IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.1. No.10, December 2024
DOI : https://doi.org/10.62872/rc7s4723

Legal Aspects Related To Information Security In E-Commerce

Darmawan Sutawijaya
Faculty of Law Universitas Pembangunan Nasional "Veteran" Jakarta, Jakarta, Indonesia

Received: November 12, 2024
Revised: December 12, 2024
Accepted: December 20, 2024
Published: December 30, 2024

Corresponding Author:
Author Name*: Darmawan Sutawijaya
Email*: darmawan.sutawijaya@upnvj.ac.id

***Abstrak*:** *Legal protection concerning information security and personal data in Indonesia continues to evolve. While regulations such as the Electronic Information and Transactions Law (UU ITE) and Personal Data Protection regulations exist, their enforcement and effectiveness are still limited. Weak law enforcement, coupled with low public awareness, pose significant challenges to protecting e-commerce consumers. Additionally, the rapid advancement of technology often outpaces regulatory adjustments, creating a gap in ensuring comprehensive information security. This study employs a normative legal method, utilizing secondary data analysis from legal documents and relevant literature. The findings indicate that while a solid legal framework is in place, the implementation remains insufficient. To address this, adaptive regulatory updates, increased supervision, and enhanced law enforcement are imperative. Furthermore, collaboration between the government, industry stakeholders, civil society, and educational initiatives are crucial in promoting consumer awareness and safeguarding personal data. This holistic approach aims to strengthen legal protection for information security in the e-commerce sector, fostering a safer and more secure digital environment..*

Keywords : Consumer Protection, E-Commerce, Security

INTRODUCTION

The world economy is developing rapidly through the flow of globalization and free trade, as well as advances in technology, communication, and information that have expanded the space for transactions of goods and services. Amid increasingly integrated communication globalization, the internet has become a popular media, making the world smaller while fading national borders and their sovereignty and social order. Information technology in Indonesia is developing very rapidly, according to a survey conducted by the Indonesian Internet Service Providers Association (APJII). In 2024, internet users in Indonesia will have 221 million, or equivalent to 79.5%. Technological advances have brought about rapid changes and shifts in life without boundaries in this era of globalization.

The advancement of digital technology has significantly impacted various aspects of life, including in the economic sector. E-commerce or electronic commerce is one of the objective manifestations of modern economic transformation, where transactions can be carried out quickly and easily through digital platforms (Marhawati et.al., 2023). Ease of access, speed of transactions, and the ability to reach a broad market make e-commerce a rapidly growing sector. In Indonesia, e-commerce has become an essential part of the economy, with the number of users increasing every year along with the development of information technology. Although e-commerce proliferates, this progress presents new challenges, especially regarding information security. Every e-commerce transaction involves the users' personal data and financial information that need to be protected from being misused by irresponsible parties. Personal data and sensitive information collected on e-commerce platforms are vulnerable to various threats, such as data

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.1. No.10, December 2024
DOI : https://doi.org/10.62872/rc7s4723

theft, hacking, and information manipulation. These security threats not only harm consumers but can also undermine public trust in e-commerce services.

Information security breaches involving e-commerce companies are increasingly common in various countries, including Indonesia. Several incidents of user data leaks even involve large amounts of data that unauthorized parties can access. This phenomenon raises concerns about how the legal aspect can protect users' data and ensure that e-commerce platforms are responsible for the security of the information. This shows the need for solid legal regulations to address information security challenges in the e-commerce sector. Legal protection for information security and personal data in Indonesia is still being developed. Although several regulations are aimed at protecting user data, such as the Electronic Information and Transactions Law (ITE) and the Government Regulation on Personal Data Protection, their implementation often needs to be revised. Weaknesses in law enforcement and low awareness of the importance of information security are the main obstacles to protecting e-commerce consumers in Indonesia. In addition, technology's rapid development often differs from changes in existing regulations. Legal policies related to information security in e-commerce need to catch up to the technology used by industry players. This condition creates legal loopholes that can be exploited by certain parties to commit violations of information security. Therefore, more dynamic regulations are needed to keep up with the rapid progress of information technology.

