Formosa Journal of Science and Technology (FJST)
Vol. 4, No. 5, 2025: 1469-1478

The Legal Validity of Electronic Data in Indonesia: Framework, Application, and Challenges

Suprayitno[1], Tony[2], Kukuh Derajat Takarub[3]
University of North Sumatra
Corresponding Author: Suprayitno, suprayit91@gmail.com

A R T I C L E I N F O

Keywords: Electronic Data, Legal Validity, Indonesian Law

Received : 14, April
Revised : 28, April
Accepted : 30, May

A B S T R A C T

As digital transformation accelerates across public and private sectors in Indonesia, the legal recognition of electronic data becomes increasingly vital. This paper examines the regulatory framework governing electronic data in Indonesia, focusing on Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law) and its amendments. It explores how electronic records and digital signatures are treated in legal processes, addresses admissibility issues in court, and identifies key challenges in ensuring security, authenticity, and public trust.

ISSN-E: 2964-6804
DOI: https://doi.org/10.55927/fjst.v4i5.74
https://traformosapublisher.org/index.php/fjst

INTRODUCTION

Indonesia's swift digital transformation has significantly influenced trade, governance, and the legal sector. As an increasing number of transactions are conducted electronically, concerns have emerged about the legal validity and evidential weight of electronic data. This paper aims to clarify the status of electronic data under Indonesian law and to examine the practical challenges faced during its application. Discussions on personal data protection within electronic systems are inherently linked to the duties and liabilities of electronic system providers. According to Ardiansyah Parman, Chairman of the National Consumer Protection Agency (BPKN), when data breaches occur, users of electronic platforms frequently lack compensation or sufficient protection guarantees from the system providers. This issue was highlighted in an incident where a user's account was hijacked, yet the system provider did not offer compensation for the resulting losses. This situation underscores the necessity to firmly establish the accountability of electronic system operators, as data controllers and/or processors, in safeguarding users' personal data. Moreover, protecting personal data within electronic systems is closely tied to upholding the rights of data subjects.

This issue has yet to be firmly and comprehensively addressed within a robust legal framework. Although there are several laws and regulations governing the operation of electronic systems, they do not fully cover the protection of personal data. As a result, the application of personal data protection principles within electronic systems is suboptimal, leading to violations of data subjects' rights without adequate enforcement. Given this context, the problem to be examined is how the implementation of personal data protection regulations by electronic system providers can be evaluated through the lenses of dignified justice and legal certainty theories. The research method employed in this study is normative juridical, involving an analysis of existing laws and theoretical frameworks related to personal data protection, particularly focusing on the concepts of justice and legal certainty.

From the viewpoint of Legal Certainty Theory, the lack of a dedicated law concerning personal data indicates that adequate legal protection for personal data has yet to be established. Ideally, a formal legal regulation should be enacted to serve as a clear legal framework. This would undoubtedly assist authorities and law enforcement officials in effectively handling incidents and enhancing their supervisory roles over electronic system providers. Moreover, having a law with more comprehensive provisions on personal data protection than the current regulations would provide greater legal certainty for both electronic system operators (PSE) and Indonesian citizens—many of whom rely heavily on electronic systems—ensuring the safeguarding of their privacy rights.

Data security refers to the measures taken to safeguard data from damage, whether deliberate or accidental, unauthorized modifications, and unauthorized dissemination without the consent of the data owner. This protection is carried out in accordance with applicable laws and regulations. Simply put, data security is a system designed to maintain and protect the data within an organization. It typically involves securing physical hardware, software applications,

administrative controls, and access management. When properly implemented, an effective data security strategy can shield critical organizational assets and business information from cybercrime, insider threats, and reduce losses caused by human error.

Maintaining data security also requires focusing on three key aspects: confidentiality, integrity, and availability. Data security is closely intertwined with cybersecurity; competent cybersecurity practices usually indicate adherence to data security standards as well. Various types of data security methods are used to protect confidential and sensitive information, including personal data.

Cybersecurity is defined as an organization's effort to defend its information technology systems against illegal threats and attacks, including unauthorized access. It encompasses tools, policies, and security concepts aimed at safeguarding organizational assets and users. By implementing robust cybersecurity measures, organizations can minimize risks posed to IT systems, thereby protecting both the organization and individuals, including the subjects of personal data.

