



The Urgency of Personal Data Protection Regulation in Digital Legal Systems

Meiliven Maqdeline Marentek¹

¹ Universitas Diponegoro, Semarang, Indonesia

Abstract

Article history:

Received: July 25, 2025

Revised: September 3, 2025

Accepted: October 24, 2025

Published: December 30, 2025

Keywords:

Cyber Law,
Cyber Security,
Digital Privacy,
Electronic Systems,
Personal Data Protection.

Identifier:

Zero Open

Page: 92-115

<https://zeraopen.com/journal/jclis>

Advances in information technology and digital transformation have increased the use of electronic systems in various aspects of society. This situation has given rise to new legal challenges regarding personal data protection and electronic system security. This study aims to analyze the effectiveness of regulations on personal data protection and electronic systems and to examine the urgency of strengthening digital legal regulations in the era of information technology development. The study employs a normative legal method using a legislative approach and a conceptual approach. The legal materials used consist of primary legal sources, namely Law No. 27 of 2022 on Personal Data Protection and Law No. 11 of 2008 on Electronic Information and Transactions, as amended by Law No. 1 of 2024, as well as secondary legal materials in the form of scientific journals and academic. The research findings indicate that personal data protection regulations have provided a legal foundation for safeguarding the privacy rights of the digital community; however, their implementation still faces various challenges, such as weak oversight, low digital security literacy, and the increasingly complex evolution of cyber threats. This study also found that strengthening digital legal regulations is an urgent necessity to create legal certainty, enhance public trust, and provide more effective protection for the personal data security of the public in the era of digital transformation.

*Corresponding author:
(Meiliven Maqdeline Marentek)

©2025 The Author(s).

This is an open-access article under CC-BY-SA license (<https://creativecommons.org/licence/by-sa/4.0/>)



1. Introduction

The development of information and communication technology has driven major transformations in various aspects of modern society's life, especially in the implementation of public services, digital economy activities, and the management of electronic-based information systems. Increasingly massive digitalization has a positive impact on the efficiency and accessibility of services, but on the other hand it also poses new challenges in the form of increasing threats to data security and the protection of people's privacy rights. The use of electronic systems that has not been fully balanced with the strengthening of regulations and the readiness of cybersecurity infrastructure has led to the emergence of various legal problems related to the misuse of personal data, cyber attacks, and digital information leaks that have a wide impact on society and the state. In the context of the modern legal state, the protection of personal data and the security of electronic systems is not only a technical issue, but also part of the protection of human rights that must be guaranteed through effective regulations and adaptive to the development of digital technology (Daeng et al., 2023).

The existence of Law Number 27 of 2022 concerning Personal Data Protection is an important step in strengthening the national legal system in the field of data protection and digital security. The regulation is present as a response to the increasing public need for legal certainty related to the management of personal data in electronic systems. In addition, Law Number 11 of 2008 concerning Information and Electronic Transactions and amendments through Law Number 1 of 2024 also provides a legal basis for the implementation of electronic systems and law

enforcement for various forms of digital violations. However, the increasingly complex development of cyber threats shows that the existence of regulations is not fully able to provide optimal protection for personal data and public information security (Wardana, 2024).

The development of digital technology has created a new interaction space that facilitates the rapid and wide exchange of information. However, this condition also opens up opportunities for various forms of law violations in cyberspace such as data theft, misuse of digital identities, hacking of electronic systems, and distribution of personal data without the consent of the data owner. According to Tanjung and Febrianisa (2024), the weak implementation of digital security regulations and low standards of electronic system protection are still the dominant factors that cause a high risk of data leakage and privacy violations in the digital era. This condition shows that legal regulations are not only required to be present normatively, but must also be able to be implemented effectively in the practice of implementing electronic systems.

In addition to regulatory aspects, challenges in personal data protection are also influenced by low legal awareness and digital security literacy in society. Many users of electronic systems do not understand the importance of personal data protection and the legal risks that can arise from the misuse of digital information. Chaudhary et al. (2022) explained that low cybersecurity awareness is one of the causes of increasing digital threats in various sectors. On the other hand, technological developments that take place faster than regulatory developments cause legal gaps in anticipating new forms of digital crime. Therefore, regulatory

reform and strengthening of the supervisory system are urgent needs in order to create more comprehensive legal protection for the digital society.

