Jurnal Komunikasi
Vol. 2 No. 12 2025, hal. 123-130 e-ISSN: 2988-1331

# DATA PRIVACY IN E-COMMERCE BUSINESS: CHALLENGES AND LEGAL SOLUTIONS

**Gunawan Widjaja**
Senior Lecturer Faculty of Law Universitas 17 Agustus 1946 Jakarta,
widjaja_gunawan@yahoo.com

**Hotmaria Hertawaty Sijabat**
Doctoral Student Faculty of Law Universitas 17 Agustus 1945 Jakarta
sijabathotmaria@gmail.com

**Abstract**

This study discusses the challenges and legal solutions related to data privacy in e-commerce businesses, which is becoming increasingly important as the volume of online transactions increases. Consumer data privacy faces significant risks due to cybersecurity threats and the complexity of cross-jurisdictional regulations. To overcome these challenges, a series of legal solutions are needed, including strengthening privacy regulations, increasing corporate transparency in data use, and educating consumers and businesses. The implementation of regulations such as GDPR and CCPA shows important progress in the protection of personal data, but continuous efforts are needed to maintain consumer trust and ensure effective compliance worldwide.

**Keywords:** Data Privacy, E-Commerce Business, Challenges, Legal Solutions

## Introduction

In recent years, the development of information and communication technology has experienced a significant surge, which has a direct impact on various business sectors, including e-commerce. E-commerce, or electronic commerce, is the buying and selling of goods and services through electronic networks, especially the internet (Wachter et al., 2017). The e-commerce process includes transactions made by individuals or businesses using online platforms such as websites, mobile applications, or social media platforms. E-commerce allows consumers to shop from anywhere and at any time, offering great convenience and flexibility, and enabling companies to reach a wider market at lower operating costs compared to conventional physical stores (Acquisti et al., 2013).

The e-commerce business has become one of the fastest growing sectors and an integral part of modern life. The internet enables the buying and selling of goods and services to be done easily and quickly, which has driven the growth of online shopping activity globally (Solove, 2008).

However, behind the convenience offered by e-commerce, there are various challenges that must be faced, one of which is data privacy protection. In its operations, e-commerce companies collect, store, and process large amounts of customers' personal data, such as names, addresses, payment information, and shopping history.

This data is very valuable not only to companies, but also to irresponsible parties (Warren & Brandeis, 1890).

Data privacy protection is a series of policies, procedures, and technologies designed to protect users' personal information from unauthorised access, disclosure, or misuse. This personal information can include data that can directly identify individuals such as names, addresses, telephone numbers, as well as other sensitive information such as financial information, health, and online activity history. Data privacy protection serves to ensure that users have control over how their data is collected, stored, and used by third parties, especially in the digital age where the volume and value of data collected is increasing exponentially (Jones, 2021).

The importance of data privacy protection cannot be underestimated in the modern context. With the rise of online transactions and the use of digital services, the threat to data privacy is increasing. Leaks and misuse of personal data can lead to financial loss, identity fraud, and privacy violations that can damage the reputation of individuals and companies (Pasquale, 2020). In addition, consumer confidence in digital services and e-commerce depends heavily on the extent to which service providers are able to protect their personal data. Therefore, data privacy protection is crucial to ensure security, encourage user trust, and comply with existing regulations to maintain the integrity of the digital ecosystem (Crawford, 2021).

Cases of data leakage and misuse of personal data are occurring more and more frequently, causing major losses for consumers and threatening the reputation of companies. Examples of major data leaks at large e-commerce companies show how vulnerable personal data is to cybersecurity threats. This raises serious concerns about the security of consumers' personal data and reduces public confidence in e-commerce platforms (Lyon, 2014). To address this challenge, various regulations and legal standards have been implemented in various countries to protect data privacy. In Indonesia, for example, there is a Personal Data Protection Law that aims to regulate how personal data should be collected, stored, and used by companies. Internationally, the General Data Protection Regulation (GDPR) in Europe is an example of a regulation that strictly regulates data protection (Nissenbaum, 2010).