THEORETICAL REVIEW

Legal Framework in Indonesia

The ITE Law (Law No. 11 of 2008)

Indonesia's main legal basis for electronic data is Law No. 11 of 2008 on Electronic Information and Transactions, commonly known as the ITE Law, which has been amended by Law No. 19 of 2016 and further supported by Government Regulation No. 71 of 2019 (GR 71/2019).

Key provisions include:

a. Article 5(1): Electronic information and/or electronic documents are recognized as valid legal evidence.
b. Article 6: Electronic documents are considered equivalent to written documents, provided they are accessible, displayable, and can be verified.
c. Article 11: Electronic signatures have the same legal force as manual signatures if they meet certain requirements.

The implementation of electronic systems by electronic system organizers (PSE) must be based on the values of dignified justice, PSE must be able to guarantee the privacy of electronic system users and maintain the security of their information and data7. One way that PSE can guarantee the privacy of its users is by implementing the latest and most sophisticated protection and security efforts to prevent hacking and leakage of personal data. Implementing electronic systems with dignity also means that PSE respects the rights and privacy of users. This has also been mandated in, for example, the ITE Law and PP 71/2019 where PSE must organize electronic systems reliably and safely and be responsible for the operation of their electronic systems. So it can be concluded that this must be done by PSE, one of which is to maintain the security of data and privacy of electronic system users. However, in reality, there are still many cases of personal data leaks that occur, both in private and public electronic systems. In private electronic systems, one of the biggest cases that has ever occurred and still cannot be forgotten to this day is the Tokopedia data leak case

that occurred in March 2020. Meanwhile, in the public sphere, leakage cases occurred in eHAC and BPJS Kesehatan. Often, cases of personal data leakage end with coordination between PSE and Kemenkominfo and BSSN. The public is not given information about the development and continuation of the cases that occur.

Law Number 27 of 2022 concerning Personal Data Protection which was ratified on October 17, 2022 was born from considerations stated in the 1945 Republic of Indonesia Law. Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia states that, "Everyone has the right to protection of themselves, their families, honor, dignity and property under their control, and has the right to a sense of security and protection from the threat of fear to do or not do something that is a basic human right." This confirms that all citizens without exception have the right to protection of themselves, their families, honor, dignity and property under their control. The right to personal data is a property right inherent in every individual as a subject of personal data. Protection of personal data applies to every individual, both Indonesian citizens and foreign citizens in Indonesia in relation to all processing of personal data including collection, use, storage, sending, and deletion.

Government Regulation No. 71 of 2019

GR 71/2019 strengthens the implementation of the ITE Law by detailing provisions on electronic systems and transaction organizers. It provides technical guidelines for data processing, cybersecurity, and interoperability.

From the existing positive law, in the sector of electronic system implementation specifically and in the laws that exist in general in Indonesia, Indonesia actually still does not have specific personal data protection regulations. This creates uncertainty for ESOs, as well as law enforcement officers, in the event of data leaks and data breaches. In the regulation of electronic system implementation mentioned above, there is not even a clear recognition of the concept of "data controller" and "data processor" explicitly. In the ITE Law, there is no clear distinction between ESOs as data controllers and as data processors. There is still a mixed impression that ESOs are always data controllers and processors. When compared to the EU GDPR, there should actually be a distinction between data controllers and data processors and there should be a clear division in terms of their obligations and responsibilities. One form of human rights that must be protected is the right to privacy. The right to privacy can be protected by establishing a regulation in the form of a legally binding law. The scattered regulation of personal data protection and the lack of integration in a law indicate a legal vacuum and legal uncertainty. The distribution shows that there has been no harmonization and integration in the level of legislation in its normative hierarchy16. Legal vacuum will cause various complications of problems. One of the difficulties that can be faced by the competent authorities in organizing electronic systems, namely the Ministry of Communication and Information, is the difficulty in making decisions or taking follow-up actions in the event of a data leak case17. To protect human privacy

rights, it can actually be realized by forming a special law that regulates the protection of personal data

METHODOLOGY

The method used in this study is normative juridical, namely examining the existing rules and theories related to the problem of personal data protection, especially from the theory of Justice and legal certainty.

RESULTS AND DISCUSSION

Legal Requirements for Valid Electronic Data

For electronic data to be legally valid and enforceable under Indonesian law, the following conditions must be met:

a. Authenticity: Must be identifiable and linked to the creator or sender.
b. Integrity: Content must not be altered after creation.
c. Readability: Data must be accessible and displayable for verification.
d. Compliance: Must meet standards outlined in relevant regulations, especially when involving public services or state institutions.

