Jurnal Sosial dan Teknologi (SOSTECH)
Volume 6, Number 6, Juni 2026
p-ISSN 2774-5147 ; e-ISSN 2774-5155

Consumer Privacy Rights in E-Commerce

Devia Julianda*, Irfan Rizky Hutomo, Muhammad Zainuddin
Universitas Darul Ulum Islamic Centre Sudirman GUPPI, Indonesia
Email: deviajulianda@gmail.com*, irfansky94@gmail.com, mzundaris@gmail.com

Keywords:
Privacy Rights;
Consumers;
E-Commerce;
Personal Data Protection;
Digital Law

Abstract

The rapid expansion of e-commerce in Indonesia has been fueled by advances in digital technology, leading to a significant increase in the collection and processing of customers' personal data by digital service providers. While electronic transactions offer convenience and efficiency, the risk of consumer privacy violations is equally growing. The misuse of personal data, information leaks, and a lack of transparency in data management by e-commerce platforms are major issues in today's digital ecosystem. A legal study is therefore necessary to understand the extent to which Indonesian regulations protect consumer privacy rights in e-commerce. This study aims to examine Indonesian laws protecting consumers' right to privacy in online transactions and to identify implementation challenges. A normative juridical research methodology is employed, drawing on statutory and doctrinal perspectives. The primary legal sources examined include Law Number 27 of 2022 concerning Personal Data Protection (the PDP Law), Law Number 8 of 1999 concerning Consumer Protection, and other relevant regulations such as Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. Secondary legal sources, including scholarly literature, academic publications, and the views of relevant legal experts, are also utilized. This study is expected to offer a more comprehensive understanding of consumer privacy protection in digital transactions and to provide policy recommendations for improving the effectiveness of existing regulations. With robust legal protection in place, it is hoped that consumer privacy rights in e-commerce can be better guaranteed, thereby strengthening public trust in digital transactions

INTRODUCTION

People's consumption habits have changed significantly as a result of advances in digital technology, one notable manifestation of which is the growing use of e-commerce as the primary mode of transaction (Danuri, 2019). The rapid growth of the e-commerce industry in Indonesia reflects the increasing number of consumers turning to digital services to meet their daily needs (Wirapraja, 2018). However, behind the convenience offered lies a consequence that cannot be ignored: the expanding collection and management of consumers' personal data by e-commerce service providers. The personal data collected includes identity information, transaction history, and shopping preferences, which, if not properly managed, can expose consumers to various risks (Prayuti, 2024).

One of the primary risks in online transactions is the misuse of personal data by irresponsible parties (Priliasari, 2023). As the scope of e-commerce expands, consumer data has become a highly valuable commodity for both service providers and interested third parties. This misuse can take the form of identity theft, digital fraud, and opaque profiling practices that harm consumers. Without adequate protection, consumers risk losing control over their personal data, potentially threatening their fundamental rights in the digital environment (Kurnianingrum, 2023).

The right to privacy is an essential component of consumer protection in the context of digital transactions. According to Rahmawati (2023), the right to privacy pertains to an individual's authority over the collection, use, and sharing of their personal information. Within the e-commerce ecosystem, consumers' right to privacy encompasses aspects such as consent to data use, the right to know how their data is managed, and the right to request deletion or correction of personal data in the event of inconsistencies or misuse (Charos, 2023). These rights provide consumers with assurance that their data will not be exploited by digital service providers.

Consumers' right to privacy in e-commerce also encompasses the principles of transparency and control. Transparency requires service providers to furnish consumers with clear information about how their data is collected and for what purposes (Sahabuddin, 2024), while the principle of control empowers consumers to set limits on the use of their data. Both principles play a role in building trust between consumers and service providers, enabling the e-commerce ecosystem to develop in a healthier and more responsible manner (Lidya, 2020).

Personal data protection in e-commerce is further grounded in the principles of fairness and security. The principle of fairness holds that consumers' personal data must not be used in a discriminatory manner or to the detriment of any particular party (Ulum, 2020), while the principle of security requires digital service providers to implement robust protective measures to prevent data leakage or misuse. When these principles are properly observed, consumer privacy rights in e-commerce can be more effectively guaranteed, creating a safer ecosystem for all parties (Patricia, 2024).

