



Education on Personal Data Protection in the Era of Digital Transformation among Indonesian and Thai Societies

Siti Mutmainah^{1*}, Hani Irhamdessetya², Vincentius Simon Suyanto³, Hargianti Dini Iswandari^{4*}, Nico Irawan⁵

^{1,2,3,4}Universitas Ngudi Waluyo Semarang

⁵Thai Global Business Administration Technological College

Corresponding Author: Siti Mutmainah hargianti.dini@gmail.com

ARTICLE INFO

Keywords: Personal Data Protection, Digital Transformation, Legal Education, Indonesia, Thailand

Received : 17, April

Revised : 19, June

Accepted: 21, August

©2026 Mutmainah, Irhamdessetya, Suyanto, Iswandari, Irawan: This is an open-access article distributed under the terms of the [Creative Commons Atribusi 4.0 Internasional](https://creativecommons.org/licenses/by-sa/4.0/).



ABSTRACT

Digital transformation in Indonesia and Thailand has increased the use of personal data in electronic services, while also intensifying risks of misuse, data breaches, and limited public legal awareness. This study aims to analyze the regulation of personal data protection education in the legal systems of Indonesia and Thailand and to compare the role of the state in strengthening digital legal literacy. This research uses a normative legal method with statutory, conceptual, and comparative approaches. Data were collected through library research on primary and secondary legal materials, without respondents or informants, and analyzed using qualitative juridical analysis. The findings show that both countries have established personal data protection frameworks, but public education requires more systematic implementation. This study highlights legal education as an essential instrument for protecting digital society.

INTRODUCTION

Digital transformation has altered the relationship among society, the state, and electronic service providers because almost every social, economic, educational, and governmental activity now generates personal data that can be processed on a large scale. At the beginning of 2024, the number of global internet users reached 5.35 billion, while Indonesia had 185.3 million internet users and Thailand had 63.21 million internet users (Kemp, 2024a, 2024b, 2024c). This condition shows that personal data protection is no longer merely a technical issue, but a public legal concern related to the right to privacy, digital security, and public trust. The World Bank (2021) emphasizes that data can generate social and economic value, but it also requires governance capable of preventing misuse and building trust. Therefore, personal data protection education is an urgent necessity so that society does not merely function as users of digital services, but also as legal subjects who understand their rights, risks, and mechanisms of protection.

In the context of Southeast Asia, Indonesia and Thailand occupy important positions because both countries have rapidly developing digital ecosystems and specific legal frameworks on personal data protection. Indonesia enacted Law Number 27 of 2022 concerning Personal Data Protection, which positions personal data protection as part of human rights and recognizes public participation through education, training, advocacy, socialization, and supervision (Republic of Indonesia, 2022). Thailand has enacted the Personal Data Protection Act, Buddhist Era (BE) 2562 (2019), which mandates the personal data protection committee and office to improve public understanding and provide training for data controllers, data processors, data protection officers, employees, service providers, and the general public (Kingdom of Thailand, 2019). The Association of Southeast Asian Nations (2021a) also emphasizes the need to harmonize data protection principles and cross-border data governance to build trust in the regional digital economy. Thus, comparing Indonesia and Thailand is relevant to examine how legal norms not only regulate prohibitions and sanctions, but also shape the legal awareness of digital society.

Theoretically, personal data protection is related to the theory of the right to privacy, digital consumer protection theory, and the concept of the rule of law, which requires the state to provide both normative guarantees and mechanisms for public empowerment. Greenleaf (2023) shows that by 2023 there were 162 national data privacy laws worldwide, indicating a global tendency toward increasingly institutionalized privacy protection. However, Solove (2021) criticizes the view that simplifies user behavior through the concept of the privacy paradox, because user choices are often influenced by information asymmetry, service design, and limited ability to understand risks. This critique is important for the present study because legal education cannot be understood merely as the delivery of information, but as a process of strengthening citizens' capacity to assess consent, processing purposes, and the legal consequences of providing personal data. On this basis, personal data protection education can be positioned as a bridge between written legal norms and public behavior in the digital space.