The responsibility of e-commerce service providers to protect user data is also an essential factor in information security. E-commerce service providers play a significant role in protecting users' data through strict privacy policies and adequate protection technology. However, not all service providers have a strong enough system to secure user data, increasing the risk of data leaks that could harm consumers. From a consumer perspective, information security is one of the key factors influencing their trust in e-commerce platforms. Consumers who feel their data could be more secure tend to be careful or even leave the platform. Therefore, legal certainty in protecting the security of users' data provides a sense of security for consumers and supports the growth of the e-commerce sector itself. Clear and compelling legal regulations will build public trust in e-commerce platforms.[1]

In addition, consumer awareness of their rights related to information security still needs to be improved. Many consumers must fully understand how their data is used or how to protect it. This is a challenge in itself in efforts to maintain information security in the e-commerce sector. To increase this awareness, education, and socialization are needed involving various parties, such as the government, service providers, and community organizations. Based on the background above, the author would like to discuss how legal regulations in Indonesia protect information security in e-commerce transactions and what legal strategies effectively increase information security protection in the e-commerce sector.

METHODOLOGY

The research method is a way that must be taken to find the right answer or find the truth to answer the questions to be analyzed. The research approach used in this study is the normative legal approach method, which uses legal research based on secondary data sources. Where legal research has emphasized the study of legal documents and library materials that are related to the main issues.

[1] Salim H.S, *Hukum Kontrak Teori dan Teknik Penyusunan Kontrak,* Sinar Grafika, Jakarta, 2003, Page 49

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.1. No.10, December 2024
DOI : https://doi.org/10.62872/rc7s4723

RESULTS AND DISCUSSION

One of the factors influencing the development of contract law in Indonesia is progress in the field of trade. Buying and selling transactions are generally included in the agreements regulated in Book III of the Civil Code. This agreement is classified as an actual agreement, namely an agreement only considered to have occurred when the goods that are the object of the agreement have been delivered. The Internet has made it easier for consumers to find goods and services. The benefits of the Internet indirectly impact increasing trade competition and more affordable prices, with various product and service choices and the ease of shopping from various providers worldwide, anytime and anywhere. E-commerce has become an essential element for the economies of developing countries.

Electronic transactions, which are also sales and purchase transactions, indeed involve an agreement. However, agreements in e-commerce are different from conventional agreements; transactions can occur without a physical meeting between the two parties because the agreement is made electronically. This electronic transaction is stated as an electronic contract, which binds both parties. Electronic contracts are a form of automation in forming contracts and apply to online transactions. The application of electronic contracts aims to reduce costs, save time, and simplify the complexity that often occurs in physical contracts. Agreements in e-commerce transactions are still guided by Article 1320 of the Civil Code. This article states that an agreement must meet the legal requirements to be considered binding on both parties. The requirements for the validity of an agreement include subjective and objective requirements.[2]

Subjective requirements[3]:

1. There is an agreement between both parties to remind themselves;
2. Capable of agreeing:

Objective requirements:

1. Regarding a particular matter;
2. A lawful cause.

The provisions regarding electronic contracts are regulated in Article 18, which states that an electronic commerce contract is valid if there is an agreement between the parties. Electronic transactions stated in an electronic contract are binding on the parties. An electronic commerce contract must at least include the identities of the parties, specifications of the agreed goods or services, the legality of the goods or services, transaction value, terms, and payment terms, procedures for delivery of goods or services, and return procedures if there is a discrepancy. Electronic commerce contracts can also use electronic signatures and must be prepared in Indonesian.[4]

Consumer personal data protection in e-commerce transactions is a critical issue in today's era of technological advancement. E-commerce has changed the way we conduct transactions by enabling the exchange of goods, services, and information online via the Internet. However, along with the growth of e-commerce, concerns have arisen regarding the privacy and security of personal data. Information such as name, address, telephone number, and financial details are valuable data and are at risk of being misused if

[2] Nanin Koeswidi Astuti and Robertus Nugroho Perwiro Atmojo, Perlindungan Konsumen Atas Risiko Keamanan Informasi Dalam Transaksi E-Commerce, *Honeste Vivere*, Vol. 32 No. 2, 2022, Page 98-107

[3] Dinda Dinanti and Yuliana Yuli Wahyuningsih, Perlindungan Hukum Atas Hak-Hak Tersangka Pada Proses Penyidikan Perkara Pidana Dalam Perspekti Hak Asasi Manusia, *Jurnal Yuridis*, Vol. 3 No. 2, 2016, Page 89-98

[4] Ahmadi Miru, *Hukum Kontrak dan Perancangan Kontrak*, PT. Raja Grafindo Persada, Jakarta, 2007, Page 127

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.1. No.10, December 2024
DOI : https://doi.org/10.62872/rc7s4723

they fall into the hands of unauthorized parties. Therefore, clear and firm legal protection is needed to ensure the security of consumers' data. Regulations governing the protection of personal data in e-commerce transactions aim to protect consumers from the risk of data misuse, personal information breaches, and privacy violations. This law covers various aspects, including data security, user consent, the responsibility of electronic system providers, and legal sanctions for violations of personal data protection. Many countries, including Indonesia, have passed laws governing personal data protection in the context of e-commerce. These laws give consumers the right to control their data, set security requirements for e-commerce service providers, and impose sanctions for privacy and data security violations.[5]