Digital security issues are also closely related to public trust in electronic system operators and state institutions. Dharmajaya and Minangkabawi (2024) stated that weak personal data protection can affect the level of public trust in digital systems, especially if there is an information security breach that causes social and economic losses. From a legal perspective, the state has an obligation to ensure that any implementation of electronic systems is carried out based on the principles of security, prudence, and protection of people's privacy rights. Therefore, the effectiveness of regulatory implementation is an important factor in determining the success of the personal data protection and cybersecurity system nationally.

At the global level, the development of cyber threats has prompted various countries to strengthen international cooperation in the development of digital security and data protection regulations. Trim and Lee (2021) emphasized that cyber threats are a cross-border problem that requires policy harmonization and collaboration between institutions and countries. In this context, the national legal system must be able to adapt to the development of international digital law so as not to be left behind in facing the dynamics of information technology that continues to develop. Strengthening national regulations is also needed to ensure legal certainty for the responsible and sustainable use of digital technology.

In addition, the development of cyber law in Indonesia shows that digital law regulations continue to undergo the process of adjusting to the needs of society and technological developments. Fairuzzen et al. (2024) explains that cyber law

regulation must be able to accommodate ethical aspects, protection of digital rights, and overall security of electronic systems. Therefore, the discussion of the effectiveness of personal data protection regulations and electronic system security is very important in order to evaluate the extent to which national laws are able to provide protection to the public in the digital era. Thus, this research not only focuses on the normative aspects of laws and regulations, but also examines the urgency of strengthening digital legal regulations as part of efforts to maintain information security and people's privacy rights.

Based on this background, this study formulated two research questions. First, how effective are the regulations on personal data protection and electronic systems in providing legal protection for the security of people's digital data? Second, why is strengthening regulations on personal data protection and electronic system security an important urgency in the development of digital law in the current era of information technology?

2. Methods

This study uses normative juridical research methods with a statutory approach and a conceptual approach. The normative juridical method was chosen because this research focuses on the analysis of legal norms that govern the protection of personal data, the security of electronic systems, and the effectiveness of digital legal regulations in providing protection to society in the era of information technology development. This approach is used to examine various legal provisions related to data protection and cybersecurity, especially Law Number 27 of 2022

concerning Personal Data Protection, Law Number 11 of 2008 concerning Information and Electronic Transactions and amendments through Law Number 1 of 2024, as well as various other supporting regulations related to the implementation of electronic systems and the protection of digital privacy rights. Normative juridical research is carried out by examining legal principles, legal systematics, synchronization of laws and regulations, and the development of digital legal concepts from the perspective of protecting people's rights.

The data sources in this study use primary legal materials, secondary legal materials, and tertiary legal materials. The primary legal material consists of laws and regulations related to personal data protection, electronic system security, and cyber law. Secondary legal materials were obtained from various scientific journals, academic articles, law books, previous research results, and scientific publications relevant to the theme of data protection and digital security in the last five-year period. The tertiary legal materials are used as support in understanding legal terms and concepts related to information technology and data protection. The technique of collecting legal materials is carried out through library research by examining various legal sources and scientific literature that are indexed by Google Scholar and have relevance to the research focus. According to Saly et al. (2023), normative legal research has an important function in evaluating the effectiveness of regulations and identifying weaknesses in legal norms that are developing in the modern digital society.

The legislative approach is carried out by examining the normative provisions contained in the Personal Data Protection Law and the Electronic Information and

Transaction Law to find out the extent to which these regulations are able to provide legal certainty and protection of people's privacy rights. In addition, a conceptual approach is used to understand the concepts of legal protection, cybersecurity, digital rights, and state responsibility in the implementation of electronic systems. Legal analysis is carried out qualitatively by interpreting various legal provisions and relating them to the development of digital technology and the phenomenon of data security threats that are developing in society. The analysis process is carried out through the identification of legal norms, interpretation of the provisions of laws and regulations, and evaluation of the effectiveness of the implementation of regulations in the practice of implementing electronic systems.