The development of information technology in the digital era has led to the emergence of new trends, cultures, and behaviors in society, both positive and constructive or negative. What can be done from the perspective of technology users is to be careful. If you pay attention, many social media users, both intentionally and unintentionally, spread their personal information or data to social media, which of course can increase the risk of financial or non-financial losses. In general, the public is not yet aware of the impact of misuse of information, resulting in low public awareness of personal data protection. Even so, the government has taken initial action on personal data protection by ratifying the Personal Data Protection Law so that in the future it is hoped that the Law can provide legal protection for personal data subjects. This initial action is very important considering that uncontrolled disclosure of personal data can pose many risks to personal data subjects and organizations and increase the possibility of criminal acts, ranging from threats, bullying, fraud to hacking of accounts owned by personal data subjects.

Before the enactment of Law Number 27 of 2022 concerning Personal Data Protection in October 2022, there were actually already sectoral regulations governing personal data protection. In general, the Personal Data Protection Law was created with the aim of providing protection and legal certainty for cases of misuse of personal data, including data leaks that often occur in Indonesia. The implementation of Law Number 27 of 2022 concerning Personal Data Protection will certainly be easier if derivative regulations or implementing regulations in the form of Government Regulations have been made. This is because the Law on Personal Data Protection in Indonesia has not regulated in detail the implementation of personal data protection which in the future will be compiled by an independent authorized institution appointed by the President. 2.) Legal protection of personal data from the aspect of data security and cybersecurity is also conveyed in Law Number 27 of 2022 concerning Personal Data Protection, Law of the Republic of Indonesia Number 11 of 2008 concerning Information and

Electronic Transactions, such as Government Regulation Number 71 of 2019 concerning Electronic System and Transaction Organizers, Regulation of the Minister of Communication and Informatics Number 20 of 2016 concerning Personal Data Protection in Electronic Systems. In these regulations, it can be concluded that organizations need to maintain data security and cybersecurity owned by an organization, whether the organization is a controller of personal data or a processor of personal data. Organizations are even required to conduct periodic audits, reliability certification by third parties or consultants to ensure that the information systems they have are still in the safe category. According to Article 31 of Law Number 27 of 2022 concerning Personal Data Protection, it is also explained about the activity of recording personal data processing.

This is to ensure critical assets that need to be maintained by the organization and also to implement proper data and cyber security. Legal protection of personal data from the aspect of data security and cyber security that already exist in the regulations must be supported by proper implementation. For this, organizations as controllers of personal data or processors of personal data are advised to use cyber and data privacy consulting services in order to find out what is needed by the organization in order to comply with applicable regulations and implement data and cyber security that is in accordance with the conditions, goals and needs of the company.

Electronic Signatures and Certification Authorities

Indonesian law distinguishes between certified and uncertified electronic signatures:

a. Certified signatures must be issued by a registered Certification Authority (CA) recognized by the Ministry of Communication and Informatics (Kominfo).
b. Digital certificates help ensure the signer's identity and data integrity.

These mechanisms are crucial for the acceptance of electronic contracts, tax filings, and court submissions.

Unwittingly, the growth of the technology, information, and communication industry is also influenced by the existence of the Law on Personal Data Protection. This is because with the Law on Personal Data Protection, users of products designed by the technology, information, and communication industry feel safer because there are already regulations that protect their privacy rights and guarantee protection and legal certainty. In addition, when viewed from a larger perspective, countries that already have personal data protection regulations will be more trusted to do business with than countries that do not yet have a Law on Personal Data Protection. This is because based on international personal data protection regulations, it is recommended to send data abroad to countries that already have a Law on Personal Data Protection that is equivalent to that country or higher in terms of the competence of the Law on Personal Data Protection that is owned. Meanwhile, the Law on Personal Data Protection also applies to public institutions such as law enforcement and intelligence agencies, but has not been clearly regulated regarding exceptions for law enforcement and intelligence agencies. This needs to be clarified regarding exceptions so that there

are no violations of citizens' privacy and personal data rights when law enforcement and intelligence agencies carry out their duties and authorities. Currently, the Law on Personal Data Protection has regulated efforts to protect personal data, including the definition of personal data, types of personal data, rights of personal data subjects, processing of personal data, obligations of controllers and processors of personal data, prohibitions and sanctions, both in administrative and criminal forms, for any party that violates efforts to protect personal data. The implementation of personal data protection is carried out by an independent institution formed and appointed by the president and is directly responsible to the president. However, the appointment of the independent institution has not been made so that the responsibility and authority of the institution are not yet clear.