Indonesia provides constitutional protection for citizens' data through Article 28G Paragraph (1) of the 1945 Constitution. This article affirms the individual's right to protect themselves, their family, honor, dignity, and property under their control. In addition, the article also guarantees security and protection from threats when exercising fundamental rights. The Constitutional Court (MK) has analyzed this article about privacy and related rights in Decision Number 20/PUU-XIV/2016. In the context of personal data protection, there are two commonly used methods: securing the physical aspects of personal data and implementing regulations to ensure privacy. More than 107 countries have passed personal data protection laws at the regulatory level. With solid legal protection, consumers will feel safer and more confident when conducting e-commerce transactions. They have the right to know how their data is used and to ensure its confidentiality. However, it is essential to remember that technology constantly evolves, so legal protection must be updated and adjusted periodically. In addition, consumer awareness and education regarding personal data protection are crucial factors in maintaining information security in e-commerce.[6]

Legal Regulations in Indonesia in Protecting Information Security in E-Commerce Transactions

The rules for protecting consumer personal data in e-commerce transactions include several essential aspects that must be considered. The following are the main points:[7]

1. Privacy Policy: Every e-commerce platform or site must have a transparent privacy policy that clearly explains how consumers' personal data is collected, used, and protected.
2. Consumer Consent: Consumers must provide voluntary consent before the e-commerce platform collects and uses their data. This consent must be given with a complete understanding of the purpose of using their data.
3. Data Security: E-commerce platforms must implement adequate security measures to protect consumers' data from unauthorized access, use, or disclosure. This includes implementing encryption, network protection, and other security measures.
4. Data Deletion: Consumers can delete their data from the e-commerce system. E-commerce platforms need to provide a mechanism for consumers to easily submit a request for data deletion.
5. Data Sharing: If consumers' data is to be provided to third parties, the e-commerce platform must provide a clear explanation and obtain the consumer's consent first. Consumers should also be informed about the recipients of the data and the purpose for which it is shared.

[5] Dinda Dinanti and Muthia Sakti, Aspek Yuridis Jua Beli Surat Keterangan Sakit melalui E-Commerce, *Jurnal Ilmiah Penegakan Hukum*, Vol. 7 No. 1, 2020, Page 62-68

[6] RR Dewi Anggraeni and Acep Heri Rizal, Pelaksanaan Perjanjian Jual Beli Melalui Internet (E-Commerce) Ditinjau Dari Aspek Hukum Perdataan, *Salam: Jurnal Sosial Dan Budaya Syar-i*, Vol. 6 No. 3, 2019, Page 223-238

[7] Mieke Komar Kantaatmadja, *Cyberlaw*, Elips, Jakarta, 2002, Page 2

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.1. No.10, December 2024
DOI : https://doi.org/10.62872/rc7s4723

6. Supervision and Enforcement: Governments and authorities should strictly supervise personal data protection practices in e-commerce and apply strict sanctions to e-commerce platforms that commit violations.

Legal regulations in Indonesia to protect information security in e-commerce transactions have made significant progress, but they still need help. Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE) and Law No. 27 of 2022 concerning Personal Data Protection are the primary basis for data and information security regulations in the digital realm. Both laws include provisions on sanctions for violations involving misuse of electronic data and protection of consumer personal data. In addition, Government Regulation No. 82 of 2012 concerning the Implementation of Electronic Systems and Transactions stipulates the responsibilities of electronic system providers, including the obligation to secure data and handle incidents that threaten information security. However, the rapid development of technology often creates legal loopholes that need to be fully accommodated in existing regulations. In practice, law enforcement for data security violations still needs to be improved by weak oversight mechanisms and low public understanding of their privacy rights. Therefore, cooperation is needed between the government, e-commerce industry players, and consumers to strengthen regulations and increase data security awareness. Dynamic regulatory updates that align with technological advances are expected to strengthen personal data protection and increase public trust in e-commerce services.[8]

In Indonesia, legal regulations related to information security in e-commerce transactions are increasingly essential, along with the rapid growth of this sector. One of the principal regulations supporting electronic transactions' security is Law No. 11 of 2008 concerning Information and Electronic Transactions (ITE). The ITE Law acts as a legal basis that covers various aspects of electronic transactions, including information protection. In this law, the provisions on sanctions for violations of electronic information aim to protect users from data misuse and unauthorized transactions. With the ITE Law, it is hoped that e-commerce actors can operate according to the rules, minimizing information security risks. In addition, Government Regulation No. 82 of 2012 concerning the Implementation of Electronic Systems and Transactions also plays a vital role in information security, regulating the responsibilities of electronic system organizers regarding the obligation to protect user data and information. Organizers must implement data leakage prevention measures and handle security incidents effectively. This regulation aims to encourage e-commerce organizers to strengthen their information security systems to reduce threats to user data.[9]