This research also uses prescriptive analysis techniques, namely providing legal arguments and recommendations for strengthening personal data protection and digital security regulations in the future. According to Firdaus (2024), the development of cyber law requires a harmonization of laws that are able to adapt to the dynamics of information technology and digital threats that continue to develop. Therefore, this study not only analyzes the existence of legal norms formally, but also examines the urgency of strengthening digital legal regulations in ensuring the security of personal data, protection of privacy rights, and legal certainty for the people who use electronic systems in the era of digital transformation.

3. Results

3.1. The Effectiveness of Personal Data Protection Regulations and Electronic Systems in Providing Legal Protection for the Public's Digital Data Security

The development of digital technology has changed the pattern of people's interactions in various aspects of life, including economic activities, public services, education, and social communication. This digital transformation has led to an increase in the use of electronic systems in the management of people's personal data. On the other hand, the increase in digital activities also poses legal risks in the form of data misuse, digital identity theft, and various forms of privacy violations that threaten people's rights to the security of personal information. This condition encourages the state to present legal regulations that are able to provide protection for personal data and the security of electronic systems. In the context of national law, regulations regarding personal data protection and digital security are regulated through Law Number 27 of 2022 concerning Personal Data Protection and Law Number 11 of 2008 concerning Information and Electronic Transactions as amended through Law Number 1 of 2024. The presence of these regulations shows the state's efforts to build a legal protection system for the digital society.

The Personal Data Protection Law provides a legal basis related to the rights of data subjects, the obligations of data controllers, and responsibilities in the management of people's personal information. The regulation is an important instrument in creating legal certainty for the use of personal data in the digital space. According to Daeng et al. (2023), the existence of personal data protection

regulations is a strategic step in strengthening the national legal system in the era of digital transformation because it is able to provide restrictions on the use and processing of data by certain parties. Through these arrangements, the public has the right to know the use of their personal data, obtain protection against data misuse, and demand accountability in the event of a violation of privacy rights. From a normative perspective, this arrangement suggests that the state is beginning to recognize personal data as part of a right that must be legally protected.

However, the effectiveness of the implementation of personal data protection regulations still faces various challenges. One of the main problems lies in the weak implementation of electronic system security standards in various sectors. Many electronic system operators have not implemented adequate security systems in digital data management, thus opening up opportunities for data leaks and illegal access to people's personal information. Tanjung and Febrianisa (2024) explained that the weak implementation of digital security regulations is caused by low compliance with data protection standards and suboptimal supervision of electronic systems. This condition shows that the existence of regulations has not been fully followed by the readiness of infrastructure and effective supervision mechanisms in the practice of implementing digital systems.

The effectiveness of digital law regulations is also influenced by the development of increasingly complex and dynamic cyber threats. Cyberattacks are not only carried out through hacking of electronic systems, but also through data manipulation, phishing, malware, and various other forms of abuse of digital technology. In such conditions, legal regulations are required to be able to adapt to

technological developments and changing patterns of digital threats. Wardana (2024) stated that data protection and digital security regulations need to be adaptive in order to be able to provide optimal legal protection to the public. If regulations do not develop along with technological developments, there will be a legal vacuum that can be used by digital crime perpetrators to commit various forms of violations in cyberspace.

In addition to the regulatory aspect, the effectiveness of personal data protection is also related to the level of legal awareness of the public in using electronic systems. Low digital security literacy causes many people to not understand the importance of personal data protection and legal risks that can arise from the unsafe use of digital technology. Chaudhary et al. (2022) explained that the lack of cybersecurity education is one of the main factors in increasing threats to public information security. Many users of electronic systems still use weak passwords, share personal information without security considerations, and lack a understanding of the potential for misuse of digital data. This condition shows that legal protection does not only depend on the existence of regulations, but also requires the active participation of the public in maintaining the security of their personal information.

On the other hand, strengthening the effectiveness of regulations also requires coordination between institutions in the supervision and enforcement of digital laws. The handling of personal data breaches and cybercrime involves various institutions that have different authorities in the national legal system. If coordination between institutions does not run optimally, then the law enforcement

process against digital violations will experience obstacles. Bechara and Schuch (2021) emphasized that cybersecurity requires cross-sector collaboration and strengthening institutional coordination so that the digital protection system can run effectively. Therefore, the effectiveness of personal data protection regulations is not only determined by the substance of the law, but also by the ability of institutions to implement and supervise the implementation of these regulations.