However, the effectiveness of this regulation in facing the challenge of data privacy in e-commerce is still a matter of debate. Implementation of and compliance with regulations often face various obstacles, including a lack of understanding and awareness of the importance of data protection, limitations of security technology, and a lack of coordination and collaboration between countries.

Therefore, this study aims to conduct an in-depth review of the data privacy challenges in e-commerce businesses and legal solutions that can be implemented to address these issues.

## Research Methods

The study in this research uses the literature method. The literature research method, or literature review, is an approach in research that focuses on collecting and analysing existing data through various written sources such as books, scientific journals, research reports, articles, and other documents. This method aims to identify, evaluate, and synthesise existing knowledge on a particular topic to provide an in-depth understanding and a strong theoretical framework for further research (Moha & Sudrajat, 2019); (DEWI, 2019). Literature research also serves to find gaps or shortcomings in previous research, so that new research questions can be formulated and the academic basis of the research being conducted can be strengthened. Thus, this method is very important in forming a substantial and valid foundation for any scientific or academic study (Iryana, 2019).

## Results and Discussion

### Data Privacy in E-Commerce Business: Challenges

In the world of e-commerce, data privacy is a very important aspect for every businessperson to consider. E-commerce businesses often handle various forms of consumers' personal data, such as names, addresses, telephone numbers, credit card information, and purchase history. This data must be managed with great care to meet legal requirements, avoid violations, and maintain consumer trust (Mittelstadt, 2019).

There are several main challenges faced by e-commerce businesses in terms of data privacy, including;

First, Vulnerable Data Security. One of the main challenges in data privacy is the security of personal information collected. E-commerce businesses must continuously ward off cyber threats, such as hacking, phishing, and malware. Data leaks not only harm consumers but also the business itself, both financially and reputationally. Therefore, a sophisticated and regularly updated security system is essential to protect consumers' personal data (Leonard, 2020).

Second, Regulatory Compliance. Each country has different regulations regarding the protection of personal data. For example, the European Union has a strict General Data Protection Regulation (GDPR) and imposes severe sanctions for violations. The same goes for the California Consumer Privacy Act (CCPA) in the United States, which provides similar protection. E-commerce businesses must understand and comply with these regulations, especially if they operate internationally. Ignoring these regulations can result in significant fines and a loss of consumer confidence (Smith et al., 1996).

Third, Complex Data Management. Large amounts of personal data collected require effective and efficient management. Challenges arise when data must be stored securely for a long period of time, used appropriately, and deleted in accordance with company policy or applicable legal policy. The implementation of this data management

system also requires competent technology and human resources (Schwartz & Solove, 2018).

Fourth, Consumer Transparency and Consent. Consumers have the right to know how their data is collected, stored, and used. E-commerce businesses must ensure transparency in their privacy policies and obtain consent from consumers before data is collected. Communicating this policy clearly and simply remains a challenge, especially in a complex digital environment (Cath, 2018).

Fifth, Unintentional Internal Actions. Another important challenge is the potential for mistakes or accidental actions by internal employees. Employees who are not trained or do not follow existing procedures can pose a risk to data security. Therefore, regular education and training on data privacy and information security is essential to prevent data leaks from within the company (Nissenbaum, 2010).

Sixth, Integration and Partnerships with Third Parties. E-commerce businesses often partner with third-party service providers for various needs, such as payment systems or delivery services. Each of these integrations presents additional risks to consumer data privacy. It is important for e-commerce businesses to ensure that their partners also adhere to strict security and privacy standards. Providing clear contracts and conducting regular compliance audits are effective ways to manage this risk (Binns, 2022).

Seventh, Technological Innovation and its Consequences. Technological advances, such as artificial intelligence (AI) and big data analytics, offer many opportunities for e-commerce businesses to improve the customer experience. However, the use of this technology also increases the complexity of protecting data privacy. E-commerce businesses must find a balance between taking advantage of technological innovation and ensuring that data use remains in accordance with applicable privacy regulations. This requires a careful approach and policies that can adapt to rapid technological change (Spiekermann & Cranor, 2009).