Admissibility of Electronic Evidence in Indonesian Courts

Under Article 5(1) of the ITE Law, electronic data is admissible as evidence. However, courts require:

a. Proof of authenticity and origin
b. Verification by expert testimony or digital forensic analysis, if disputed
c. Chain of custody documentation for sensitive digital evidence

The Supreme Court Regulation No. 1 of 2019 on e-Litigation further supports the use of electronic documents in judicial processes.

In processing personal data, the Regulation of the Minister of Communication and Information requires electronic system organizers to provide notification and also request approval in accordance with the purpose to the subject of personal data and determine the legal basis for processing personal data, especially when collecting personal data. Furthermore, if processing or analysis is carried out, it must also be carried out in accordance with the agreement. Then regarding the sending of personal data, the method of sending, the purpose of sending, the accuracy of the data, and also the agreement must also be considered. The data sent must be verified for accuracy and in accordance with the agreement of the owner of the personal data. In addition, it is also necessary to apply the provisions of laws and regulations regarding the exchange of personal data across national borders. In terms of storage, data including personal data must be encrypted and treated in accordance with the data classification that has been determined in the data management policy or privacy policy contained in the policy owned by the electronic system organizer. Finally, regarding destruction, electronic system organizers need to determine a retention schedule, determine procedures and parties responsible for retention in order to be able to carry out data retention periodically in accordance with the specified policy.

Based on the Regulation of the Minister of Communication and Information concerning the Protection of Personal Data in Electronic Systems, it also regulates the obligations of Electronic System Organizers, there are several obligations related to data security and cybersecurity, namely that every Electronic System Organizer is required to carry out certification for the reliability or feasibility test of the electronic system it manages in accordance with the provisions of laws and regulations, Electronic System Organizers are required to have internal rules that

regulate the protection of personal data or can also be called a personal data protection policy (privacy policy), Electronic System Organizers are required to provide an audit track record of all activities of the electronic system they manage. In terms of implementation, consultants do recommend that organizations know critical assets (crown jewels) where these assets can include confidential data, personal data of both general and specific types. By knowing critical assets, organizations will be able to implement appropriate data security and cybersecurity techniques. The method for determining critical assets can be carried out in accordance with Article 31 of the Personal Data Protection Law Number 27 of 2022, namely by carrying out data processing recording activities. Electronic System Organizers are also required to provide a contact person who can be easily contacted by personal data subjects regarding the management of their personal data or can also be called a Data Protection Officer (DPO).

Challenges in Implementation

Despite the robust legal framework, several challenges remain:

a. Technical capacity gaps among law enforcement, courts, and lawyers
b. Lack of public awareness and trust in digital documents
c. Cybersecurity vulnerabilities that may affect data authenticity
d. Cross-border legal issues, particularly with cloud storage and international transactions

In the field of electronic system implementation, there are several laws and regulations that regulate the content of the material as described. Regulations on personal data protection in general are still spread across at least 32 sectoral laws and regulations. There is no specific law that contains material on personal data protection. Of the four positive laws mentioned above related to the implementation of electronic systems, the most comprehensive one containing provisions on personal data protection is Permenkominfo 20/2016. However, when viewed from the legal force side, based on the hierarchy of laws and regulations as regulated in Law No. 12 of 2011 concerning the Formation of Laws and Regulations, the legal product in the form of a Ministerial Regulation does not have the same legal force as a Law. This also becomes an obstacle for law enforcement authorities to take action against cases of data leaks that occur.

With the introduction of the Personal Data Protection Law, it is anticipated that the fundamental rights and freedoms of individuals regarding personal data protection will be safeguarded. The law aims to enhance legal protections surrounding personal data, provide clear legal certainty in cases of misuse, and ensure organizational compliance, especially within business and industrial sectors that handle substantial amounts of personal data. Prior to this law, personal data protection was governed by various sector-specific regulations, which were often fragmented and limited in scope. Consequently, these sectoral rules were insufficient to fully guarantee comprehensive legal protection and certainty for personal data. Examples of such regulations include Law No. 7 of 1971 on Archives, Law No. 7 of 1992 (amended by Law No. 10 of 1998) on Banking, Law No. 8 of 1997 on Company Documents, Law No. 36 of 1999 on Telecommunications, Law No. 11 of 2008 on Electronic Information and

Transactions, Law No. 39 of 1999 on Human Rights, Law No. 8 of 1999 on Consumer Protection, Law No. 23 of 2006 on Population Administration, Law No. 36 of 2009 on Health, and other regulations such as Government Regulation No. 71 of 2019 on Electronic System and Transaction Organizers and the Minister of Communication and Information Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems. More recently, Law No. 4 of 2023 on the Development and Strengthening of the Financial Services Sector has also been enacted to bolster customer personal data protection within the financial industry.