Furthermore, Law No. 27 of 2022 concerning Personal Data Protection introduces comprehensive protection for citizens' data, especially in e-commerce. This law regulates personal data collection, use, and storage and gives individuals the right to access and control their data. With more robust legal protection, consumers can feel safer in transacting on e-commerce platforms, driving the growth of this sector.

However, even though regulations have been drafted, their implementation in the field still faces various challenges.[10] Weak law enforcement and low public awareness of the importance of data protection are

[8] Tasya Safiranita Ramli and et.all, Aspek Hukum Platform E-Commerce Dalam Era Transformasi Digital, *Jurnal Studi Komunikasi Dan Media*, Vol. 24 No. 2, 2020, Page 119-136

[9] Yudi Anton Rikmadani, *Hukum Telematika Dasar-Dasar Aspek Perdata dan Aspek Pidana*, Mujahid Press, Bandung, 2018, Page 11

[10] O.C. Kaligis, Penerapan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Dalam Prakteknya, Yarsif Watampone, Jakarta, 2012, Page 53-54

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.1. No.10, December 2024
DOI : https://doi.org/10.62872/rc7s4723

obstacles to maintaining information security. Many security breaches need to be followed up seriously, causing consumers to be reluctant to transact on e-commerce platforms. Therefore, increasing public awareness and more effective law enforcement are needed in addition to strengthening regulations. Overall, legal regulations in Indonesia regarding information security in e-commerce transactions have begun to form but still require improvements in implementation and enforcement. Strengthening regulations, increasing public awareness, and building collaboration between the government, industry players, and the community are expected to improve information security in e-commerce transactions, thereby creating better consumer trust and protection.[11]

Effective Legal Strategies in Enhancing Information Security Protection in the E-Commerce Sector

The discussion on effective legal strategies to improve information security protection in the e-commerce sector covers various aspects, from legal policies to the involvement of industry players and public awareness. ***First,*** the right legal strategy requires flexible regulations that can adapt to the development of digital technology and the ever-changing patterns of online transactions. The rapid innovation of technology demands that e-commerce regulations can anticipate new data security risks. In Indonesia, improving the ITE and Personal Data Protection Law can strengthen consumer protection by adjusting regulations to emerging risks. ***Second***, strengthening the supervision mechanism and law enforcement is essential to an effective legal strategy. The government must set strict sanctions for data security violations and strengthen the institutions responsible for supervising the e-commerce sector. Consistent law enforcement will increase trust in regulations, encouraging industry players to be more responsible in protecting user information. Strict supervision by the government will also create a deterrent effect for violators so that the risk of misuse of personal data can be minimized. ***Third***, the importance of collaboration between the government, industry players, and the public to strengthen information security in e-commerce. Industry players must comply with information security standards in the regulations and ensure that their data protection technology is constantly updated. Meanwhile, the government can guide the implementation of appropriate security technology for e-commerce players. This collaboration will build a safer and more protected e-commerce ecosystem.[12]

In addition, increasing consumer awareness of their rights to personal data protection is also an essential part of an effective legal strategy. Consumers need to be educated about the importance of information security and the steps that can be taken to protect their data. Public awareness campaigns, regulatory socialization, and digital education can strengthen the role of consumers in maintaining information security and supporting existing regulations. With a legal strategy that involves regulatory updates, consistent law enforcement, cooperation between stakeholders, and increasing consumer awareness, information security protection in the e-commerce sector can be more effective. This comprehensive approach will strengthen the legal system and create a safer e-commerce environment, increasing consumer confidence in online transactions.[13]

[11] Josua, Sitompul, *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*, PT. Tatanusa, Jakarta, 2012, Page 26-27

[12] Dinda Dinanti and Dwi Desi Yayi Tarina, The Punishment of Perpetrators of Corruption with the Approach of the Local Wisdom (Businesses Looking for Alternative Model of Criminal in Indonesia), *International Journal of Multicultural and Multireligious Understanding,* Vol. 6 No. 7, 2019, Page 32-44

[13] Sarif Hidayat, Hari Suryantoro and Jansen Wiratama, Pengaruh Media Sosial Facebook Terhadap Perkembangan E-Commerce Di Indonesia, *Jurnal Simetris,* Vol. 8 No. 2, 2017, Page 415-420