The development of cyber law in Indonesia shows that digital law regulations are still in the process of adjusting to the dynamics of global information technology. The amendment to the Electronic Information and Transaction Law through Law Number 1 of 2024 is a form of the state's effort to update the digital legal system to be more relevant to the development of the modern digital society. Fairuzzen et al. (2024) explains that cyber law must be able to accommodate aspects of digital rights protection, ethics of technology use, and electronic system security in a balanced manner. Thus, the effectiveness of personal data protection regulations is not only related to the existence of the rule of law, but also concerns the ability of the law to create a balance between technological developments and the protection of people's rights.

In addition, the effectiveness of regulations can also be seen from their ability to build public trust in the digital system. Dharmajaya and Minangkabawi (2024) stated that weak personal data protection can affect the level of public trust in the use of digital services and electronic systems. From a legal perspective, public trust is an important element in supporting the success of national digital transformation. Therefore, personal data protection regulations must be able to provide security

guarantees and legal certainty for the public as users of electronic systems. If regulations can be implemented effectively, the protection of people's privacy rights will be stronger and the use of digital technology can take place more safely and responsibly.

Overall, the effectiveness of personal data protection regulations and electronic systems still faces various challenges both in terms of implementation, supervision, digital literacy, and the ever-changing development of cyber threats. However, the existence of the Personal Data Protection Law and regulatory changes in the Electronic Information and Transaction Law show the state's commitment to strengthening the national digital legal system. Therefore, strengthening the implementation of regulations, increasing public legal awareness, and developing a digital security surveillance system are important factors in realizing effective legal protection for the security of people's digital data.

3.2. The Urgency of Strengthening Personal Data Protection and Electronic System Security Regulations in the Development of Digital Law

The rapid development of information technology has created major changes in the lives of modern society. Almost all people's activities now depend on the use of electronic systems, ranging from communication, economic transactions, public services, education, to the storage of personal data in digital platforms. This condition causes personal data to become one of the important assets that has enormous economic, social, and legal value. However, the increasing use of digital technology is also followed by increasing threats to people's data security and privacy rights. These threats include data theft, misuse of digital identities, hacking of

electronic systems, and distribution of personal information without the consent of the data owner. This situation shows that the protection of personal data and the security of electronic systems have become an urgent need in the modern legal system. Therefore, strengthening digital legal regulations is very important to provide adequate legal protection for society in the era of digital transformation.

The urgency of strengthening personal data protection regulations can be seen from the increasing dependence of the public on digital-based services. In practice, the public often provides personal data to various electronic system operators without clearly knowing how the data is stored, used, and protected. This condition creates vulnerability to data misuse by irresponsible parties. Saly et al. (2023) explained that the development of digital technology has caused personal data to become an object that is very vulnerable to violations of the law if it is not balanced with strong regulations and an effective supervisory system. Therefore, the existence of personal data protection regulations is important to provide legal certainty for the public's right to the security of their personal information.

Strengthening regulations is also urgent due to the development of cyber threats that are increasingly complex and difficult to control. Today's digital crime is no longer carried out simply, but uses increasingly sophisticated and organized technology. Violations of electronic system security can have a wide impact, both on individuals, institutions, and social stability in general. Wardana (2024) stated that data protection and digital security regulations must be continuously updated in order to be able to keep up with technological developments and global cyber threat patterns. In this context, the law cannot be static because the development of the

digital space takes place much faster than the process of forming regulations. If regulations are not strengthened in an ongoing manner, there will be legal gaps that can be used by digital crime perpetrators to commit various forms of violations of people's personal data.

The urgency of strengthening personal data protection regulations is also related to the protection of human rights in the digital space. The right to privacy is part of the fundamental right that must be guaranteed by the state, including in the use of information technology and electronic systems. The presence of Law Number 27 of 2022 concerning Personal Data Protection shows that the state is beginning to place data protection as part of the protection of citizens' rights. However, the implementation of these regulations still requires strengthening in aspects of supervision, law enforcement, and protection mechanisms for victims of digital data breaches. Triadi, Sumiadi, and Yusrizal (2022) explained that victims of personal data misuse often experience economic, psychological, and social losses due to weak legal protection systems in the digital space. Therefore, strengthening regulations is important to ensure that the public's right to information security is effectively protected.

