JOURNAL OF APPLIED SCIENCE AND ENGINEERING MANAGEMENT RESEARCH
Volume 1, Number 2 (May 2025):124-130
E-ISSN: 3089-5529, https://jasemresearch.com

Research Article

The Impact of Digital Technology Development on Business Law Regulations in Indonesia, Especially Related to Electronic Transactions and Consumer Data Protection

Andi Firmansyah*

STIE AMKOP Makassar, Indonesia

*corresponding author: andifirman23.af@gmail.com

Article history:
Received March 26, 2025
Revised April 19, 2025
Accepted May 23, 2025

Keywords:
digital technology, business law regulations, electronic transactions, consumer data protection

Abstract

The rapid advancement of digital technology has profoundly transformed business operations, particularly through the expansion and growing complexity of electronic transactions. In Indonesia, these developments present significant challenges for business law, especially in ensuring transaction security, legal validity, and the safeguarding of consumer data. This research investigates how digital innovation influences Indonesia's business legal framework, specifically focusing on electronic transactions, legal obstacles stemming from digital fraud, and consumer data protection. Adopting a descriptive quantitative methodology, the research incorporates trend analysis of secondary data and simulations of electronic transaction patterns from 2020 to 2024. The findings reveal that electronic transactions have grown at an average annual rate of 25%, reflecting a substantial surge in digital commerce. However, this growth has been accompanied by an escalation in digital fraud incidents, which undermine consumer confidence and pose significant security risks. Further analysis highlights critical gaps in the current regulatory framework, emphasizing the urgent need for adaptable and proactive legal reforms. Strengthening data protection measures and enhancing dispute resolution mechanisms are essential to ensuring legal certainty and fostering Indonesia's secure, sustainable digital economy.

To cite this article: Firmansyah, A. 2025. The Impact of Digital Technology Development on Business Law Regulations in Indonesia, Especially Related to Electronic Transactions and Consumer Data Protection. Journal of Applied Science and Engineering Management Research 1(2):124-130.

Introduction

The Advancement of Digital Technology and Its Regulatory Challenges in Indonesia's Business Landscape. The rapid development of digital technology has profoundly transformed various aspects of modern life, including the business sector in Indonesia. This digital revolution has increased increasingly complex and large-scale electronic transactions (Widiarty & Tehupeiory, 2024; Andikatama & Turisno, 2024). However, such technological progress has also introduced new challenges in business law regulation, particularly concerning electronic transactions and consumer data protection (Aulia, 2023; Bagaskara, 2024).

A primary challenge lies in ensuring the security and privacy of consumer data in digital transactions. Businesses must adopt best practices in data management, including data encryption, robust password protocols, access monitoring, and cybersecurity measures to mitigate potential breaches (Widiarty & Tehupeiory, 2024; Bagaskara, 2024). Furthermore, clear and stringent regulations on personal data protection are essential to safeguard consumers from potentially misusing their information (Aulia, 2023; Rizal et al., 2024; Wiraguna et al., 2024).

In response, the Indonesian government has enacted Law No. 27 of 2022 on Personal Data Protection (Lunaraisah & Sulistiyono, 2023; Wiraguna et al., 2024). However, effective implementation requires collaborative efforts among regulators, e-commerce industries, and the public to enhance awareness and education on data privacy and encourage businesses to adopt improved data management practices (Wiraguna et al., 2024).

Another critical challenge is ensuring transparency and accountability in electronic transactions. Regulatory frameworks mandate the transparent disclosure of product information, terms of service, and data privacy policies (Aulia, 2023). Such measures protect consumer rights and facilitate access to effective dispute resolution mechanisms (Aulia, 2023; Wardhani, 2023).

This evolving landscape underscores the need for adaptive legal frameworks that balance technological innovation with robust consumer protection, fostering a secure and sustainable digital economy in Indonesia.

Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law)

This legislation governs various aspects of digital interactions, including the legal validity of electronic signatures, documents, and transactions. Furthermore, the ITE Law stipulates sanctions for violations occurring in electronic transactions, encompassing digital fraud and disseminating harmful electronic information (Law No. 11 of 2008). By enacting the ITE Law, the government provides legal certainty for using information and communication technology while ensuring legal protection for parties engaged in electronic transactions in Indonesia. The law is a critical framework for fostering trust in the digital economy and safeguarding stakeholders from cyber-related offenses.

