government agencies, which complicates the enforcement of consumer protection laws. Multiple agencies, including the Ministry of Trade, the Ministry of Communication and Information Technology, and the Financial Services Authority (OJK), all play roles in regulating e-commerce and consumer protection in the digital realm. However, these agencies often have overlapping mandates, leading to confusion and inefficiency in enforcing consumer protection laws. The lack of a clear and unified regulatory body responsible for overseeing the digital marketplace results in inconsistent enforcement of existing laws. For example, platform providers, who facilitate online transactions and store consumer data, are subject to different sets of regulations depending on their sector, making it difficult to ensure comprehensive consumer protection (Marsela et al., 2024).

The absence of a cohesive legal framework for digital platforms is particularly problematic. As online platforms continue to grow in influence, they play an integral role in facilitating transactions, collecting consumer data, and managing customer relationships (Stănescu, 2019). Despite this, there is no clear, overarching legal framework that governs platform providers' responsibilities in safeguarding consumer rights. While the Consumer Protection Law holds businesses accountable for informing consumers about transactions and ensuring the availability of

products, enforcement of these terms is often inconsistent. Platform providers are also often not held accountable for losses consumers may suffer during online transactions, which further exposes consumers to potential harm.

Moreover, Indonesia's current regulations are not sufficiently tailored to address the challenges posed by the growing use of digital platforms and the new business models emerging from the digital economy. Digital platforms have revolutionized industries, created new opportunities but also raised concerns about unfair competition, monopolistic practices, and the potential for exploitation of consumer data. Price-fixing agreements, data misuse, and breaches of privacy policies are becoming more common in e-commerce, undermining consumer welfare and trust in the digital marketplace. The lack of clear guidelines for addressing these issues within the current regulatory framework exacerbates the risks that consumers face.

Indonesia also faces challenges in aligning its legal framework with international standards, particularly in terms of data protection. As global trade and e-commerce transactions become more interconnected, there is an increasing need for Indonesia to adopt regulations that align with global best practices, such as the EU's General Data Protection Regulation (GDPR). Without clear and comprehensive data protection laws that align with international norms, Indonesia risks becoming an outlier in global e-commerce and data protection discussions.

The growing importance of consumer protection in the digital economy cannot be overstated. As Indonesia's digital economy continues to expand, the current legal framework needs to evolve to address the complexities of digital transactions. Strengthening data protection laws, improving cybersecurity measures, and creating a more cohesive regulatory structure are critical steps towards ensuring that consumers are adequately protected in the digital marketplace. By addressing these gaps, Indonesia can foster a safer, more transparent e-commerce environment that benefits both consumers and businesses alike.

3.2. Enforcement Mechanisms and Compliance Challenges

Enforcement mechanisms and compliance challenges in Indonesia's consumer protection laws, particularly in the digital economy, remain a critical issue due to the rapid expansion of e-commerce and the increasing complexity of digital transactions (Mulyani et al., 2023). Indonesia's consumer protection framework, primarily governed by Law No. 8 of 1999, was initially developed to address traditional business transactions. It aimed to regulate consumer rights and ensure fairness in the relationship between consumers and businesses. However, the advent of the digital economy and the proliferation of online transactions have exposed significant gaps in the law's ability to protect consumers effectively in this new context (Subagyono et al., 2023).

One of the primary enforcement challenges lies in the outdated legal provisions that fail to address the nuances of digital transactions. While the Consumer Protection Law outlines the rights and obligations of consumers and businesses, it does not cover crucial aspects like data protection, cryptography, or e-commerce privacy policies (Moeslim et al., 2025). These areas have become increasingly important as e-commerce has flourished, making the existing provisions inadequate for addressing the security risks and consumer rights issues in digital transactions. The law, while ensuring transparency and fairness, particularly through standard contracts and consumer disclosures in e-commerce, is not equipped to address the challenges of cybersecurity and personal data protection in the digital age.