In addition, the urgency of strengthening digital law regulations is also influenced by the low level of digital security awareness and literacy in society. Many digital technology users do not understand the importance of maintaining the confidentiality of personal data as well as the legal risks that can arise from the use of insecure electronic systems. Chaudhary et al. (2022) stated that low cybersecurity awareness is one of the factors that causes a high risk of personal data breaches in

various sectors. In these conditions, regulations not only function as an instrument of legal regulation, but also as a means of education and the formation of a digital legal culture in society. Strengthening regulations must be followed by increasing digital literacy so that people are able to understand their rights and obligations in the use of electronic systems.

The urgency of strengthening regulations is also related to the need for legal certainty in the implementation of electronic systems. The development of the digital economy and the wider use of information technology require a legal system that is able to provide security and trust guarantees for the community. Tanjung and Febrianisa (2024) explained that weak regulation and supervision of electronic systems can reduce public trust in the use of digital services. From a legal perspective, public trust is an important element in supporting the stability and sustainability of digital transformation. Therefore, personal data protection regulations must be able to provide guarantees that every data management is carried out in a safe, transparent, and responsible manner in accordance with the principles of privacy protection.

Strengthening digital security regulations is also important because cyber threats today have a cross-border character. Digital crime is no longer limited to a specific region, but can be carried out globally through internet networks and information technology. Trim and Lee (2023) emphasized that cybersecurity requires international collaboration and regulatory harmonization between countries in the face of increasingly complex digital threats. In this context, the national legal system needs to adapt to the development of international digital law in order to be able to

provide more effective protection for the public. Strengthening national regulations is also needed so that the state has a strong legal basis in conducting international cooperation related to handling cybercrime and digital data protection.

The amendment to the Electronic Information and Transaction Law through Law Number 1 of 2024 shows the need to update digital legal regulations according to technological developments and community needs. Firdaus (2024) explained that cyber law must be able to adapt to the dynamics of information technology developments and the ever-changing challenges of digital ethics. Digital legal regulation not only serves to regulate the use of technology, but also to maintain a balance between digital innovation and the protection of people's rights. Therefore, strengthening regulations is very important so that the law is able to provide certainty, protection, and justice in the use of electronic systems.

On the other hand, weak personal data protection can have a wide social impact on society. Dharmajaya and Minangkabawi (2024) stated that data security breaches can affect the level of public trust in digital systems and institutions that manage public information. If people feel that their personal data is not well protected, trust in digital transformation will decrease and can hinder the development of the digital economy as a whole. Therefore, the urgency of strengthening personal data protection regulations is not only related to legal aspects, but also related to social stability, information security, and sustainable development of a digital society.

Thus, strengthening regulations on personal data protection and electronic system security is an urgent need in the development of modern digital law. Strong,

adaptive, and implementive regulations are needed to deal with the development of cyber threats, protect people's privacy rights, increase public trust, and create legal certainty in the use of digital technology. Therefore, the state needs to continue to update regulations, strengthen supervision of electronic systems, improve digital security literacy, and build cross-sector cooperation to create a more effective and sustainable digital legal protection system.

4. Discussion

The development of digital technology has brought major changes to the social, economic, and legal systems of modern society. The use of electronic systems in various life activities shows that digital transformation has become an important part of national and global development. However, these technological developments also present various new legal challenges, especially related to the protection of personal data and the security of electronic systems. The results of the study show that the existence of Law Number 27 of 2022 concerning Personal Data Protection and the amendment of the Electronic Information and Transaction Law through Law Number 1 of 2024 are important steps in strengthening the national digital legal system. However, the effectiveness of these regulations still faces various obstacles in implementation, supervision, and adjustment to the increasingly complex development of cyber threats.

Normatively, personal data protection regulations have provided a legal basis for the recognition of people's privacy rights in the digital space. The presence of these regulations shows that the state is beginning to pay serious attention to the

protection of people's digital rights as part of human rights. However, in practice, various problems are still found related to weak data protection and the implementation of electronic system security standards is not optimal. Saly et al. (2023) explained that the main challenge in personal data protection does not only lie in the existence of regulations, but also in the effectiveness of implementation and supervision of electronic system operators. This shows that the formation of legal regulations must be followed by institutional readiness, strengthening supervision, and increasing the capacity of human resources in the field of digital security.