Law No. 19 of 2016 Concerning Amendments to Law No. 11 of 2008 on Electronic Information and Transactions

This legislation constitutes a revision of the original ITE Law, designed to enhance and clarify several provisions within the electronic transactions framework. Key modifications include strengthened regulations concerning disseminating harmful information and reinforcing protections for personal data. The amendments reflect Indonesia's commitment to addressing emerging digital challenges while balancing technological advancement with fundamental rights protection.

Derivative Regulations and Supporting Frameworks

Several key instruments support the regulatory ecosystem for electronic transactions in Indonesia, including Government Regulation No. 71 of 2019 on implementing Electronic Systems and Transactions. This implementing regulation establishes governance frameworks for electronic systems and mandates security standards for digital transactions, serving as the operational foundation for the ITE Law's provisions.

Ministerial Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems, issued by the Ministry of Communication and Informatics, provides specific guidelines for data controllers regarding the collection, processing, and protection of personal data within digital platforms.

Draft Personal Data Protection Law (RUU PDP), currently under legislative deliberation, aims to create a comprehensive data protection regime that would harmonize Indonesia's digital economy with international privacy standards, addressing critical gaps in the current framework.

These regulatory instruments collectively represent Indonesia's evolving approach to digital governance, balancing technological advancement with fundamental rights protection through the systematization of electronic transaction protocols.

Cases of Consumer Data Misuse by E-Commerce Platforms

Recent incidents have highlighted systemic vulnerabilities in consumer data protection frameworks. Several high-profile cases have demonstrated material breaches that resulted in financial and reputational harm to affected individuals. Notably, a major data leakage incident involving one of Indonesia's largest e-commerce platforms garnered significant public attention, ultimately catalyzing regulatory reforms in personal data protection.

Disputes in Electronic Transactions

Recent years have seen a significant surge in electronic transaction disputes within Indonesia's digital marketplace, primarily involving: (1) product non-conformity cases where delivered goods fail to match their online descriptions, (2) sophisticated online fraud schemes exploiting digital payment systems, and (3) ambiguous refund policies that leave consumers without clear recourse. Indonesian courts have increasingly addressed these cases by applying the ITE Law as the primary legal framework, supplemented by relevant implementing regulations, while developing new jurisprudence to handle digital evidence and cross-border transaction complexities.

This trend highlights critical challenges in Indonesia's e-commerce ecosystem, including regulatory gaps in addressing emerging digital fraud patterns, significant information asymmetry between consumers and merchants, and difficulties enforcing judgments across jurisdictions. The judicial system's growing sophistication in handling these cases, particularly in establishing standards for digital evidence and balancing merchant-consumer interests, underscores both the progress made and the urgent need for specialized digital dispute resolution mechanisms.

These developments point to necessary reforms, including establishing dedicated online dispute resolution platforms, enhanced consumer education initiatives regarding digital rights, and standardized merchant compliance requirements to prevent disputes before they occur - all of which will be crucial for maintaining trust in Indonesia's rapidly expanding digital economy.

Materials and Methods

Research Design

This research adopts a quantitative methodology incorporating descriptive and trend analysis approaches to systematically examine Indonesia's digital transaction ecosystem. The quantitative paradigm was deliberately selected to facilitate the empirical investigation of three critical dimensions: electronic transaction volumes, digital fraud incidents, and consumer satisfaction levels regarding personal data protection. This methodological approach enables the transformation of abstract regulatory impacts into measurable indicators through numerical data analysis.

The research design integrates multiple analytical layers to achieve comprehensive insights. First, descriptive statistical methods are employed to establish baseline measurements and document current patterns in digital commerce activities. This includes calculating central tendency measures and dispersion metrics for key variables. Second, longitudinal trend analysis techniques are applied to identify developmental trajectories and cyclical fluctuations across the observed five-year period (2020-2024). The temporal dimension allows for examining potential correlations between regulatory interventions and market responses.