Previous studies show that the enactment of legislation is not always followed by adequate social and institutional readiness. Syailendra et al. (2024) found that Law Number 27 of 2022 concerning Personal Data Protection represents an important step for Indonesia, but its implementation still faces governmental challenges in establishing an effective protection system. Faisal and Zuliarti (2024) emphasize the existence of an awareness gap in Indonesian society, because legal protection will not be effective if individuals do not understand their rights and the threats to their personal data. Wibowo et al. (2024) also show that personal data protection has implications for consumer trust and digital economic development, especially after data breach cases on electronic commerce platforms. These findings indicate that legal research on personal data protection needs to move beyond formal compliance analysis toward legal education analysis as a prerequisite for the effectiveness of norms.

In the Thai context, Ketmaneechairat et al. (2024) discuss the integration of personal data protection and data governance, showing that compliance with the Personal Data Protection Act, BE 2562 (2019), requires a management framework that can be applied by organizations. However, their study focuses more strongly on organizational compliance management than on legal education for the public as data subjects. Soemitro et al. (2023) show that personal data protection models in several countries may differ between repressive approaches through sanctions and preventive approaches through education, indicating that the educational aspect must be placed as an important part of legal policy. The research gap lies in the limited normative-comparative studies that specifically compare the educational mandate within the personal data protection laws of Indonesia and Thailand. Therefore, this study is based on the scholarly need to assess the extent to which personal data protection education is positioned as a state obligation, a mechanism of public participation, and a risk-prevention strategy in the era of digital transformation.

This study aims to analyze the regulation of personal data protection education in Indonesian and Thai law and to compare the normative construction of the roles of the state, supervisory authorities, and society in building digital legal literacy. It also aims to identify similarities, differences, and weaknesses in the regulation of legal education in both countries by using a normative legal approach based on statutory, conceptual, and comparative analysis. Theoretically, this study contributes to the development of personal data protection law studies by positioning education as a normative element that determines the effectiveness of the right to privacy. Practically, this study may serve as input for policymakers, supervisory institutions, educational institutions, and electronic system providers in designing more structured digital legal literacy programs. Accordingly, this study is expected to strengthen the understanding that personal data protection cannot be built only through rules and sanctions, but requires continuous education capable of transforming the awareness and behavior of digital society.

THEORETICAL REVIEW

Digital Transformation and the Growth of Personal Data Risks

Digital transformation has significantly changed the way individuals interact with public services, private companies, educational institutions, financial platforms, and social media. In this digital environment, personal data is continuously collected, stored, analyzed, and exchanged as part of electronic transactions and online communication. At the global level, approximately 5.5 billion people were online in 2024, representing 68 percent of the world's population and confirming that digital interaction has become a dominant feature of contemporary society (International Telecommunication Union, 2024). In Indonesia, 72.78 percent of the population aged five years and over accessed the internet in 2024, while in Thailand, 90.87 percent of the population used the internet in the same year (Statistics Indonesia, 2025; World Bank, 2024). These figures demonstrate that personal data protection is increasingly urgent because the expansion of digital participation also increases exposure to data misuse, identity theft, fraud, unauthorized profiling, and data breaches.

The World Bank (2021) explains that data can support development, innovation, and better public services, but it can also create harm when governance, accountability, and public trust are weak. This argument is relevant to Indonesia and Thailand because both countries are experiencing rapid digitalization while also facing challenges in strengthening citizens' awareness of data protection. The Organisation for Economic Co-operation and Development (2024) also emphasizes that privacy concerns and lack of control over personal data can affect public trust in digital platforms. Therefore, the digital transformation era requires not only technological infrastructure, but also legal education that enables citizens to understand the risks and legal consequences of sharing personal data. In this context, personal data protection education becomes a preventive strategy to reduce vulnerability in digital society.