Consumer privacy rights in e-commerce are also closely tied to the dimension of digital trust. In an ecosystem built on online transactions, trust is a key element determining the sustainability of the relationship between consumers and service providers. Where consumers perceive that their personal data is not being managed responsibly or is being misused, trust in e-commerce services will inevitably decline (Pohan, 2023). Ensuring privacy protection is therefore beneficial not only to consumers but also to the long-term sustainability of the e-commerce industry.

With adequate protection of privacy rights, consumers can engage in digital transactions with greater confidence and without undue concern about potential data misuse (Wariati, 2014). Robust privacy protection can also encourage broader adoption of e-commerce across society, as trust in digital systems is a key factor in consumers' decisions to use technology-based services. Without strong guarantees of protection, concerns about personal data security can impede the development of e-commerce and reduce public participation in the digital economy.

Overall, consumer privacy rights in e-commerce constitute an integral part of consumer protection in the digital era. These rights not only safeguard consumers' personal data but also foster trust and transparency within the e-commerce ecosystem (Lisdayanti, 2024). With growing awareness of the importance of privacy rights among both consumers and service providers, it is hoped that the e-commerce industry can develop more responsibly and sustainably without compromising the fundamental rights of consumers in the digital environment.

Based on the foregoing, three main research gaps are identified. First, research on consumer privacy rights protection has been fragmented, focusing separately on the Consumer Protection Law, the PDP Law, or Government Regulation Number 71 of 2019, without integrating all three regulatory frameworks. Second, research in Indonesia has tended to be descriptive and has not yet adopted a comparative approach drawing on international standards such as the General Data Protection Regulation (GDPR). Third, no study has specifically identified implementation gaps in existing regulations while simultaneously offering structured strategies for strengthening them. The novelty of this research lies in its use of a normative juridical approach with simultaneous comparative analysis of the three principal regulations, its conceptual comparison of Indonesian privacy protection principles with the GDPR, and its identification of implementation gaps alongside the formulation of holistic and integrated strategies to strengthen consumer privacy protection in e-commerce.

The objectives of this study are to examine the laws and regulations protecting consumer privacy rights in e-commerce, to identify problems and challenges in their implementation, and to formulate strategies for strengthening consumer privacy protection. The theoretical benefits include enriching the study of consumer protection law and information technology law, as well as developing the concept of personal data protection in the context of e-commerce in developing countries. Practically, this research provides input for policymakers — including the Kementerian Komunikasi dan Informatika and the Otoritas Jasa Keuangan — in designing more effective and integrated personal data protection policies, and serves as an evaluation of the implementation of the PDP Law and its derivative regulations, as well as a reference for legal practitioners, e-commerce business actors, and researchers.

METHOD

The research method used in this study is normative juridical, namely a method that emphasizes the study of applicable positive law and relevant legal doctrine. The legislative approach and the conceptual approach were the methods employed in this investigation. Regulations governing Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), Law No. 8 of 1999 concerning Consumer Protection, and Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions are examples of legislative approaches that examine the protection of consumer privacy rights in e-commerce. Furthermore, a conceptual approach is employed to comprehend the legal principles of safeguarding consumer privacy rights and contrast them with ideas evolving globally, such as the General Data Protection Regulation (GDPR) enacted in the European Union. Both primary and secondary legal resources served as the study's data sources. Laws and rules directly pertaining to the defense of customers' right to privacy in online transactions are considered primary legal resources. Books, scholarly publications, legal papers, and professional views pertinent to privacy protection and e-commerce laws are examples of secondary legal documents. Data analysis was conducted using qualitative normative analysis, which examines and interprets applicable legal regulations and compares them with existing legal theories and concepts. This method allows the research to provide a deeper understanding of the effectiveness of existing regulations in protecting consumer privacy rights in the e-commerce ecosystem. Furthermore, this method also allows for the identification of weaknesses and challenges in the implementation of these regulations and provides policy recommendations to strengthen legal protection for consumer privacy rights in digital transactions.