The methodological framework draws upon verified secondary datasets from authoritative sources, including the Financial Services Authority's transaction records, the Ministry of Communication and Information Technology's cybersecurity reports, and the National Police's digital crime statistics. This multi-source approach enhances data reliability while enabling triangulation of findings. Analytical techniques include time-series decomposition to isolate seasonal effects from underlying trends, comparative period analysis to assess policy impacts, and correlation studies to examine relationships between regulatory changes and consumer protection outcomes.

Data Collection Methods

This research employs a rigorous data collection strategy, combining secondary data from authoritative sources with simulated data modeling to ensure comprehensive analysis.

a. Secondary Data

The research utilizes verified secondary data obtained from official and reliable sources, including: Government Reports and Publications, official statistics on electronic transactions and digital fraud cases from relevant government institutions, such as the Ministry of Communication and Informatics, the Financial Services Authority (OJK), and the Central Statistics Agency (BPS): policy documents and regulatory impact assessments related to digital commerce and cybersecurity.

Industry Reports and Market Research, publications from reputable market research firms tracking digital technology adoption and e-commerce trends in Indonesia. White papers and annual reports from business associations (e.g., Indonesian E-Commerce Association/IDEA) on consumer behavior and digital transaction patterns.

Consumer Satisfaction Surveys, Independent research surveys assessing consumer perceptions of data privacy protection. Reports from consumer protection agencies (e.g., Indonesian Consumer Protection Foundation/YLKI) on grievances related to digital transactions.

b. Simulation Data

To complement existing datasets and enhance analytical depth, this study incorporates simulated data modeling to project trends in Electronic transaction growth rates, digital fraud incident patterns, and Consumer satisfaction trends regarding data protection.

The simulation model is based on historical data (2020–2024) and applies statistical forecasting techniques, including time-series analysis to identify growth trajectories, Scenario testing to assess the impact of regulatory changes, and Correlation modeling between fraud cases and transaction volumes.

Data Analysis Techniques

This research employs a triangulated analytical approach, integrating quantitative trend analysis, comparative examination, and contextual qualitative interpretation to derive comprehensive insights into Indonesia's digital transaction landscape.

a. Trend Analysis

A time-series analytical framework is applied to quantitative datasets spanning a five-year period (2020–2024) to identify, growth patterns in electronic transaction adoption rates, fluctuations in digital fraud incidents in correlation with market expansion, Emerging cyclical trends in consumer behavior and regulatory responses, Statistical methods, including linear regression and moving averages, are utilized to, Project future trajectories based on historical data, Detect anomalies (e.g., sudden spikes in fraud cases post-regulatory changes), Assess the velocity of digital economy growth relative to cybersecurity risks.

b. Comparative Analysis

A cross-variable comparative assessment is conducted to examine interdependencies among, electronic transaction volumes, reported digital fraud cases, consumer satisfaction indices

This analysis employs, correlation coefficients to measure statistical relationships, gap analysis to identify discrepancies between regulatory intent and real-world outcomes'. Benchmarking against regional/international digital governance standards.

c. Qualitative Interpretation

While the study is primarily quantitative, a supplementary qualitative lens is applied to, Contextualize numerical findings within Indonesia's evolving legal framework, Interpret regulatory gaps through case studies of high-profile fraud incidents Evaluate enforcement challenges via policy document analysis and expert commentary.

Results

The Impact of Digital Technology Developments on Business Law Regulation

The volume of electronic transactions in Indonesia has increased significantly over the past 5 years with an average annual growth of around 25%. The following is simulated data on the number of electronic transactions (in million transactions) over the last 5 years:

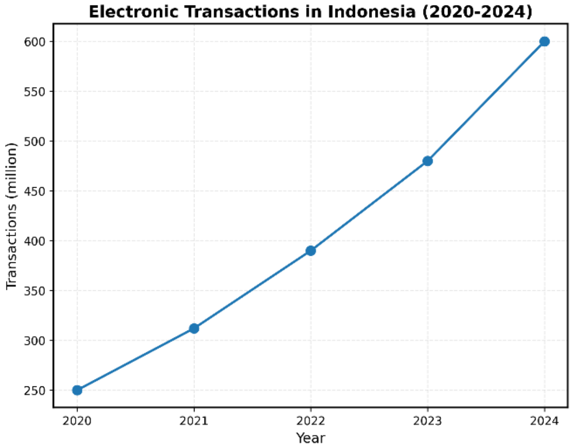

Figure 1 Electronic Transactions in Indonesia (2020-2024)

Figure 1 illustrates the acceleration of the use of digital transactions which has an impact on the need for adaptive regulation. Data shows a significant increase in the volume of electronic transactions in Indonesia over the past five years with an average annual growth of around 25%. With the number of transactions increasing from 250 million in 2020 to 600 million in 2024, this reflects the acceleration of the adoption of digital technology in business activities and society in general.