In addition, the rapid development of cyber threats causes legal regulations to often lag behind information technology developments. Today's cyberattacks are carried out with increasingly complex methods and involve various forms of digital manipulation that are difficult to detect through conventional systems. In these conditions, legal regulations must be adaptive and able to adapt to the dynamics of digital threats. Wardana (2024) stated that strengthening personal data protection regulations must be carried out on a sustainable basis so that the legal system is able to cope with changing technological developments. Therefore, digital law cannot be understood as a static rule, but as a legal system that must develop according to the needs of modern digital society.

The results of the study also show that low legal awareness and digital security literacy of the public are one of the factors that affect the effectiveness of personal data protection. Many people do not understand the risks of using electronic systems and the importance of maintaining the security of personal information in daily

digital activities. Chaudhary et al. (2022) explain that cybersecurity education has an important role in reducing the risk of data breaches and increasing public awareness of digital threats. In this context, legal protection does not only depend on formal regulation, but also requires the active participation of the public in keeping their personal data safe. Therefore, strengthening regulations must be accompanied by an increase in digital literacy and cyber law education on a sustainable basis.

On the other hand, the discussion of personal data protection is also closely related to the aspect of public trust in digital systems and electronic service providers. Public trust is an important element in supporting the development of the digital economy and information technology transformation. Dharmajaya and Minangkabawi (2024) stated that weak data protection can reduce the level of public trust in the use of digital services and electronic systems. From a legal perspective, the state has a responsibility to ensure that any data management is carried out in a secure, transparent manner, and in accordance with the principles of protection of the right to privacy. Therefore, strengthening digital regulations and law enforcement is an important part of maintaining social stability and the sustainability of digital transformation in society.

In addition to the national aspect, personal data protection also has an international dimension because cyber threats are cross-border. Digital crimes can be committed from various regions by utilizing the global internet network so that its handling requires cooperation between countries and harmonization of international regulations. Bechara and Schuch (2021) emphasized that cybersecurity requires cross-sectoral and cross-border collaboration to deal with the development

of global digital threats. In this context, the national legal system needs to adapt to the development of international cyber law in order to be able to provide more effective legal protection to the public. This shows that strengthening national regulations must be accompanied by the development of international cooperation in the field of digital security and personal data protection.

The amendment to the Electronic Information and Transaction Law through Law Number 1 of 2024 also shows the need to carry out digital legal reform in a sustainable manner. Fairuzzen et al. (2024) explained that the development of cyber law requires regulations that are able to accommodate aspects of digital ethics, protection of people's rights, and the development of information technology in a balanced manner. Thus, digital legal regulation not only serves to control the use of technology, but also to create legal certainty and protection of people's rights in the ever-evolving digital space.

Based on the results of the research and discussion, it can be understood that the effectiveness of personal data protection and electronic system security is not only determined by the existence of formal regulations, but also influenced by legal implementation, institutional readiness, public awareness, and the state's ability to adjust regulations to the development of digital technology. Therefore, strengthening the digital legal system must be carried out comprehensively through regulatory updates, strengthening supervision, increasing cybersecurity literacy, and developing cross-sector cooperation to create more effective legal protection for society in the era of digital transformation.

5. Conclusion

Advances in information technology and digital transformation have created new challenges within the legal system, particularly regarding the protection of personal data and the security of electronic systems. The increasingly widespread use of digital systems across various sectors of society has made personal data a critical element that must be legally protected. The enactment of Law No. 27 of 2022 on Personal Data Protection, as well as amendments to the Law on Information and Electronic Transactions through Law No. 1 of 2024, demonstrate the state's efforts to strengthen the national digital legal system and provide legal certainty regarding the protection of citizens' privacy rights in the digital space.