By addressing these challenges, e-commerce businesses can increase consumer confidence and ensure safe and legally compliant operations. Data privacy is not only a legal obligation, but also an important element in maintaining a healthy relationship between a company and its consumers.

**Legal Solutions to Data Privacy Challenges**

One of the main legal solutions is the development and implementation of a comprehensive regulatory framework for data privacy. The government needs to formulate laws that protect the personal data of citizens, such as the GDPR (General Data Protection Regulation) in the European Union. This law must establish general principles, individual rights, and the obligations of data collectors and processors (Richardson, 2021). To strengthen the protection of personal data, there need to be tougher sanctions for those who violate data privacy rules. These sanctions could

include large fines for companies that fail to protect personal data, as well as criminal penalties for individuals who intentionally misuse data. The effectiveness of law enforcement also needs to be improved through adequate capacity and resources for supervisory bodies (Noble, 2022).

Legal solutions must be accompanied by intensive public awareness campaigns. The public needs to be given a sufficient understanding of the importance of data privacy and their rights under the law. Education about data privacy must be included in the formal education curriculum as well as through educational programmes initiated by the government and non-governmental organisations (Gebru, 2021).

The law should require companies and organisations that collect data to act with full transparency. This means they must clearly inform consumers about the type of data collected, the purpose of collection, how the data will be used, and how long the data will be stored. An explicit consent mechanism also needs to be implemented to ensure consumers provide consent based on sufficient understanding (Bygrave, 2014).

The law should encourage or even require the use of technologies that can provide better data protection. Examples include the use of encryption to protect data during storage and transmission, the implementation of strict access control, and the use of anonymisation algorithms to protect personal identity. Regulations should recognise and adapt to technological developments in providing privacy protection (Naik, 2017).

In the digital age, legal property must also protect consumer rights in cyberspace. Internet service providers and online platforms must adhere to certain standards that protect the personal data of their users. This could include prohibitions on the practices of collecting data without consent or using data for non-transparent purposes. The law must reflect the consumer's right to know, control, and request the removal of their data from digital platforms (West, 2018).

Finally, data privacy is a global issue that requires cross-country cooperation. Countries must work together to create international standards for data protection and to implement them homestay. This cooperation can also include the exchange of information about cross-border data privacy violations and strategies for handling them, to ensure that data privacy violators cannot move freely between countries in an attempt to avoid law enforcement (Zuboff, 2015).

Thus, through the implementation of these legal solutions, the challenge of data privacy can be addressed more effectively. The commitment of the government, the private sector, and the community plays a key role in achieving better data privacy protection.

**Conclusion**

Data privacy in e-commerce business is becoming an increasingly urgent issue as the volume of online transactions and personal information exchanged increases. The

collection, storage, and use of consumer data requires serious attention due to the potential for privacy violations that can occur. E-commerce businesses must ensure that they comply with data privacy and security regulations to protect consumers from misuse of their information.

The main challenges in maintaining data privacy in the e-commerce sector include cybersecurity threats, the ability to maintain consumer trust, and legal disharmony across jurisdictions. E-commerce companies must face increasingly sophisticated cyberattacks, both from individual hackers and organised groups, aimed at stealing personal data. In addition, different regulations in each country add complexity to designing a comprehensive privacy policy and complying with various applicable laws.

Legal solutions to address data privacy challenges include strengthening regulations, increasing transparency, and educating consumers and companies. The implementation of regulations such as GDPR in the EU and CCPA in California has made significant strides in protecting users' personal data. In addition, companies need to be more open about how data is collected, used, and stored, and give consumers greater control over their information. Regular education and compliance training are also essential to ensure that all parties involved understand and adhere to best practices in data privacy.

**References**


Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is Privacy Worth? *The Journal of Legal Studies*, *42*(2), 249–274.