The rapid growth of Indonesia's e-commerce market, now the largest in Asia, has placed additional pressure on the regulatory framework. Despite the introduction of several relevant laws, including the Trade Law No. 7 of 2014, the Consumer Protection Law No. 8 of 1999, and the Electronic Information and Transactions (ITE) Law No. 19 of 2016, enforcement remains a significant challenge. These laws cover a broad range of issues, such as trade protection, consumer rights, and

electronic transactions, but the overlapping nature of these regulations creates confusion and inefficiency in enforcement. For example, the ITE Law provides legal protection for online transactions, recognizing electronic evidence and digital signatures, but does not fully cover data protection or establish a clear supervisory mechanism to ensure compliance. Furthermore, regulations like Government Regulation No. 80 of 2019 and No. 71 of 2019 address e-commerce transactions but fail to address the full spectrum of cybersecurity risks and data privacy concerns.

A central issue in enforcement is the lack of a comprehensive, unified regulation for personal data protection. Indonesia's current legal framework for personal data is scattered across 32 different regulations, none of which provide the kind of centralized, cohesive protections needed in the digital economy. This fragmentation leaves businesses with little guidance on how to handle consumer data responsibly, making it difficult for regulators to enforce compliance effectively. While administrative sanctions and criminal fines exist, these penalties are often insufficient to deter businesses from engaging in practices that compromise consumer privacy or data security (Park, 2019). Moreover, the delayed implementation of a draft bill on personal data protection exacerbates the issue, as the bill is expected to take several years for full implementation, leaving consumers vulnerable in the meantime.

Additionally, Indonesia's regulatory framework suffers from institutional fragmentation, as multiple government agencies, including the Ministry of Trade, the Ministry of Communication and Information Technology, and the Financial Services Authority (*Otoritas Jasa Keuangan*/OJK), are tasked with regulating different aspects of the digital economy. This division of responsibilities creates enforcement challenges, as these agencies often have overlapping mandates, leading to inefficiencies and confusion. For example, platform providers, who play a key role in facilitating online transactions, are subject to different sets of regulations depending on their sector, complicating efforts to ensure consumer protection. The lack of a clear and unified regulatory body to oversee e-commerce and digital transactions further exacerbates these enforcement challenges.

Another significant challenge is the growing prevalence of cybercrimes, including hacking, phishing, and identity theft, which pose serious risks to consumer protection in the digital economy. While some provisions in the ITE Law and other regulations address cybercrimes, they do not provide detailed guidelines or comprehensive measures to ensure that businesses take sufficient precautions to protect consumer data. The absence of strict cybersecurity requirements leaves consumers vulnerable to fraud and exploitation. To address this, there is an urgent need for stronger enforcement of cybersecurity measures and stricter regulations to hold businesses accountable for failing to secure consumer data adequately.

The rise of digital platforms, which facilitate transactions across various sectors, also presents unique enforcement challenges. Platforms have significant control over the goods and services sold, as well as consumer data, yet the current legal framework does not hold platform providers fully accountable for consumer losses or data breaches (Aji & Subakdi, 2024). While the Civil Code outlines the obligations of platform providers, enforcement of these terms is often inconsistent. The lack of clear legal responsibilities for platform providers in ensuring consumer protection and safeguarding personal data leads to gaps in accountability.

Lastly, there is a challenge in regulating monopolistic practices and ensuring fair competition in the digital marketplace. Price-fixing agreements and data misuse are becoming more common as businesses, particularly digital platforms, seek to exploit consumer data for profit. This lack of regulation could harm consumers by reducing their purchasing power or exposing them to privacy violations. The absence of robust mechanisms to monitor and enforce compliance with fair competition laws complicates efforts to protect consumers from these harmful practices.

In conclusion, Indonesia's consumer protection laws are currently struggling to keep pace with the challenges of the digital economy. While several regulations exist to address e-commerce and consumer rights, the fragmented nature of these laws, combined with inadequate enforcement mechanisms and the rise of new risks like cybersecurity threats and data misuse, creates significant challenges for regulators. Strengthening enforcement, developing comprehensive data protection regulations, and improving coordination between regulatory agencies are critical steps towards ensuring that Indonesian consumers are adequately protected in the increasingly complex digital marketplace.