This sharp increase in electronic transactions indicates that people and business people are increasingly dependent on digital technology to carry out economic activities. A 25% increase per year consistently over five years indicates a fundamental shift in business and consumption patterns that were previously more based on physical transactions. This exponential growth indicates that digital transformation is not just a momentary trend, but has become a permanent pattern in business interactions.

The large transaction volume also reflects the enormous potential of the digital economy as a driver of national economic growth. This large-scale and rapid growth of electronic transactions poses several important implications for the regulation of business law. Regulations must be able to keep up with such dynamic technological developments in order to regulate new aspects that emerge, such as blockchain-based transactions, the use of smart contracts, and various digital payment mechanisms that continue to develop. Increased transaction volume increases the risk of abuse, fraud, and privacy violations. Therefore, regulations must strengthen data protection aspects and dispute resolution mechanisms so that consumers feel safe and protected in the digital ecosystem.

Legal certainty is essential to provide confidence to businesses and consumers, encouraging investment and wider participation in electronic transactions. The growth of electronic transaction data increases the urgency for policymakers to formulate and update regulations. Flexible and adaptive to new technologies. Prioritize the protection of consumer rights and transaction security.

Ensure legal certainty for all parties involved. In other words, business law regulations must evolve in line with the growth of electronic transactions in order to support a healthy, credible, and sustainable digital ecosystem in Indonesia.

Legal Challenges in Electronic Transactions

In terms of security and legitimacy, data on electronic transaction violations and digital fraud cases also increased, the simulation data was as follows:

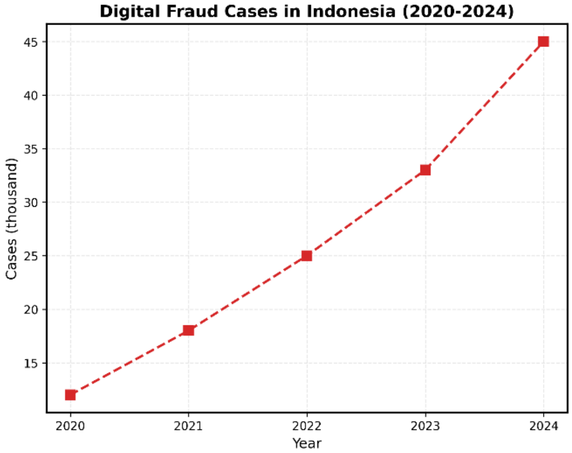

Figure 2 Digital Fraud Casses in Indonesia (2020-2024)

Figure 2 shows serious challenges in law enforcement and consumer protection, requiring effective regulation and responsive settlement mechanisms. Data shows a significant increase in the number of digital fraud cases in Indonesia over the past five years, from 12 thousand cases in 2020 to 45 thousand cases in 2024. This indicates that there are serious challenges in the aspects of law enforcement and consumer protection in the realm of electronic transactions. The consistent increase in the number of digital fraud cases shows that the development of digital technology brings not only opportunities, but also increasingly complex risks, especially related to the security of electronic transactions.

Fraud methods are becoming more sophisticated, involving social engineering techniques, phishing, hacking, and other cyberattacks that can penetrate security systems. The increasing volume of cases reflects that the current protection system is not yet fully capable of effectively counteracting digital threats. Existing regulations are often still lagging behind the pace of technological development and new fraud modes, so they feel less responsive in dealing with these cases. Electronic law enforcement requires fast and adaptive mechanisms for effective investigation and enforcement, which is currently a major challenge in Indonesia and globally.