Personal Data Protection as a Human Rights and Legal Protection Issue

Personal data protection is closely related to the right to privacy, human dignity, personal autonomy, legal certainty, and consumer protection. Solove (2021) argues that privacy problems should not be understood merely as individual failure to protect information, because users often face complex systems, information asymmetry, and limited bargaining power. This view is important because digital users may give consent without fully understanding the purpose, scope, and consequences of data processing. Greenleaf (2023) shows that personal data protection has become a global legal trend, with many countries establishing national data privacy laws to protect individuals in digital environments. Thus, personal data protection has developed from a technical issue into a legal and human rights concern.

In the Indonesian context, personal data protection has been formally recognized through Law Number 27 of 2022 concerning Personal Data Protection. This law regulates the rights of data subjects, obligations of personal data controllers and processors, data transfer, sanctions, and public participation in personal data protection (Republic of Indonesia, 2022). In Thailand, the Personal Data Protection Act, BE 2562 (2019), establishes legal principles concerning consent, sensitive personal data, rights of data subjects, duties of data controllers, complaint mechanisms, and sanctions (Kingdom of Thailand, 2019). Both legal frameworks show that personal data protection is no longer optional, but part of the legal responsibility of the state and electronic service providers. However, legal protection will be meaningful only when society understands the rights and remedies provided by law.

Legal Education and Digital Literacy as Preventive Protection

Legal education plays an important role in transforming formal legal rights into practical public capacity. In the context of personal data protection, education helps individuals understand what personal data is, how it may be processed, why consent matters, and what legal steps can be taken when violations occur. Soemitro et al. (2023) explain that personal data protection systems may rely on both repressive approaches through sanctions and preventive approaches through education. Preventive protection is especially important because data misuse often occurs before individuals are aware that their rights have been violated. Therefore, personal data protection education should be understood as an essential component of digital legal literacy.

Digital literacy and legal literacy should be integrated because personal data risks often arise from everyday online behavior. Citizens may share identity cards, passwords, one-time passwords, banking information, health data, location data, or biometric data without understanding the risks. Faisal and Zuliarti (2024) identify an awareness gap in Indonesia's cyberspace, showing that legal protection is difficult to implement effectively when citizens do not understand their rights and the threats to their personal data. The Organisation for Economic Co-operation and Development (2024) also notes that privacy concerns and perceived lack of control over personal data influence how individuals interact with websites, applications, and social media. Therefore, education on personal data protection should include practical skills, such as reading privacy notices, managing consent, recognizing phishing, protecting digital identity, and reporting violations.

Comparative Legal Framework of Indonesia and Thailand

Indonesia and Thailand provide relevant comparative cases because both countries have enacted specific personal data protection laws while operating within fast-growing digital ecosystems. Indonesia's Law Number 27 of 2022 contains an explicit public participation provision in Article 63, which includes education, training, advocacy, socialization, and supervision as part of personal data protection (Republic of Indonesia, 2022). This provision shows that the Indonesian legal framework recognizes the importance of public involvement in strengthening legal awareness. Thailand's Personal Data Protection Act, BE 2562 (2019), also contains educational elements through the authority of the Personal Data Protection Committee and the Office of the Personal Data Protection Committee. Section 16 and Section 44 provide a basis for promoting public understanding, academic services, knowledge development, and training related to personal data protection (Kingdom of Thailand, 2019).

The comparison shows that both countries recognize education as part of personal data protection, but they differ in institutional emphasis. Indonesia emphasizes public participation within the general structure of personal data protection, while Thailand gives clearer institutional duties to specific personal data protection bodies. Ketmaneechairat et al. (2024) argue that Thailand's personal data protection implementation requires integration with data governance and organizational compliance systems. Meanwhile, Syailendra et al. (2024) explain that Indonesia's personal data protection law still faces challenges related to implementation, institutional readiness, and enforcement. These differences indicate that comparative analysis is important to understand how legal education can be structured as both a public participation mechanism and an institutional responsibility.

