Law Synergy Conference (LSC)
Volume I; Number I; Month 6, Year 2024; Pages 247-254
Website:https://sinergilp.com
E-ISSN: 3048-3530

Legal Challenges in Electronic Transactions and E-Commerce

Zulkarnain P[1], T. Riza Zarzani[2].
zulpasaribu12@gmail.com rizazarzani@dosen.pancabudi.ac.id
Panca Budi Development University

Abstract

This study examines the legal challenges that arise in electronic transactions and e-commerce in Indonesia, with a focus on consumer protection and the validity of electronic evidence in legal disputes. Although Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) and Law Number 8 of 1999 concerning Consumer Protection have provided a significant legal basis, their implementation still faces various obstacles. Consumer protection in electronic transactions is faced with issues such as personal data protection, the responsibility of e-commerce organizers, and effective dispute resolution. On the other hand, the validity of electronic evidence is often questioned, especially regarding authentication, system reliability, and the admissibility of evidence in court. Through normative legal analysis, this study identifies legal gaps and provides recommendations to strengthen regulations and improve legal protection in electronic transactions in Indonesia. It is hoped that this study can contribute to the development of laws that are adaptive to the development of digital technology, so that a safer, fairer, and more sustainable e-commerce ecosystem is created.

Keywords: *Electronic Transactions, Consumer Protection, Electronic Evidence*

INTRODUCTION

In recent decades, the development of information and communication technology has drastically changed the global business landscape. One of the most significant changes is the emergence of electronic transactions and electronic commerce (e-commerce) which are now an integral part of everyday life. E-commerce allows consumers and businesses to conduct transactions efficiently and effectively without time and space constraints. In Indonesia, the growth of e-commerce has increased rapidly, in line with the increasing internet penetration and adoption of digital technology.(Santy 2023)

However, this rapid development also brings various legal challenges that must be faced by the Indonesian legal system. Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) is the main legal basis governing electronic transactions in Indonesia. Although the ITE Law has provided a legal basis for electronic transactions, there are still various problems and challenges that need to be overcome to ensure that the law can keep up with rapid technological developments and protect the interests of all parties involved in electronic transactions.(Setiawan 2021)

One of the main challenges faced in electronic transactions is consumer protection. Article 9 of the ITE Law stipulates that electronic system organizers are required to provide protection for consumers' personal data contained in their electronic systems (Law No. 11/2008). However, in practice, many consumers experience misuse of personal data or losses due to non-transparent and unfair transactions. The unclear responsibilities of e-commerce organizers and weak supervision of

e-commerce business actors often leave consumers in a weak position and vulnerable to fraud or violations of rights.

In addition, issues related to the validity of electronic evidence in legal disputes are also a significant challenge. Article 5 of the ITE Law recognizes that electronic information and/or electronic documents and their printouts are valid legal evidence (Law No. 11/2008). However, the acceptance and assessment of electronic evidence in the judicial process still raises various problems, especially related to the validity, authentication, and integrity of electronic data. The lack of understanding and expertise among law enforcement regarding electronic evidence often hinders a fair and effective law enforcement process.(Mighty and Pakpahan 2023)

Furthermore, the issue of electronic contracts also requires special attention. Article 18 of the ITE Law states that contracts made through an electronic system are considered valid and legally binding if they are carried out in accordance with the provisions of laws and regulations (Law No. 11/2008). However, in practice, many electronic contracts are not drafted with attention to the basic principles of contracts, such as agreement, legal capacity, and clarity of the rights and obligations of the parties. This often causes disputes between consumers and business actors that are difficult to resolve due to the lack of adequate legal protection.

Another issue that needs attention is the protection of intellectual property rights in electronic transactions. Online commerce often involves products protected by intellectual property rights, such as trademarks, copyrights, and patents. However, the enforcement of intellectual property rights in e-commerce still faces various obstacles, especially related to product counterfeiting, copyright infringement, and the distribution of illegal content. Article 25 of the ITE Law states that anyone who without permission distributes, transmits, or makes accessible electronic information or electronic documents containing content protected by intellectual property rights may be subject to criminal sanctions (Law No. 11/2008). However, the implementation of this provision is often ineffective due to limitations in supervision and law enforcement in cyberspace.(Fachrurozy, Sidi, and Zarzani 2023)

In addition, other legal challenges in electronic transactions are related to the security and integrity of electronic systems. Article 15 of the ITE Law states that electronic system organizers are required to organize reliable, secure, and responsible electronic systems to maintain the operational sustainability of the electronic systems they operate (Law No. 11/2008). However, many cases of data leaks, cyber attacks, and system vulnerabilities indicate that many e-commerce organizers have not met adequate security standards. This not only harms consumers, but also threatens the sustainability of the e-commerce business itself.