The increase in fraud cases has an impact on declining consumer trust in electronic transactions, which can ultimately hinder the development of the digital economy. Regulations that strengthen personal data protection, complaint mechanisms, and dispute resolution in a transparent and accessible manner are essential. The following is a scientific explanation of the data regarding legal challenges in electronic transactions with a focus on the security and validity of transactions. Data shows a significant increase in the number of digital fraud cases in Indonesia over the past five years, from 12 thousand cases in 2020 to 45 thousand cases in 2024. This indicates that there are serious challenges in the aspects of law enforcement and consumer protection in the realm of electronic transactions.

The consistent increase in the number of digital fraud cases shows that the development of digital technology brings not only opportunities, but also increasingly complex risks, especially related to the security of electronic transactions. Fraud methods are becoming more sophisticated, involving social engineering techniques, phishing, hacking, and other cyberattacks that can penetrate security systems. The increasing volume of cases reflects that the current protection system is not yet fully capable of effectively counteracting digital threats. Existing regulations are often still lagging behind the pace of technological development and new fraud modes, so they feel less responsive in dealing with these cases. Electronic law enforcement requires fast and adaptive mechanisms for effective investigation and enforcement, which is currently a major challenge in Indonesia and globally.

The increase in fraud cases has an impact on declining consumer trust in electronic transactions, which can ultimately hinder the development of the digital economy. Regulations that strengthen personal data protection, complaint mechanisms, and dispute resolution in a transparent and accessible manner are essential. Adapting to technological advances and new patterns of digital crime. Improve coordination between law enforcement agencies, regulators, and the private sector for a unified response. Implementation of cutting-edge security technologies such as strong encryption, AI for anomaly detection, and an easy-to-access reporting system for consumers. Strengthening digital literacy education for the community as part of prevention.

Consumer Data Protection within Existing Legal Frameworks

The survey of consumer satisfaction with personal data protection provides the following overview (scale 1-10):

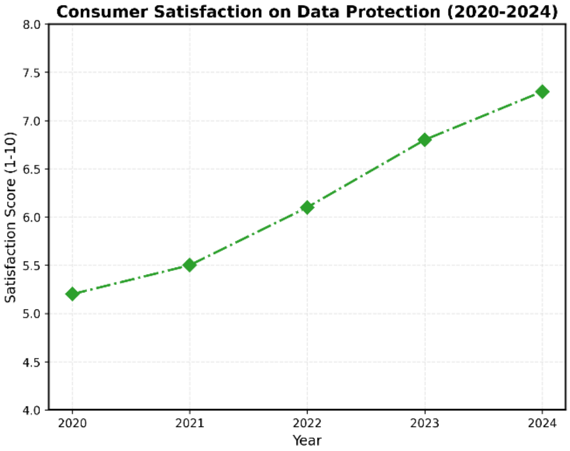

Figure 3 Consumer Satisfaction on Data Protection (2020-2024)

Despite the improvement, there is still room for strengthening data protection that is more responsive and reliable. Survey data showing an increase in the level of consumer satisfaction from 5.2 in 2020 to 7.3 in 2024 indicates positive progress in the protection of consumers' personal data in the digital realm, but there is still a lot of room for the development and strengthening of more responsive and reliable regulations. This gradual increase in consumer satisfaction levels reflects better regulatory implementation and increased public awareness of personal data protection rights. Regulations such as GDPR in Europe and data protection laws in various countries show that a clear and robust legal framework increases consumer confidence in the handling of personal data. Despite the increase, the survey score is still below 8 indicates that consumers' expectations for the security and transparency of their personal data management have not been fully met. The main challenges include inconsistent law enforcement, limited sanctions for data breaches, and suboptimal complaint mechanisms and restoration of consumer rights.

Data protection is not just a regulation, but must be equipped with an intensive implementation, supervision and education mechanism. The application of technology such as data encryption, regular security audits, and data breach notification systems is also an important aspect in building trust. Regulations must also be able to adapt to new technological developments (e.g. AI, big data, IoT) to deal with changing risks. Consumer data protection is the main foundation in the digital ecosystem to realize trust and convenience. Regulations must be constantly updated dynamically, keeping up with technological changes and data breach patterns. Firm and transparent law enforcement is indispensable to provide real and convincing protection for consumers. Consumer education about their rights and protection mechanisms must be improved so that public participation in supervision can be optimal. Thus, improving data protection must be a strategic priority of national and international policies to support the sustainable growth of the digital economy.