Regional Governance, Research Gap, and Conceptual Relevance

Personal data protection in Indonesia and Thailand cannot be separated from broader regional data governance in Southeast Asia. The Association of Southeast Asian Nations (2021b) developed the Data Management Framework to support responsible data management and strengthen trust in the digital economy. The Association of Southeast Asian Nations (2021c) also introduced Model Contractual Clauses for Cross-Border Data Flows, which provide contractual tools for personal data transfer across jurisdictions. These regional instruments are relevant because personal data processing often crosses national borders through electronic commerce, financial technology, cloud services, social media platforms, and digital public services. Therefore, personal data protection education must also include awareness of cross-border risks and the responsibilities of organizations that process data beyond national boundaries.

Previous studies have discussed personal data protection from the perspectives of legal reform, privacy rights, organizational compliance, data governance, and economic development. Syailendra et al. (2024) focus on challenges and opportunities in Indonesia's personal data protection law, while Wibowo et al. (2024) examine the relationship between personal data protection and economic development. Ketmaneechairat et al. (2024) analyze the integration of personal data protection and data governance in Thailand, but their study focuses more on organizational management than public legal education. This shows a research gap because limited studies specifically compare personal data protection education in Indonesia and Thailand through a normative legal approach. Therefore, the present study contributes theoretically by positioning education as a core element of personal data protection law and contributes practically by offering insights for policymakers, supervisory authorities, educational institutions, and electronic system providers in strengthening digital legal literacy.

METHODOLOGY

Research Type and Approach

This study employed normative legal research with a qualitative juridical design. Normative legal research was selected because the study focuses on legal norms, statutory provisions, legal principles, and institutional mandates concerning personal data protection education in Indonesia and Thailand. This method is appropriate for examining written law as a doctrinal system and for evaluating how legal provisions define rights, obligations, and public education mechanisms in the digital era (Varuhas, 2023). The study used three approaches, namely the statutory approach, the conceptual approach, and the comparative approach. The statutory approach was used to examine relevant regulations, the conceptual approach was used to analyze legal concepts such as privacy, consent, public participation, and digital legal literacy, while the comparative approach was used to compare the legal regulation of personal data protection education in Indonesia and Thailand.

Legal Materials and Selection Technique

This study did not involve a population, sample, respondents, or informants because it was not designed as empirical field research. Instead, the object of the study consisted of legal materials selected through purposive legal material selection based on relevance, authority, accessibility, and direct connection to the research topic. The primary legal materials included the Constitution of the Republic of Indonesia, Law Number 27 of 2022 concerning Personal Data Protection, Law Number 11 of 2008 concerning Electronic Information and Transactions as amended, Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, the Constitution of the Kingdom of Thailand BE 2560 (2017), and the Personal Data Protection Act, BE 2562 (2019). Secondary legal materials consisted of journal articles, books, official reports, and institutional publications discussing privacy rights, personal data protection, digital transformation, and legal education from 2020 to 2024. Tertiary legal materials included legal dictionaries,

legal encyclopedias, official databases, and supporting indexes used to clarify terminology and verify legal sources.

Data Collection Technique and Research Instrument

Data were collected through library research and legal documentation study. Library research was used because normative legal research relies on the examination of legal texts, scholarly writings, and authoritative documents to answer legal questions through doctrinal analysis (Al Amaren et al., 2020). The main research instrument was a legal material review sheet developed by the researcher to classify legal provisions, identify educational mandates, record institutional responsibilities, and compare normative arrangements between Indonesia and Thailand. The use of a structured review sheet is consistent with document analysis, which requires researchers to prepare materials, extract relevant information, analyze the content, and distill findings systematically (Dalglish et al., 2020).

The items in the review sheet were derived from the research objectives and from key legal concepts in personal data protection law, including data subject rights, public participation, consent, legal literacy, institutional duties, complaint mechanisms, and preventive protection. Since this study did not use questionnaires, interviews, or measurement scales, statistical validity and reliability tests were not applied. Instead, the credibility of the data was maintained through source authentication, cross-checking of official legal documents, consistency review between primary and secondary legal materials, and systematic comparison of legal provisions. This procedure is appropriate because doctrinal legal research is concerned with methodically finding, examining, explaining, and justifying enacted legal frameworks, while legal problems are addressed through the analysis and interpretation of legal norms and authoritative legal sources (Majeed et al., 2023; Nyathi, 2023).