Given the various legal challenges that exist, it is important to thoroughly examine the applicable legal framework and evaluate its effectiveness in dealing with dynamic technological developments. This study aims to analyze the legal challenges in electronic transactions and e-commerce in Indonesia, as well as provide recommendations to strengthen regulations and improve legal protection for all parties involved. Thus, it is hoped that the Indonesian legal system can keep up with technological developments and ensure that electronic transactions are carried out fairly, transparently, and safely.

METHOD

This research uses a normative legal method with an analytical-descriptive approach.(Indra Utama Tanjung 2024)The normative legal method was chosen because this study focuses on the study

of laws and regulations governing electronic transactions and e-commerce in Indonesia, especially Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE) and other related regulations. The analytical-descriptive approach is used to analyze and describe various legal issues that arise in the practice of electronic transactions, as well as to evaluate the effectiveness of existing regulations in facing the challenges presented by the development of digital technology. The data used in this study are secondary data obtained from various legal sources, including laws and regulations, government documents, court decisions, as well as academic literature and related journal articles. This study will also use data taken from case studies and reports on legal issues in electronic transactions in Indonesia, which will be analyzed to identify legal loopholes and challenges faced in implementing regulations.(Yam 2022)

In its analysis, this study will evaluate the provisions in the ITE Law, such as Article 5 on the validity of electronic evidence, Article 9 on personal data protection, Article 18 on electronic contracts, and Article 25 on intellectual property rights. In addition, this study will also compare existing regulations in Indonesia with international best practices, especially related to e-commerce regulations in developed countries. This comparative approach aims to identify practices that can be adopted or adapted to the legal context in Indonesia. Data analysis will be conducted descriptively-qualitatively, where the data obtained will be interpreted and compiled into a narrative that describes the current legal conditions, challenges faced, and possible solutions that can be taken to improve the existing regulatory framework. This study will also provide concrete recommendations for policy makers to improve the effectiveness of regulations in electronic transactions and e-commerce, with the ultimate goal of creating a safe, fair, and sustainable e-commerce ecosystem in Indonesia. With this approach, it is hoped that this research can provide a significant contribution to the development of laws related to electronic transactions in Indonesia, as well as provide useful insights for academics, legal practitioners, and policy makers in facing legal challenges that arise due to the rapid development of information and communication technology.

RESULTS AND DISCUSSION

Consumer Protection in Electronic Transactions and E-Commerce

Consumer protection is one of the most crucial aspects of electronic transactions and e-commerce, given the cross-border, indirect, and often anonymous nature of these transactions. In Indonesia, consumer protection in electronic transactions is regulated primarily by Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) and Law Number 8 of 1999 concerning Consumer Protection. Although these two laws provide the legal basis for consumer protection, in practice there are still various challenges that need to be overcome to ensure that consumers are adequately protected in the e-commerce ecosystem.(Santri, Zarzani, and Hasibuan 2022)

One of the main issues in consumer protection in electronic transactions is the issue of personal data protection. Article 26 paragraph (1) of the ITE Law states that anyone who uses personal data in electronic transactions must obtain the consent of the data owner regarding the storage, use, and distribution of the data. This provision emphasizes the importance of clear and explicit consent from consumers before their personal data is used by other parties. However, in practice, many e-commerce platforms do not fully comply with this provision, which causes the risk of data leakage and misuse of consumers' personal information (Law No. 11/2008).

The use of personal data by e-commerce service providers is often done without adequate notice to consumers or without clear consent. For example, in many cases, consumers are not given the option to refuse the collection or use of their data, or the provisions related to the use of personal data are often hidden in long and complex terms and conditions, which are difficult for ordinary consumers to understand. This raises the risk of misuse of personal data by irresponsible parties, which can harm consumers financially and their privacy. The provisions in Article 26 of the ITE Law which require the consent of the data owner are often ignored or not implemented effectively by business actors in the e-commerce sector (Law No. 11/2008).

In addition, Article 15 of the ITE Law also stipulates that electronic system organizers are required to organize a reliable and secure system to protect personal data from unauthorized access. However, data leaks still often occur, indicating that many e-commerce service providers have not optimally complied with this provision. Data leaks that occur not only have an impact on the loss of consumer trust in e-commerce platforms but also cause losses that can have long-term impacts, both for consumers and business actors.