3.3. Recommendations for Strengthening Consumer Protection in the Digital Economy

The rapid expansion of Indonesia's digital economy, particularly through e-commerce and online transactions, has created significant opportunities for both consumers and businesses. However, this growth has also exposed several vulnerabilities within the existing consumer protection framework, which was originally designed for traditional forms of commerce. Indonesia's current legal structure, primarily governed by Law No. 8 of 1999 on Consumer Protection, provides a foundational basis for protecting consumer rights but is insufficient to address the complex challenges arising from the digital economy (Akhmaddhian & Agustiwi, 2016; Pattipeiluhu et al., 2020). The law, while ensuring that consumers are protected in transactions, was developed when the market was more traditional, and it has struggled to keep pace with the evolution of e-commerce and digital transactions.

One of the most pressing issues is the lack of a unified personal data protection law. Indonesia's fragmented approach to personal data protection, which currently involves over 30 separate regulations, creates significant gaps in consumer safeguards. This fragmented regulatory framework is insufficient in the face of mounting concerns about data misuse, cybercrimes, and the increasing risks associated with cross-border data flows. To address these issues, Indonesia needs to enact a comprehensive, centralized law that governs the collection, processing, and storage of personal data. Such a law should align with international standards, particularly the European Union's General Data Protection Regulation (GDPR), to ensure robust protections for consumer data in the digital sphere. Clear guidelines should be established to define the responsibilities of businesses in managing consumer data, and the law should include severe penalties for violations, particularly data breaches. In addition, an independent supervisory body should be created to monitor compliance, investigate breaches, and ensure that businesses adhere to privacy standards, thus fostering greater consumer trust in the digital economy (Marsela et al., 2024).

Alongside data protection, the regulation of e-commerce practices must be strengthened. While existing laws like the Consumer Protection Law and the Electronic Information and Transactions Law (ITE Law) do offer some protections for online transactions, they are largely insufficient in regulating the complexities of modern e-commerce. As the digital marketplace grows, it is essential that Indonesia revises its legal framework to address emerging challenges such as online fraud, cybercrimes, and unfair business practices (Zulham, 2023). Specific provisions should be included in the updated laws to ensure that businesses handle online transactions securely and transparently. For example, platform providers should be held accountable for ensuring the authenticity of products and services offered through their platforms, as well as guaranteeing that transactions are secure and consumer data is not exploited. Moreover, businesses should be required to implement fair and transparent terms of service that protect consumers' legal rights, including providing consumers with clear avenues for dispute resolution.

Digital platforms also play a central role in Indonesia's e-commerce ecosystem, serving as intermediaries between buyers and sellers. However, the current legal framework does not sufficiently hold platform providers accountable for risks that consumers face during online transactions. As facilitators of transactions, platforms have control over the goods and services they host, and they often dictate the terms and conditions under which transactions occur. Indonesia's legal framework should be updated to make platform providers more accountable for consumer protection. For example, platforms should be required to ensure that their terms and conditions are transparent and that they do not create imbalances between consumers and businesses. Platforms should also be held responsible for resolving consumer complaints related to defective goods, fraud, or unfair practices. If platforms fail to meet these obligations, they should face legal consequences to ensure compliance with consumer protection standards.

Furthermore, cybersecurity is another critical area where Indonesia's current laws fall short. With the increase in cybercrimes such as data breaches, identity theft, and hacking, it is crucial that Indonesia adopts stronger cybersecurity measures to protect consumers in the digital space. While some regulations address aspects of cybersecurity, they are not comprehensive enough to tackle the evolving nature of online threats. Indonesia should implement more robust cybersecurity standards for businesses, particularly those that handle sensitive consumer data. Companies should be mandated to notify consumers promptly in the event of a data breach, and they should be held responsible for implementing adequate security measures to prevent cyber threats. Additionally, cooperation with international cybersecurity organizations will be vital to ensure that Indonesia's legal framework is aligned with global best practices and can effectively combat cross-border cybercrime.

Another challenge is the low level of consumer awareness regarding their rights and the available protections under Indonesian law. Many consumers are unaware of the legal remedies available to them in the event of fraud or data misuse, which undermines the effectiveness of consumer protection laws. To address this, Indonesia should launch comprehensive educational campaigns to raise awareness about consumer rights in the digital economy. These campaigns should focus on educating consumers about their rights under the law, how to protect their personal data online, and what to do if they experience unfair practices or data breaches. By empowering consumers with this knowledge, Indonesia can create a more informed and confident consumer base, which in turn will promote better compliance with consumer protection regulations.