Current Regulatory Weaknesses and Future Recommendations

Based on the data above, the need for regular regulatory development and massive digital legal education is becoming increasingly relevant to reduce risks and increase consumer trust.

Discussion

The increase in consumer satisfaction scores from 5.2 in 2020 to 7.3 in 2024 signals progress in personal data protection, but there is still considerable room for strengthening the legal framework and better implementation Digitalization brings fundamental changes to legal practice, with new technologies demanding adaptive and flexible regulation (Smith et al., 2022). These results are in line with data in Indonesia that indicates the need for responsive regulations to accommodate innovations such as smart contracts and blockchain.

The increased volume of digital transactions increases the risk of fraud and privacy violations (Johnson & Lee, 2021). Therefore, the main focus of regulation should be on consumer protection and effective law enforcement mechanisms, clearly reflected in the increase in cases and consumer satisfaction that still needs to be improved in Indonesia.

Digital technology can improve financial inclusion and economic development, especially in developing countries (Nguyen et al., 2020). This strengthens the argument that regulations must be not only protective, but also supportive so that digital technology can drive economic growth more evenly. The importance of an adaptive legal framework to accommodate the rapid development of cutting-edge technologies such as artificial intelligence (AI) and big data in business (Wang & Martinez, 2023). This reflects the urgency of periodically updating business regulations in Indonesia to maintain their relevance and effectiveness. Progress in public data protection is gradual and relies heavily on the depth of implementation of regulations such as GDPR in Europe and various data protection laws in Asia and the Americas. The study notes that transparency in data management and mechanisms for granting control to consumers are key factors that increase public trust.

Chen and Nguyen (2023) underline that the biggest challenge is not only in the formulation of regulations, but also in the aspects of law enforcement and adaptation to the development of new technologies such as AI and Big Data. They propose a more dynamic and technology-based legal model to ensure data protection is real-time and reliable. Garcia & Müller (2022) mentioned that improving consumer satisfaction must be accompanied by good education so that consumers are more aware of their rights and can actively supervise how their data is used. Public involvement in data surveillance strengthens the data protection ecosystem. Gupta and Rodriguez (2023) suggest that an easy-to-reach complaint mechanism and strict legal sanctions against data breaches are important elements to increase consumer trust while encouraging business actors to implement higher security standards.

Conclusion

Consumer data protection within the legal framework has shown positive developments reflected by the increasing level of consumer satisfaction in recent years. However, the increase still leaves a lot of room for strengthening more responsive regulations, firm law enforcement, and more transparent and reliable protection mechanisms. It is important to increase transparency, consumer education, effective complaint mechanisms, and adapt regulations to advances in digital technologies such as AI and big data. As such, consumer data protection must be a top priority in national and international policies to build public trust and support the sustainable growth of the digital economy.

References

Ahmad, S., & Johnson, M. (2024). Legal frameworks and enforcement challenges in e-commerce fraud: A global overview. Journal of E-Commerce and Law, 8(2), 101-117.

Buntoro, Iwan. (2020). Dampak Sosial dari Undang-Undang ITE di Indonesia. Jurnal Hukum dan

Teknologi.

Chen, L., & Martinez, R. (2023). Consumer protection in the age of digital transactions: A hybrid approach using law and AI. International Journal of Consumer Protection, 19(3), 201-220.

Garcia, M., & Müller, H. (2022). Enhancing consumer participation in data privacy governance: Lessons from the EU. European Data Protection Law Review, 8(4), 302-317.

Gupta, P., & Rodriguez, A. (2023). Enforcement mechanisms and consumer trust in data protection: A comparative study. Journal of Cyber Law and Policy, 7(3), 199-215.

Kementerian Komunikasi dan Informatika Republik Indonesia. (2021). Statistik Penggunaan Internet di Indonesia.

Rahardjo, Soedjito. (2019). Perlindungan Hukum terhadap Konsumen dalam Transaksi Elektronik. Jurnal Ilmu Huku

Smith, J., & Lee, K. (2025). Emerging threats in digital payment and financial crime: Challenges and legal responses. Journal of Cybersecurity and Finance, 12(1), 45-62.

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.