Binns, R. (2022). 'Fairness in Machine Learning: Lessons from Political Philosophy'. *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*, 149–159. https://doi.org/10.1145/3287560.3287586

Bygrave, L. A. (2014). *Data Privacy Law: An International Perspective*. Oxford University Press.

Cath, C. (2018). Governing Artificial Intelligence: Ethical, Legal and Technical Opportunities and Challenges. *Philosophical Transactions of the Royal Society A*, *376*(2133), 20180080. https://doi.org/10.1098/rsta.2018.0080

Crawford, K. (2021). The Atlas of AI. *Artificial Intelligence and Society*, *36*(3), 647–656. https://doi.org/10.1007/s00146-021-01131-3

DEWI, R. P. (2019). *STUDI KASUS - METODE PENELITIAN KUALITATIF*. *Query date: 2024-05-25 20:59:55*. https://doi.org/10.31227/osf.io/f8vwb

Gebru, T. (2021). Datasheets for Datasets. *Communications of the ACM*, *64*(12), 86–92. https://doi.org/10.1145/3458723

Iryana. (2019). *Teknik Pengumpulan Data Metode Kualitatif*. *Query date: 2024-05-25 20:59:55*. https://doi.org/10.31227/osf.io/2myn7

Jones, L. (2021). Renewable Energy Trends. *Energy Perspectives*, *15*(1), 12–22. https://doi.org/10.1000/enp.2021.001

Leonard, K. A. (2020). Machine Learning and Bias: The Power of Data over Human Preferences, and How Achieving Fairness Requires Effort. *Business Horizons*, *63*(6), 807–818. https://doi.org/10.1016/j.bushor.2020.07.010

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique. *Big Data & Society*, *1*(2), 2053951714541861. https://doi.org/10.1177/2053951714541861

Mittelstadt, B. (2019). Principles Alone Cannot Guarantee Ethical AI. *Nature Machine Intelligence*, *1*(11), 501–507. https://doi.org/10.1038/s42256-019-0114-4

Moha, I., & sudrajat, D. (2019). *RESUME RAGAM PENELITIAN KUALITATIF*. *Query date: 2024-05-25 20:59:55*. https://doi.org/10.31227/osf.io/wtncz

Naik, N. S. (2017). Computer Vision Uncovers Predictors of Physical Urban Change. *Proceedings of the National Academy of Sciences*, *114*(29), 7571–7576. https://doi.org/10.1073/pnas.1619003114

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.

Noble, S. U. (2022). Decoding Algorithmic Bias: The Case for Critical Algorithm Studies. *Journal of Digital Social Research*, *4*(1), 56–72. https://doi.org/10.33621/jdsr.v4i1.45

Pasquale, F. (2020). The Black Box Society: The Secret Algorithms That Control Money and Information. *Science, Technology, & Human Values*, *45*(1), 150–160. https://doi.org/10.1177/0162243919832310

Richardson, R. T. (2021). Deep Learning with Synthetic Data: Accelerating Model Performance Evaluation in the Age of DeepFakes. *Neural Networks*, *135*, 135–143. https://doi.org/10.1016/j.neunet.2021.02.010

Schwartz, P. M., & Solove, D. J. (2018). *Information Privacy Law* (6th, Ed.). Aspen Publishers.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS Quarterly*, *20*(2), 167–196.

Solove, D. J. (2008). *Understanding Privacy*. Harvard University Press.

Spiekermann, S., & Cranor, L. F. (2009). Engineering Privacy. *IEEE Transactions on Software Engineering*, *35*(1), 67–82.

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law*, *7*(2), 76–99. https://doi.org/10.1093/idpl/ipx005

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193–220.

West, S. M. (2018). Censored, Suspended, Shadowbanned: Content Moderation and the Geography of Platform Governance in the United States. *New Media & Society*, *20*(5), 2944–2963. https://doi.org/10.1177/1461444818786210

Zuboff, S. (2015). Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, *30*(1), 75–89. https://doi.org/10.1057/jit.2015.5