RESULTS AND DISCUSSION

Regulations Protecting Consumer Privacy Rights in E-Commerce

In Indonesia, the protection of consumer privacy rights in e-commerce is governed by a number of laws designed to guarantee the safety and appropriate use of personal information. Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), which thoroughly governs the rights of data owners, the responsibilities of data controllers, and the procedures for managing and safeguarding personal data, is the main law that supports personal data protection in Indonesia (Rifa, 2024). Additionally, Law No. 8 of 1999 concerning Consumer Protection (Consumer Protection Law) specifies certain features of consumer protection in digital transactions, which affirms consumers' rights to security and convenience in transactions, including the protection of personal information (Tampubolon, 2016). Another regulation supporting privacy protection in e-commerce is Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP PSTE), which stipulates the obligations of electronic system providers in managing user data.

Law No. Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) serves as the primary foundation for regulating the protection of consumer privacy rights, including in the e-commerce ecosystem. Article 4 of the PDP Law explicitly states that every individual has the right to protection of their personal data, including the right to know the purpose of data processing, the right to provide and revoke consent, and the right to object to data processing deemed detrimental. Furthermore, Article 15 stipulates the obligations of data controllers to ensure the security of the personal data they manage and to limit data access and processing to legitimate and transparent purposes only. In the context of e-commerce, this regulation emphasizes that digital service providers must manage user data responsibly and must not misuse it for commercial gain without the data owner's consent.

In addition to the PDP Law, Another important factor in ensuring consumer privacy rights in digital transactions is Law No. 8 of 1999 about Consumer Protection (Consumer Protection Law). Customers have the right to accurate, transparent, and truthful information about products and services, according to Article 4(d), including how their personal data will be used by service providers. Article 6 stipulates the obligations of business actors to treat consumers well, including maintaining the confidentiality of their personal data. Therefore, every e-commerce platform that collects and uses customer data must ensure that it is used in accordance with the principles of transparency and clear consent.

Another regulation that plays a role in protecting consumer privacy rights in e-commerce is Government Regulation No. 71 of 2019 pertaining to Electronic Systems and Transactions Implementation (PP PSTE). Article 14 of the PP PSTE stipulates that electronic system operators are required to ensure the security and protection of users' personal data by implementing an adequate security system. Furthermore, Article 20 states that electronic system operators that manage user personal data must have data protection mechanisms that comply with national and international standards. It aims to prevent the leakage or misuse of personal data in digital transactions.

In addition to the PP PSTE, regulations in the financial and digital trade sectors also contribute to consumer data protection. For example, in the fintech sector, Through POJK No.

12/POJK.03/2021 concerning Consumer Protection in the Financial Services Sector, the Financial Services Authority (OJK) mandates that digital-based financial institutions manage client personal data with caution. However, the Minister of Trade Regulation No. Law No. 50 of 2020 pertaining to Business Licensing, Advertising, Development, and Supervision of Business Actors in Electronic Commerce requires e-commerce businesses to ensure transparent privacy policies for consumers.

With these various regulations, consumer privacy rights in e-commerce have a strong legal basis. These regulations oblige digital service providers to manage personal data securely and responsibly. Furthermore, the right for consumers to control the use of their data reflects legal efforts to protect privacy rights in the digital environment (Kusnadi, 2021).

Overall, regulations in force in Indonesia address various aspects of protecting consumer privacy rights in e-commerce, ranging from individual rights to their personal data, business actors' obligations to maintain data security, to the mechanisms that must be implemented in digital information management. With this regulation, it is hoped that the e-commerce ecosystem can develop more responsibly, where business interests can run in line with the protection of consumer rights in digital transactions (Hasanah, 2024).

Analysis of Challenges and Strategies for Strengthening the Protection of Consumer Privacy Rights in E-Commerce

One of the main challenges in protecting consumer privacy rights in e-commerce is the rampant leakage and misuse of personal data by digital platforms. As the number of online transactions increases, more personal data is collected by e-commerce service providers. However, many of these platforms lack robust security systems to protect user information from cyberattacks or unauthorized access. As a result, data leaks frequently occur, and consumers' personal data can be exploited for various illegitimate purposes, such as fraud, identity theft, or data trading on the black market.