Finally, enforcement of consumer protection laws in Indonesia needs to be more robust and centralized. At present, enforcement is hampered by overlapping regulatory authority and fragmented responsibilities across multiple agencies. This creates confusion and delays in addressing consumer grievances. To remedy this, Indonesia should consolidate the responsibility for consumer protection under a single regulatory body that is empowered to oversee all aspects of consumer protection, from e-commerce to data privacy. This body should have the authority to investigate complaints, impose penalties, and take legal Law ion against businesses that violate consumer rights. Additionally, the use of technology, such as online complaint portals and digital platforms, could help streamline the process of consumer redress and make it easier for consumers to report issues and seek resolution.

In conclusion, as Indonesia's digital economy continues to grow, it is crucial that the country's consumer protection laws evolve to meet the demands of the digital age. By enacting a unified personal data protection law, strengthening e-commerce regulations, enhancing platform accountability, improving cybersecurity measures, promoting consumer education, and ensuring effective enforcement, Indonesia can build a legal framework that protects consumers and fosters trust in the digital

economy. This comprehensive approach will not only benefit consumers but will also create a more secure and fair environment for businesses to thrive in.

4. Conclusion

The study found that Indonesia's current consumer protection laws are inadequate for addressing the growing challenges posed by the digital economy. The absence of a comprehensive data protection law and the fragmented regulatory approach leave consumers vulnerable to risks such as data breaches, identity theft, and cybercrimes. The existing laws, including Law No. 8 of 1999 on Consumer Protection and the ITE Law, are outdated and fail to align with international standards like the European Union's General Data Protection Regulation (GDPR), which has become a global benchmark for privacy and data protection. This misalignment, particularly in the context of cross-border data flows, exacerbates the challenges posed by e-commerce and online transactions.

To address these concerns, Indonesia needs to overhaul its legal framework to provide a unified and comprehensive approach to consumer protection in the digital age. This paper recommends the establishment of a centralized personal data protection law that consolidates existing regulations and adheres to global standards, with severe penalties for violations. In addition, e-commerce laws must be updated to tackle issues such as fraud and cybercrimes, with businesses held accountable for securing online transactions and protecting consumer data. Platforms should be made responsible for ensuring the authenticity of products and services, as well as for handling consumer complaints.

Furthermore, enhanced cybersecurity regulations are crucial, with businesses required to promptly notify consumers in the event of data breaches. Educational campaigns should be launched to raise consumer awareness of their rights and available protections in the digital economy. Finally, the enforcement of consumer protection laws should be streamlined under a single regulatory body, empowered to investigate and address grievances efficiently. By implementing these recommendations, Indonesia can foster a safer, more secure digital environment for consumers, while ensuring a fairer playing field for businesses.

References

Aji, M. P., & Subakdi, S. (2024). Sosialisasi Kesadaran Keamanan Siber dan Perlindungan Data Pribadi Bagi Warga di Kelurahan Pangkalan Jati, Kota Depok. *Jurnal Syntax Admiration*, *5*(8), 2928-2937.

Akhmaddhian, S., & Agustiwi, A. (2016). Perlindungan Hukum Terhadap Konsumen Dalam Transaksi Jual Beli Secara Elektronik Di Indonesia. *Unifikasi: Jurnal Ilmu Hukum*, *3*(2), 40-60.

Arifin, R., Kambuno, J. A., Waspiah, W., & Latifiani, D. (2021). Protecting the Consumer Rights in the Digital Economic Era: Future Challenges in Indonesia. *Jambura Law Review*, *3*, 135-160.

Ciocchetti, C. A. (2007). E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors. *American Business Law Journal*, *44*(1), 55-126.

Corones, S., & Davis, J. (2017). Protecting consumer privacy and data security: Regulatory challenges and potential future directions. *Federal Law Review*, *45*(1), 65-95.

Darajat, I. K. (2014). Perlindungan Hukum Bagi Pelaku Usaha Dan Konsumen Dalam Transaksi Jual Beli Secara Online Dengan Pembayaran Melalui Paypal. *E-Journal Graduate Unpar*, *1*(2), 48-53.