Research Procedure

The research was conducted in several sequential stages. The first stage was problem identification, which involved formulating the legal issue of personal data protection education in the context of digital transformation in Indonesian and Thai societies. The second stage was the collection of primary and secondary legal materials from official legal databases, government websites, academic journal databases, and international institutional reports. The third stage involved classification of legal materials based on jurisdiction, legal hierarchy, subject matter, and relevance to public education, digital literacy, and data protection rights. The fourth stage consisted of legal interpretation, including grammatical, systematic, and teleological interpretation to understand the meaning, purpose, and function of relevant legal provisions. The final stage involved comparative analysis to identify similarities, differences, strengths, and weaknesses in the regulation of personal data protection education in Indonesia and Thailand.

Data Analysis Technique

The data were analyzed using qualitative juridical analysis. This analysis was conducted by interpreting legal norms, examining the relationship among statutory provisions, assessing the coherence of legal principles, and comparing the normative structure of personal data protection education in Indonesia and Thailand. The comparative analysis focused on three main dimensions, namely the legal basis of personal data protection education, the institutional responsibility for public education, and the position of society as a participant in data protection governance. The analysis was supported by Zotero for reference management and Microsoft Excel for organizing legal materials, coding legal themes, and mapping similarities and differences between the two jurisdictions. The results of the analysis were presented descriptively and argumentatively to produce a systematic legal explanation regarding the role of education as a preventive instrument in personal data protection law.

RESEACRH RESULTS

Normative Recognition of Personal Data Protection in Indonesia and Thailand

The analysis shows that Indonesia and Thailand have both established personal data protection as a legal concern within their national legal systems. In Indonesia, personal data protection is regulated through Law Number 27 of 2022 concerning Personal Data Protection, which provides the main legal basis for data subject rights, personal data processing, obligations of personal data controllers and processors, cross-border transfer, administrative sanctions, and public participation. In Thailand, personal data protection is regulated through the Personal Data Protection Act, BE 2562 (2019), which governs consent, sensitive personal data, data subject rights, data controller duties, data processor obligations, complaint mechanisms, and sanctions. The findings indicate that both legal systems recognize personal data protection not merely as a technical matter, but as a legal framework related to privacy, digital security, and public trust. This normative recognition forms the foundation for strengthening public education in the era of digital transformation.

Table 1 presents the primary legal materials examined in this study and summarizes their main normative relevance to personal data protection. The table identifies the legal instruments that form the basis of analysis in Indonesia and Thailand, including laws, government regulations, and constitutional provisions. These materials were selected because they directly regulate or support the protection of personal data, electronic system governance, privacy rights, and institutional responsibilities in the digital environment. The purpose of this table is to show that both countries already have formal legal foundations for regulating personal data protection, although the scope and emphasis of each legal instrument differ.

Table 1. Primary Legal Materials and Main Normative Findings

Jurisdiction	Primary Legal Material	Main Finding
Indonesia	Law Number 27 of 2022 concerning Personal Data Protection	Establishes personal data protection rights, obligations of controllers and processors, data transfer rules, sanctions, and public participation.
Indonesia	Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions	Supports the regulation of electronic system governance and digital accountability.
Thailand	Personal Data Protection Act, Buddhist Era (BE) 2562 (2019)	Establishes consent requirements, sensitive data protection, data subject rights, institutional duties, complaint mechanisms, and sanctions.
Thailand	Constitution of the Kingdom of Thailand Buddhist Era (BE) 2560 (2017)	Provides constitutional protection related to privacy and personal rights.

Based on Table 1, the findings indicate that Indonesia's personal data protection framework is primarily centered on Law Number 27 of 2022 concerning Personal Data Protection, supported by regulations on electronic systems and transactions. Meanwhile, Thailand's framework is primarily based on the Personal Data Protection Act, BE 2562 (2019), and supported by constitutional recognition of privacy-related rights. These legal materials demonstrate that both jurisdictions recognize personal data protection as a formal legal issue. However, the table also shows that personal data protection is not regulated in isolation, but is connected to broader issues of electronic system governance, privacy, institutional responsibility, and public trust.