In addition to the ITE Law,(Dhadha et al. 2021)personal data protection is also regulated by Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP 71/2019), which emphasizes the obligation of electronic system organizers to maintain the confidentiality, integrity, and availability of managed personal data. However, the implementation of this regulation still faces major challenges, especially in terms of effective supervision and law enforcement. There are still many e-commerce companies that ignore this obligation or only comply partially without ensuring that their security systems are truly capable of protecting consumer data from increasingly complex cyber threats.

The responsibility of e-commerce organizers towards consumers is another aspect that needs to be considered in the context of legal protection. Article 9 paragraph (1) of the Consumer Protection Law states that business actors are required to provide correct, clear and honest information regarding the condition and guarantee of goods and/or services traded. In the context of e-commerce, this provision is often ignored, which causes consumers to receive products or services that do not match the description given on the e-commerce platform (Law No. 8/1999).

Many consumers suffer losses due to inaccurate or misleading information regarding products sold online. For example, the products received by consumers often do not match the images or descriptions displayed on the website, both in terms of quality, size, color, and other technical specifications. In addition, a problem that often arises is the lack of clarity regarding the return or refund policy, which is often not explained in detail or is difficult for consumers to access.(Rianto, Zarzani, and Saragih 2024)

Article 18 of the Consumer Protection Law also stipulates that business actors are prohibited from creating standard clauses that include provisions on the transfer of responsibility, namely clauses that state that consumers must bear all risks for losses that may occur due to the use of products or services. However, many e-commerce platforms still use standard clauses in their terms and conditions, which limit or even eliminate their responsibility for losses experienced by consumers. Such clauses are often found in contracts or user agreements that are unilaterally drafted by e-commerce service providers, without the opportunity for consumers to provide individual approval or rejection.

The lack of law enforcement against e-commerce providers who violate consumer rights is also a major challenge in creating a fair and transparent e-commerce ecosystem. Although the Consumer Protection Law has provided a strong legal basis to protect consumers, the implementation and enforcement of the law still face various obstacles, including low legal awareness among consumers,

limited supervisory resources, and corruption and bureaucracy that slow down the law enforcement process.

Effective dispute resolution is key to protecting consumer rights in electronic transactions. Article 45 of the ITE Law provides the right for parties who feel aggrieved by violations of electronic information and transactions to file a civil lawsuit to obtain compensation for the losses suffered. However, lengthy and expensive legal procedures often become a barrier for consumers to seek justice. In addition, there is still a lack of fast and efficient alternative dispute resolution mechanisms, such as mediation or arbitration, that can be accessed by consumers online (Law No. 11/2008).

The absence of a dispute resolution mechanism that is easily accessible to consumers has led many consumers to choose not to assert their rights, especially in cases where the value of the losses experienced is considered disproportionate to the costs and time required to resolve the dispute legally. This creates injustice and is detrimental to consumers, especially those who do not have access to adequate legal assistance or resources.

In order to improve the dispute resolution system in electronic transactions, the government needs to introduce regulations that allow consumers to resolve disputes quickly and efficiently, either through online dispute resolution platforms or through digitally accessible courts. In addition, there needs to be an increase in legal education and consumer awareness of their rights in electronic transactions, so that they can be more proactive in protecting themselves from unfair business practices.

Consumer protection in electronic transactions and e-commerce is a complex challenge and requires a comprehensive and adaptive regulatory approach. Although the ITE Law and the Consumer Protection Law have provided an important legal basis, there are still many gaps and weaknesses in implementation that need to be addressed immediately. With tighter supervision, increased law enforcement, and the development of more accessible dispute resolution mechanisms, Indonesia can create a safer and fairer e-commerce ecosystem for all parties involved.

Validity of Electronic Evidence in Legal Disputes

The validity of electronic evidence in legal disputes is one of the important aspects regulated in Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE). Article 5 of the ITE Law emphasizes that electronic information and/or electronic documents and their printouts are valid legal evidence. This marks the legal recognition of evidence based on digital technology, which previously had not been adequately accommodated in the Indonesian legal system. However, although this provision provides a legal basis for the use of electronic evidence, its implementation in legal practice still faces various challenges that need to be overcome to ensure justice in resolving disputes involving electronic evidence.(Setiawan 2021)

One of the main challenges in the use of electronic evidence is the issue of authentication and validity. Article 5 paragraph (4) of the ITE Law states that electronic information and/or electronic documents must be guaranteed to be intact, authentic, and accessible and accountable so that they meet the requirements as valid legal evidence (Law No. 11/2008). However, in practice, the process of authenticating electronic evidence is often debated, especially when there is doubt regarding the authenticity or integrity of the electronic data.