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.1. No.10, December 2024
DOI : https://doi.org/10.62872/rc7s4723

CONCLUSIONS

The conclusion of the discussion on legal regulations in Indonesia in protecting information security in e-commerce transactions and effective legal strategies to improve information security protection in this sector shows that although Indonesia already has an adequate legal framework, such as the ITE Law, the Personal Data Protection Law, and other related regulations, challenges in its implementation remain. Existing regulations must be continuously updated to adapt to technological developments and address ever-changing security risks. In addition, an effective legal strategy must include adaptive regulatory updates, improved oversight and enforcement mechanisms, and close cooperation between the government, industry players, and the community. Consumer education and awareness also play an essential role in strengthening information security protection. With a comprehensive approach that includes strong regulations, effective law enforcement, and active involvement of all parties, information security protection in the e-commerce sector can be improved, creating a safer and more trusted digital ecosystem.

REFERENCES

Book

Kaligis, O.C. Penerapan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Dalam Prakteknya. Jakarta: Yarsif Watampone, 2012.

Kantaatmadja, Mieke Komar. Cyberlaw. Jakarta: Elips. 2002.

Miru, Ahmadi. Hukum Kontrak dan Perancangan Kontrak. Jakarta: PT. Raja Grafindo Persada. Jakarta. 2007.

Rikmadani, Yudi Anton. Hukum Telematika Dasar-Dasar Aspek Perdata dan Aspek Pidana. Bandung: Mujahid Press. 2018.

S.H, Salim. Hukum Kontrak Teori dan Teknik Penyusunan Kontrak, Jakarta: Sinar Grafika. Jakarta. 2003.

Sitompul, Josua. Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana. Jakarta: PT. Tatanusa. 2012.

Journal Article

Anggraeni, RR Dewi and Acep Heri Rizal. "Pelaksanaan Perjanjian Jual Beli Melalui Internet (E-Commerce) Ditinjau Dari Aspek Hukum Perdataan." Salam: Jurnal Sosial Dan Budaya Syar-i, Vol. 6 No. 3 (2019): 223-238. doi: http://dx.doi.org/10.15408/sjsbs.v6i3.11531

Astuti, Nanin Koeswidi and Robertus Nugroho Perwiro Atmojo. "Perlindungan Konsumen Atas Risiko Keamanan Informasi Dalam Transaksi E-Commerce." Honeste Vivere, Vol. 32 No. 2 (2022): 98-107. doi: https://doi.org/10.55809/hv.v32i2.135

Dinanti, Dinda and Yuliana Yuli Wahyuningsih. "Perlindungan Hukum Atas Hak-Hak Tersangka Pada Proses Penyidikan Perkara Pidana Dalam Perspektif Hak Asasi Manusia". Jurnal Yuridis, Vol. 3 No. 2 (2016): 89-98. doi: https://doi.org/10.35586/.v3i2.181

Dinanti, Dinda and Dwi Desi Yayi Tarina. "The Punishment of Perpetrators of Corruption with the Approach of the Local Wisdom (Businesses Looking for Alternative Model of Criminal in Indonesia)". International Journal of Multicultural and Multireligious Understanding, Vol. 6 No. 7 (2019): 32-44. doi: https://ijmmu.com/index.php/ijmmu/article/download/588/391

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.1. No.10, December 2024
DOI : https://doi.org/10.62872/rc7s4723

Dinanti, Dinda and Muthia Sakti. "Aspek Yuridis Jua Beli Surat Keterangan Sakit melalui E-Commerce". Jurnal Ilmiah Penegakan Hukum, Vol. 7 No. 1 (2020): 62-68. doi: https://doi.org/10.31289/jiph.v7i1.3719

Hidayat, Sarif, Hari Suryantoro and Jansen Wiratama. "Pengaruh Media Sosial Facebook Terhadap Perkembangan E-Commerce Di Indonesia." Jurnal Simetris, Vol. 8 No. 2 (2017): 415-420. doi: https://doi.org/10.24176/simet.v8i2.1165

Marhawati, M., Azizah, A., Erwina, E., & Raflianto, R. (2023). E-commerce dan startup: Wujud inovasi keberlanjutan bisnis di era industri 4.0. *Journal of Economics, Entrepreneurship, Management Business and Accounting*, *1*(1), 34-40.

Ramli, Tasya Safiranita and et.all. "Aspek Hukum Platform E-Commerce Dalam Era Transformasi Digital." Jurnal Studi Komunikasi Dan Media, Vol. 24 No. 2 (2020): 119-136. doi: https://doi.org/10.31445/jskm.2020.3295