Educational Mandates in Personal Data Protection Law

The study found that both Indonesia and Thailand include educational elements in their personal data protection frameworks, although their formulations differ. In Indonesia, Article 63 of Law Number 27 of 2022 recognizes public participation in personal data protection through education, training, advocacy, socialization, and supervision. This provision shows that Indonesian law places society as an active participant in the protection of personal data. In Thailand, the Personal Data Protection Act, BE 2562 (2019), assigns educational functions to institutional bodies, especially through the Personal Data Protection Committee and the Office of the Personal Data Protection Committee. The findings indicate that Indonesia emphasizes public participation, while Thailand

provides a more institutionally structured mandate for promoting public understanding and training.

Table 2 compares the educational mandates contained in the personal data protection frameworks of Indonesia and Thailand. The comparison focuses on four main aspects, namely the legal basis for education, the main form of education, the actors emphasized by the law, and the normative orientation of each legal system. This table is important because the central focus of the study is not only the existence of personal data protection laws, but also how these laws position education as a mechanism for strengthening public awareness. By presenting these aspects side by side, the table clarifies the similarities and differences between Indonesia and Thailand in regulating personal data protection education.

Table 2. Comparison of Educational Mandates in Indonesia and Thailand

Aspect	Indonesia	Thailand
Legal basis for education	Article 63 of Law Number 27 of 2022	Section 16 and Section 44 of the Personal Data Protection Act, Buddhist Era (BE) 2562 (2019)
Main form of education	Education, training, advocacy, socialization, and supervision	Promotion of public understanding, knowledge services, and training programs
Main actor emphasized	Society and public participation	Personal Data Protection Committee and Office of the Personal Data Protection Committee
Normative orientation	Participatory legal awareness	Institutional legal education and compliance support

The comparison in Table 2 shows that Indonesia and Thailand both recognize education as part of personal data protection, but they structure it differently. Indonesia emphasizes public participation through education, training, advocacy, socialization, and supervision, which reflects a participatory model of legal awareness. Thailand, on the other hand, places stronger emphasis on institutional responsibility by assigning educational and training functions to the Personal Data Protection Committee and the Office of the Personal Data Protection Committee. This finding indicates that Indonesia provides a broader participatory basis, while Thailand offers a more structured institutional mandate. Therefore, both approaches reveal different strengths in developing personal data protection education for digital society.

Institutional Responsibility for Digital Legal Literacy

The analysis shows that institutional responsibility is an important element in both countries, but Thailand provides a more explicit institutional structure for personal data protection education. Thailand's legal framework assigns educational and training-related duties to the Personal Data Protection Committee and the Office of the Personal Data Protection Committee. These duties include promoting public understanding, providing knowledge services, and developing training programs for data controllers, data processors, data protection officers, service providers, and the general public. In Indonesia, the law recognizes public participation in education and socialization, but the institutional mechanism for systematic public education still requires clearer operational implementation. This finding confirms that both countries recognize legal education, but Thailand's law presents a more direct institutional mandate for structured training and public knowledge development.

Data Subject Rights and Public Awareness

The study found that the effectiveness of personal data protection depends not only on the existence of rights in statutory provisions, but also on public understanding of those rights. Indonesian law recognizes various rights of data subjects, including the right to information, access, correction, deletion, withdrawal of consent, objection, and compensation. Thailand's law also recognizes important data subject rights, including the right to access, request correction, object to processing, withdraw consent, and submit complaints. However, the findings indicate that these rights may not be fully effective if individuals lack sufficient legal literacy to understand when their rights are violated and how remedies can be used. Therefore, public education becomes a necessary bridge between formal legal protection and the practical ability of citizens to protect their personal data.