In addition to data leaks, the lack of transparency in the management of personal data by electronic system providers is also a major challenge. Many e-commerce platforms do not provide clear information to consumers regarding how their data is collected, stored, and used. Privacy policies are often written in language that is difficult for lay users to understand, leaving consumers unaware of the risks they face when using digital services. This lack of transparency can lead to data misuse without consumers' knowledge, ultimately harming them in the long run.

Another challenge in protecting consumer privacy rights is the weak enforcement of laws against privacy violations. Although regulations related to personal data protection are in place, their implementation still faces numerous obstacles. Many cases of privacy violations are not firmly prosecuted, giving the impression that businesses can ignore their obligations without significant consequences. The lack of capacity of law enforcement to handle privacy violation cases, along with a suboptimal consumer complaint mechanism, further exacerbates this situation.

In addition to weak law enforcement, challenges in implementing the Personal Data Protection Law and other related regulations are also significant issues. The newly enacted Personal Data Protection Law is still in its early stages of implementation, requiring numerous technical and operational adjustments by both regulators and businesses. There remains uncertainty regarding the oversight and sanction mechanisms that will be implemented, as well as the industry's readiness to adapt its internal policies to the new provisions. This transition process requires significant time and resources, which could hamper the effectiveness of consumer data protection in the near future.

To address these challenges, increased oversight and sanctions against privacy violations by e-commerce platforms need to be strengthened. Authorities should be more proactive in conducting audits and inspections of electronic system providers to ensure they comply with personal data protection standards. Furthermore, strict and binding sanctions must be applied to platforms found to have committed violations, creating a deterrent effect that can encourage businesses to be more careful in managing user data (Milafebina, 2023).

In addition to stricter law enforcement, strengthening personal data protection policies through more specific and stringent regulations is also necessary. While the Personal Data Protection Law (PDP) has become the primary legal basis, more detailed derivative regulations are needed to ensure its effective implementation. Stricter data security standards should be applied to e-commerce platforms, including the requirement to implement encryption, dual authentication systems, and robust data recovery mechanisms to prevent personal data leaks and misuse.

Increasing transparency in the management of personal data by digital platforms is also a crucial strategy in strengthening the protection of consumer privacy rights. E-commerce platforms should provide easier-to-understand privacy policies and ensure that users are given clear choices regarding how their data is used. One way to increase transparency is by providing features that allow consumers to independently access, update, or delete their data. By giving consumers greater control, digital platforms can build stronger trust among their service users.

In addition to the role of regulators and businesses, consumer education regarding their privacy rights and personal data protection is also crucial. Many consumers still don't realize the importance of keeping their personal data secure during digital transactions. Digital literacy programs focused on privacy rights can help people understand the risks and how to protect their information from misuse. This education can be carried out through national campaigns, collaboration with educational institutions, and initiatives from civil society organizations that care about consumers' digital rights (Zahwani, 2024).

CONCLUSION

Consumer privacy rights in e-commerce are a crucial aspect of the ever-evolving digital ecosystem. Personal data protection has become essential to ensuring that consumers can transact safely and securely amid the rise of online transactions, without concern about the misuse of their information. Regulations in Indonesia, such as the Personal Data Protection Law (PDP Law) and other related regulations, have provided a strong legal foundation for protecting consumer privacy rights. However, their implementation continues to face various challenges, including frequent data leaks, a lack of transparency in the management of personal information by electronic system providers, and weak law enforcement against privacy violations. Further efforts are therefore needed to ensure that these regulations are effectively implemented to protect consumer interests in digital transactions. All stakeholders — the government, businesses, and consumers — must participate in building a safer and more responsible digital ecosystem.

Addressing these challenges requires concrete steps involving all relevant parties. The government must strengthen oversight of e-commerce platforms by implementing more rigorous control mechanisms and imposing stricter sanctions for privacy violations. E-commerce providers must enhance transparency in consumer data management by offering clearer and more accessible privacy policies and granting users greater control over their personal data. They must also strengthen security systems to prevent data leaks and misuse. Consumers, meanwhile, have a crucial role in safeguarding their own privacy rights by being more proactive in understanding the privacy policies of the platforms they use and taking preventive measures such as using strong passwords and exercising discretion when sharing personal information. Collaboration among the government, e-commerce platforms, and consumers is expected to further strengthen privacy protection in e-commerce, fostering a safer and more trustworthy digital environment for all parties.