In this context, authentication of electronic evidence becomes crucial because digital technology allows data to be modified or falsified in ways that are difficult to detect. For example, an email or electronic message can be manipulated by an unauthorized party to change its content or create false evidence. This challenge is compounded by a lack of understanding and technical expertise among

law enforcement on how to verify the authenticity of electronic evidence, including the use of encryption technology, digital signatures, or other authentication methods.(Antonius, Saragih, and Zarzani 2024)

In addition, the validity of electronic evidence is often questioned when there is doubt about how the evidence was collected, stored, and presented in court. For example, if electronic data is collected illegally or without valid permission, the evidence may be considered invalid and cannot be used in legal proceedings. This is regulated in Article 30 of the ITE Law which prohibits illegal access to electronic systems and provides criminal sanctions for violators (Law No. 11/2008). Therefore, it is important for parties using electronic evidence to ensure that the entire process of collecting and storing evidence is carried out in accordance with applicable legal procedures.

The reliability of electronic systems used to produce evidence is also a major concern in the legal context. Article 15 of the ITE Law requires electronic system organizers to organize reliable, secure, and responsible systems (Law No. 11/2008). However, in many cases, the reliability of electronic systems is often questioned, especially in the event of system failures, cyber attacks, or other incidents that may affect data integrity.

For example, in disputes involving electronic transactions, transaction evidence is often stored in systems that are vulnerable to cyberattacks or technical errors. If such systems are unreliable or data is leaked, the validity of the evidence produced by those systems may be questioned in court. In addition, errors in data management or the inability to recover lost or corrupted data may render such evidence unreliable.

System reliability also relates to the ability to audit and verify submitted electronic evidence. In many cases, a digital forensic audit is required to ensure that electronic data presented as evidence has not been manipulated or altered after it was collected. However, the ability to conduct such an audit is often limited by the availability of technical resources and expertise among law enforcement. In addition, the high cost of conducting a forensic audit can be a deterrent for parties involved in a dispute to use electronic evidence.

To overcome these challenges, there is a need for strengthening regulations and increasing technical capacity among law enforcement in handling electronic evidence. This includes providing specific training for judges, prosecutors, and lawyers on how to manage and evaluate electronic evidence, as well as developing national standards governing the reliability and authentication of electronic evidence. With clear and consistently applied standards, it is hoped that electronic evidence can be recognized and used effectively in legal processes in Indonesia.

The acceptance of electronic evidence in court often faces challenges, especially because there is no uniform understanding among judges on how to assess and interpret such evidence. Although Article 5 of the ITE Law recognizes the validity of electronic evidence, its application in court practice is still limited by different interpretations among judges, who are often influenced by conventional legal backgrounds that are less familiar with digital technology (Law No. 11/2008).

In addition, there is concern that electronic evidence can be misused by irresponsible parties to manipulate the legal process. For example, digital evidence that has been modified or falsified can be submitted in court without the opposing party or even the judge being aware of it. This can damage the integrity of the judicial process and result in unfair decisions. Therefore, courts need to be more careful in accepting and evaluating electronic evidence, taking into account the possibility of data manipulation or falsification.

Another challenge in the admissibility of electronic evidence is related to jurisdictional issues. In many cases, relevant electronic evidence may be stored outside of Indonesian jurisdiction, which can

complicate the process of collecting and presenting such evidence in court. For example, if data required as evidence is stored on a server located in another country, interested parties may face difficulties in gaining access to such data, especially if the country in question has strict laws regarding data protection or privacy.

To address these challenges, stronger international cooperation and the development of bilateral or multilateral agreements that allow cross-border access to electronic evidence are needed. In addition, Indonesia needs to adopt internationally recognized universal principles in handling electronic evidence, so as to ensure that legal processes involving electronic evidence are conducted fairly and in accordance with global standards.(Rahardjo 2009)

The validity of electronic evidence in legal disputes in Indonesia is a complex challenge that requires serious attention. Although the ITE Law has given legal recognition to electronic evidence, its implementation in practice still faces various obstacles related to authentication, system reliability, and admissibility of evidence in court. To overcome these challenges, improved regulation, training for law enforcement, and stronger international cooperation are needed. Thus, electronic evidence can play a more effective role in supporting fair and transparent judicial processes in Indonesia.