Elifneh, Y. W., Wonda, T. A., & Abbay, Y. A. (2024). Marketing ethics in the wholesale and retail sector: empirical evidence from Ethiopia (a qualitative inquiry). *Cogent Business & Management*, *11*(1), 2373353.

Kerber, W. (2016). Digital markets, data, and privacy: competition law, consumer law and data protection. *Journal of Intellectual Property Law & Practice*, jpw150.

Kurniawan, I. D., & Setyawan, V. P. (2024). The Importance of Protecting E-Commerce Consumer Personal Data. *IJOLARES: Indonesian Journal of Law Research*, *2*(2), 51-55.
Marsela, D., Yudhistira, Y., & Fawaid, B. (2024). Legal Protection of Consumers in Online Business: A Criminal Law Perspective in Handling Fraud and Identity Theft. *Research Horizon*, *4*(3), 99-106.
Moeslim, Y. J., Maryono, M., & Suasungnern, S. (2025). Legal Protection Of E-Commerce Consumers: A Review Of Regulation and Implementation. *Journal Evidence Of Law*, *4*(1), 159-166.
Mulyani, S., Suparno, S., & Sukmariningsih, R. M. (2023). Regulations and Compliance in Electronic Commerce Taxation Policies: Addressing Cybersecurity Challenges in the Digital Economy. *International Journal of Cyber Criminology*, *17*(2), 133-146.
Muslim, M., Aituru, Y. P., & Upara, A. R. (2025). Legal Protection of Consumers in the Digital Business World. *JHK: Jurnal Hukum dan Keadilan*, *2*(2), 15-27.
Park, S. (2019). Why information security law has been ineffective in addressing security vulnerabilities: Evidence from California data breach notifications and relevant court and government records. *International Review of Law and Economics*, *58*, 132-145.
Pattipeiluhu, I. B., Rumkel, N., & Suwarti, S. (2020). Kajian Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen Terkait Promosi Iklan Perumahan di Kota Ternate. *Khairun Law Review*, *1*(1).
Prayuti, Y. (2024). Dinamika perlindungan hukum konsumen di era digital: Analisis hukum terhadap praktik e-commerce dan perlindungan data konsumen di Indonesia. *Jurnal Interpretasi Hukum*, *5*(1), 903-913.
Rahmanto, T. Y., Kav, J. H. R. S., & Kuningan, J. S. (2019). Penegakan Hukum Terhadap Tindak Pidana Penipuan Berbasis Transaksi Elektronik. *Jurnal Penelitian Hukum De Jure*, *19*(1), 31.
Ridho, F. A., Dzaki, A., & Masruroh, A. (2024). Comparative Analysis of Civil Law Liability Towards Consumers in Business Disputes. *Research Horizon*, *4*(5), 45-54.
Saragih, A. E., & Bagaskara, M. F. (2023). Perlindungan Hukum Terhadap Konsumen Dalam Transaksi E-Commerce. *Civilia: Jurnal Kajian Hukum dan Pendidikan Kewarganegaraan*, *2*(1), 145-155.
Stănescu, C. G. (2019). The Responsible Consumer in the Digital Age: On the Conceptual Shift from'Average'to'Responsible'Consumer and the Inadequacy of the'Information Paradigm'in Consumer Financial Protection. *Tilburg Law Review*, *24*(1).
Subagyono, B. S. A., Astutik, S., Chumaida, Z. V., Romadhona, M. K., & Usanti, T. P. (2023). Consumer Dispute in Electronic Transactions: State Obligation and Dispute Settlement Under Indonesia Consumer Protection Law. *Journal of Law and Sustainable Development*, *11*(10), e1240-e1240.
Widiarty, W. S., & Fahim, M. H. K. (2024). Institutional Roles and Mechanisms in Upholding Legal Protection Under Consumer Protection Law in the Era of Globalization. *Jurnal Hukum UNISSULA*, *40*(2), 134-152.
Widijowati, D. (2023). Enhancing Consumer Protection in Electronic Commerce Transactions. *Research Horizon*, *3*(4), 283-290.
Zulham, Z. (2023). A Critical Review Of Indonesian Online Consumer Protection Online Shopping, False Advertising, And Legal Protection For Indonesian E-Commerce Customers. *Journal of Law and Sustainable Development*, *11*(5), 1-15.