REFERENCES

Charos, W. A., & Nasution, M. I. P. (2023). Perlindungan privasi dan data pribadi konsumen pada e-commerce. *Jurnal Akuntansi Keuangan dan Bisnis, 1*(2), 68–70.

Danuri, M. (2019). Perkembangan dan transformasi teknologi digital. *Jurnal Ilmiah Infokam, 15*(2).

Hasanah, R., Utari, Y. D., & Desvianti, D. (2024). The influence of legal aspects and business ethics on business sustainability in the digital era. *Demagogi: Journal of Social Sciences, Economics and Education, 2*(3), 95–110.

Kurnianingrum, T. P. (2023). Urgensi pelindungan data pribadi konsumen di era ekonomi digital. *Kajian, 25*(3), 197–216.

Kusnadi, S. A. (2021). Perlindungan hukum data pribadi sebagai hak privasi. *AL WASATH Jurnal Ilmu Hukum, 2*(1), 9–16.

Lidya, A. A. M. A. R., Budiartha, I. N. P., & Ujianti, N. M. P. (2020). Pengawasan terhadap transaksi bisnis e-commerce dalam mewujudkan perlindungan konsumen. *Jurnal Konstruksi Hukum, 1*(1), 38–43.

Lisdayanti, A., & Padmanegara, O. H. (2024). Peran teknologi blockchain dalam meningkatkan kepercayaan konsumen dan keamanan data privasi pada platform e-commerce di Indonesia. *Jurnal Manajemen Bisnis dan Keuangan, 5*(2), 347–361.

Milafebina, R., Lesmana, I. P., & Syailendra, M. R. (2023). Perlindungan data pribadi terhadap kebocoran data pelanggan e-commerce di Indonesia. *Jurnal Tana Mana, 4*(1), 157–169.

Patricia, E. (2024). Perlindungan hukum terhadap konsumen dalam e-commerce di Indonesia. *JUDICATUM: Jurnal Dimensi Cakra Hukum, 2*(1), 75–90.

Pohan, T. D., & Nasution, M. I. P. (2023). Perlindungan hukum data pribadi konsumen dalam platform e-commerce. *Sammajiva: Jurnal Penelitian Bisnis dan Manajemen, 1*(3), 42–48.

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.

Priliasari, E. (2023). Perlindungan data pribadi konsumen dalam transaksi e-commerce. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional, 12*(2).

Rahmawati, D., Aksana, M. D. A., & Mukaromah, S. (2023). Privasi dan keamanan data di media sosial: Dampak negatif dan strategi pencegahan. *Prosiding Seminar Nasional Teknologi dan Sistem Informasi, 3*(1), 571–580.

Rifa, F., & Hidayati, M. N. (2024). Kebijakan penal dalam perlindungan data pribadi nasabah fintech lending di Indonesia. *Binamulia Hukum, 13*(2), 461–481.

Sahabuddin, R., Arif, H. M., Lestari, W., Alviolin, E., & Dzaky, M. N. (2024). Transparansi informasi sebagai mediator dalam hubungan etika pemasaran digital dan kepercayaan konsumen di e-commerce. *Maximal Journal: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya dan Pendidikan, 2*(1), 27–37.

Tampubolon, W. S. (2016). Upaya perlindungan hukum bagi konsumen ditinjau dari Undang-Undang Perlindungan Konsumen. *Jurnal Ilmiah Advokasi, 4*(1), 53–61.

Ulum, M. (2020). Prinsip-prinsip jual beli online dalam Islam dan penerapannya pada e-commerce Islam di Indonesia. *Jurnal Dinamika Ekonomi dan Bisnis, 17*(1).

Wariati, A., & Susanti, N. I. (2014). E-commerce dalam perspektif perlindungan konsumen. *ProBank, 1*(1).

Wirapraja, A., & Aribowo, H. (2018). Pemanfaatan e-commerce sebagai solusi inovasi dalam menjaga sustainability bisnis. *Teknika, 7*(1), 66–72.

Zahwani, S. T., & Nasution, M. I. P. (2024). Analisis kesadaran masyarakat terhadap perlindungan data pribadi di era digital. *Journal of Sharia Economics Scholar (JoSES), 2*(2).