CONCLUSION

This study has explored the legal challenges faced in electronic transactions and e-commerce in Indonesia, with a focus on consumer protection and the validity of electronic evidence in legal disputes. Although Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) and Law Number 8 of 1999 concerning Consumer Protection have provided an important legal basis, their implementation still faces various obstacles. In terms of consumer protection, the main challenges include personal data protection, the responsibilities of e-commerce organizers, and effective dispute resolution. Many e-commerce platforms have not fully complied with provisions related to consumer protection, which poses a risk of data leakage and unfairness to consumers.

The validity of electronic evidence is also a critical issue in legal disputes. Challenges related to authentication, system reliability, and the admissibility of electronic evidence in court hinder the optimal use of digital evidence in the judicial process. The lack of clear standards and technical understanding among law enforcement officers exacerbates this situation. Therefore, it is necessary to improve regulations, education for law enforcement, and international cooperation to ensure that electronic transactions and e-commerce in Indonesia can be carried out fairly, transparently, and safely. With a comprehensive approach, it is hoped that the law can keep up with technological developments and provide adequate protection for all parties involved.

BIBLIOGRAPHY

Antonius, Agam Saputra, Yasmirah Mandasari Saragih, and T Riza Zarzani. 2024. “Criminal Elements and Prisoner Guidance in Narcotics Crimes (A Study of Prisoner Guidance at Class IIa Pancur Batu Penitentiary, Deli Serdang Regency).” Innovative: Journal Of Social Science Research 4 (1): 9868–81.

Dhadha, Tegar Pan, Laras Atika Rahayu, Dewi Sito Resmi, and Dora Kusumastuti. 2021. “The Effectiveness of the Role of the ITE Law in Protecting and Maintaining All Cyber Activities in Indonesia.” Legal Standing: Journal of Legal Studies 6 (1): 40–48.

Fachrurozy, M, Redyanto Sidi, and T Riza Zarzani. 2023. “Legal Study of Online Transportation Company Responsibilities for Consumer Safety.” Legalitas: Jurnal Hukum 15 (1): 150–57.

Indra Utama Tanjung. 2024. BASICS OF LEGAL RESEARCH METHODS. Karanganyar: CV Pustaka Dikara). https://scholar.google.com/citations?view_op=view_citation&hl=id&user=rToGqjUAAAAJ&cstart=20&pagesize=80&citation_for_view=rToGqjUAAAAJ:Wp0gIr-vW9MC.

Perkasa, Anggada, and Kartina Pakpahan. 2023. “Law Enforcement Policy in Combating Gambling Crimes Through Electronic Media in Indonesia.” SIBATIK JOURNAL: Scientific Journal in the Fields of Social, Economic, Cultural, Technology, and Education 2 (7): 2067–84.

Rahardjo, Satjipto. 2009. “Legal Education as Human Education.”

Rianto, Rianto, T Riza Zarzani, and Yasmirah Mandasari Saragih. 2024. “Legal Responsibility of Online Media Corporations and Social Media Users for Broadcasting News Shared to the Public Containing ITE Criminal Acts.” JIIP-Journal of Scientific Education 7 (1): 393–98.

Santri, Nafadilla Dwi, T Riza Zarzani, and Syaiful Asmi Hasibuan. 2022. “Legal Study of the Legal Validity of the Get Contact Application Based on the Consumer Protection Law and Regulation Number 20 of 2016.” RECTUM JOURNAL: Legal Review of Criminal Act Handling 4 (2): 480–87.

Santy, Santy. 2023. "LEGAL PROTECTION OF CONSUMERS IN E-COMMERCE TRANSACTIONS BASED ON LAW NUMBER 11 OF 2008 CONCERNING INFORMATION AND ELECTRONIC TRANSACTIONS AND LAW NUMBER 8 OF 1999 CONCERNING CONSUMER PROTECTION LEGAL." UJoST-Universal Journal of Science and Technology 2(1): 323–34.

Setiawan, M Nanda. 2021. “Criticizing the ITE Law Article 27 Paragraph (3) Viewed from the Socio-Politics of Indonesian Criminal Law.” DATIN Law Journal 2 (1): 1–21.

Yam, Jim Hoy. 2022. “Reflections on Mixed Methods Research.” EMPIRE 2 (2): 126–34.