Based on research findings, the effectiveness of regulations on personal data protection and electronic system security still faces various challenges in their implementation. Although these regulations have provided a sufficiently important legal foundation for digital data protection, the implementation of electronic security systems and oversight of electronic system operators has not yet been optimized. The increasingly complex evolution of cyber threats also indicates that legal regulations must be continuously updated to keep pace with technological advancements and the ever-changing patterns of digital crime. Additionally, the public's low legal awareness and digital security literacy are factors affecting the effectiveness of personal data protection in the digital age.

This study also demonstrates that strengthening regulations on personal data protection and electronic system security is an urgent necessity in the development of modern digital law. Personal data protection is not only related to information

security but also concerns the protection of human rights, public trust, social stability, and the sustainability of digital transformation. Therefore, the state must strengthen regulatory implementation, enhance oversight of electronic system operators, expand digital security education for the public, and foster cross-sectoral and cross-national cooperation in addressing global cyber threats.

Thus, the strengthening of the digital legal system must be carried out comprehensively through adaptive regulatory updates, capacity building for law enforcement institutions, the development of better electronic security systems, and increased public legal awareness regarding the importance of personal data protection. These steps are necessary so that the law can provide effective protection for the public and create a safe, responsible, and just digital space amidst the continuous development of information technology.

References

- Bechara, F. R., & Schuch, S. B. (2021). Cybersecurity and global regulatory challenges. *Journal of Financial Crime*, 28(2), 359-374.
- Chaudhary, S., Gkioulos, V., & Katsikas, S. (2022). Developing metrics to assess the effectiveness of cybersecurity awareness program. *Journal of Cybersecurity*, 8(1), tyac006.
- Daeng, Y., Linra, N., Darham, A., Handrianto, D., Sianturi, R. R., Martin, D., ... & Saputra, H. (2023). Perlindungan Data Pribadi dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi. *Innovative: Journal Of Social Science Research*, 3(6), 2898-2905.

- Dharmajaya, A., & Minangkabawi, H. (2024). Membangun Kepercayaan yang Berkelanjutan di Era Disruptif Komunikasi: Perspektif Media dan Komunikasi Digital. *Jurnal Komunikasi*, 18(2), 265-280.
- Fairuzzen, M. R., Putra, A. A., Reihan, A., & SH, L. P. (2024). Perkembangan Hukum dan Kejahatan Siber “Cybercrime” di Indonesia. *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory*, 2(1), 139-153.
- Firdaus, R. A. (2024). Perlindungan hukum dan pencegahan kejahatan siber di era digital dalam sistem hukum di Indonesia. *STAATSRECHT: Jurnal Hukum Kenegaraan dan Politik Islam*, 4(1), 79-104.
- Indonesia. (2008). *Law Number 11 of 2008 concerning Information and Electronic Transactions*. Statute Book of the Republic of Indonesia Year 2008 Number 58.
- Indonesia. (2022). *Law Number 27 of 2022 concerning Personal Data Protection*. Statute Book of the Republic of Indonesia Year 2022 Number 196.
- Indonesia. (2024). *Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions*. Statute Book of the Republic of Indonesia Year 2024 Number 1.
- Saly, J. N., Artamevia, H., Kheista, K., Gulo, B. J. S., Rhemrev, E. A., & Christie, M. (2023). Analisis perlindungan data pribadi terkait uu no. 27 tahun 2022. *Jurnal Serina Sosial Humaniora*, 1(3), 145-153.
- Tanjung, M. F., & Febrianisa, F. (2024). Peran Regulasi Komunikasi dalam Mengatasi Pencurian Data Nasional pada 2024. *Jurnal Mahasiswa Komunikasi Cantrik*, 4(2).

- Triadi, M., Sumiadi, S., & Yusrizal, Y. (2022, December). Protection Of Victims Of Personal Data Through Digital Media. In *Proceedings of Malikussaleh International Conference on Law, Legal Studies and Social Science (MICoLLS)* (Vol. 2, pp. 00031-00031).
- Trim, P. R., & Lee, Y. I. (2021). The global cyber security model: counteracting cyber attacks through a resilient partnership arrangement. *Big Data and Cognitive Computing*, 5(3), 32.
- Wardana, A. P. (2024). Hukum Pidana dan Perlindungan Data Pribadi: Upaya Menanggulangi Kejahatan Siber di Era Digital di Indonesia. *Pustaka: Jurnal Ilmu Politik dan Hukum*, 1(1), 20-25.