The effectiveness of personal data protection heavily depends on the proper implementation of data security and cybersecurity measures. These elements are critical within information systems, as inadequate protection can lead to both financial and non-financial harm to organizations and related parties. To secure data effectively, organizations must ensure that data remains confidential, intact, and accessible, addressing the three core principles of data security. While the Personal Data Protection Law explicitly mandates these protections, their practical application is governed by other regulations such as Law No. 11 of 2008 on Electronic Information and Transactions, Government Regulation No. 71 of 2019 on Electronic System and Transaction Organizers, and the Minister of Communication and Informatics Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems.

Specifically, Government Regulation No. 71 of 2019 requires electronic system organizers to conduct regular cybersecurity audits (Articles 18 and 69). Articles 65 to 72 discuss the role of certification institutions responsible for issuing reliability certificates, which confirm that electronic system operators comply with Indonesian regulations and industry best practices. Additionally, the Ministerial Regulation No. 20 of 2016 highlights the necessity for electronic system organizers to establish internal policies safeguarding personal data, known as internal privacy policies, to prevent breaches. Typically, personal data controllers within these organizations must maintain both internal privacy policies and external privacy notices to ensure comprehensive data protection.

CONCLUSIONS AND RECOMMENDATIONS

Indonesia has established a clear legal foundation for recognizing and validating electronic data through the ITE Law and supporting regulations. While the legal validity is well-acknowledged, practical and technological challenges continue to hinder seamless implementation. Enhanced infrastructure, capacity building, and international cooperation are necessary to fully realize the benefits of digital evidence and electronic transactions.

FURTHER STUDY

Further study is recommended to explore the effectiveness of the implementation of electronic data regulations at various levels of law enforcement and public institutions in Indonesia. Future research could focus on assessing the readiness and competence of legal practitioners, government agencies, and private sector entities in applying digital evidence standards, as well as evaluating the impact of existing cybersecurity frameworks on

maintaining data integrity and privacy. Additionally, comparative studies with countries that have mature digital legal ecosystems could provide valuable insights for policy refinement and cross-border legal harmonization in the context of electronic transactions and data protection.

REFERENCES

Rahman, Irsan, et al. "Harmonization of Digital laws and Adaptation Strategies in Indonesia focusing on E-Commerce and Digital transactions." *Innovative: Journal Of Social Science Research* 4.1 (2024): 4314-4327.

Wulandari, Mega. "Legal Review of the Validity of Electronic Deeds in International Business Transactions: An Indonesian Notary's Perspective." *Jurnal Indonesia Sosial Teknologi* 6.1 (2025).

Judijanto, Loso, Nuryati Solapari, and Irman Putra. "An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia." *The Easta Journal Law and Human Rights* 3.01 (2024): 20-29.

Barlian, Aristo Evandy A., et al. "Electronic Criminal Justice in Indonesia: Challenges and the Future Measures." *Jambura Law Review* 7.1 (2025): 243-274.

Syarief, Elza. "Security concerns in digital transformation of electronic land registration: Legal protection in cybersecurity laws in Indonesia." *International Journal of Cyber Criminology* 16.2 (2022): 32-46.

Rhogust, Muhammad. "Legal Framework for Cybersecurity in the Digital Economy: Challenges and Prospects for Indonesia." *Journal of Law, Social Science and Humanities* 1.2 (2024): 166-180.

Prasetyo, Budi, I. Gusti Ayu Ketut Rachmi Handayani, and Adi Sulistiyono. "Data Protection Laws in Indonesia: Navigating Privacy in the Digital Age." *Side: Scientific Development Journal* 2.1 (2025): 9-16.

Sidik, Suyanto. "Dampak undang-undang informasi dan transaksi elektronik (UU ITE) terhadap perubahan hukum dan sosial dalam masyarakat." *Jurnal Ilmiah Widya* 1.1 (2013): 1-7.