Preventive Function of Personal Data Protection Education

The analysis shows that personal data protection education functions as a preventive legal instrument. Education helps citizens identify risks before violations occur, including misuse of identity documents, unlawful disclosure of financial data, unauthorized profiling, phishing, and weak consent practices. The findings also show that preventive protection is especially important because digital harms may occur quickly and may involve multiple platforms or cross-border processing. In this context, education should not be limited to general awareness campaigns, but should include practical knowledge about consent, privacy notices, complaint procedures, data subject rights, digital identity protection, and safe behavior in electronic services. This result supports the article's objective of positioning legal education as an essential instrument for protecting digital society.

Comparative Findings on Indonesia and Thailand

The comparative analysis identifies both similarities and differences between Indonesia and Thailand. The main similarity is that both countries already recognize personal data protection as a legal obligation and include educational elements in their regulatory frameworks. The main difference lies in the structure of educational responsibility. Indonesia emphasizes public participation through education, training, advocacy, socialization, and supervision, while Thailand gives clearer institutional duties to its personal data protection authority. Another difference is that Indonesia's framework still requires stronger operational mechanisms for systematic public education, while Thailand's framework more clearly links education with institutional knowledge services and training. These differences indicate that Indonesia may strengthen the practical implementation of public education, while Thailand may further ensure that institutional education reaches broader society as data subjects.

Table 3 summarizes the key research findings based on the thematic analysis conducted in this study. The table connects each major theme with its main finding and its implication for the article. The themes include legal recognition, educational mandate, institutional responsibility, data subject rights, preventive protection, and comparative gaps between Indonesia and Thailand. This table is designed to provide an integrated overview of the findings so that the relationship between legal norms, public education, and digital society protection can be understood more clearly.

Table 3. Summary of Key Research Findings

Theme	Key Finding	Implication for the Article
Legal recognition	Both countries have specific personal data protection frameworks.	Personal data protection is a formal legal issue in both jurisdictions.
Educational mandate	Indonesia emphasizes public participation, while Thailand emphasizes institutional education.	Legal education is recognized but structured differently.
Institutional responsibility	Thailand has clearer institutional training duties than Indonesia.	Indonesia needs more systematic implementation mechanisms.
Data subject rights	Both countries recognize data subject rights.	Rights require public legal literacy to be effective.
Preventive protection	Education helps prevent misuse, breaches, and weak consent practices.	Legal education should be treated as a preventive instrument.
Comparative gap	Indonesia and Thailand share similar goals but differ in operational structure.	Comparative analysis strengthens the article's contribution.

Table 3 confirms that both Indonesia and Thailand have developed legal frameworks for personal data protection, but the implementation of public education remains an important area for improvement. The findings show that legal recognition alone is insufficient if society does not understand personal data rights, consent mechanisms, complaint procedures, and digital risks. The table also highlights that Indonesia and Thailand share similar objectives in protecting personal data, but differ in the structure of educational responsibility. Indonesia emphasizes public participation, while Thailand emphasizes institutional education and training. Overall, the table reinforces the main result of this study that personal data protection education should be treated as a preventive and enabling legal mechanism in the era of digital transformation.

Differences from Previous Studies

The findings differ from several previous studies because this article places personal data protection education as the central object of analysis. Earlier studies on Indonesia mainly emphasized legal reform, implementation challenges, institutional readiness, data breaches, consumer trust, and economic development. Studies on Thailand mostly focused on compliance, organizational data governance, and management systems. In contrast, this article finds that education is not merely a supporting policy, but a normative component that determines whether personal data protection rights can be understood and used by society. This distinction is important because the effectiveness of personal data protection does not depend only on the existence of sanctions or institutional rules, but also on the ability of society to understand risks, exercise rights, and participate in digital legal protection.

Overall, the study finds that Indonesia and Thailand have established legal frameworks for personal data protection, but public education remains an area that requires more systematic strengthening. Indonesia provides a strong participatory basis through Article 63 of Law Number 27 of 2022, while Thailand provides clearer institutional duties through the Personal Data Protection Act, BE 2562 (2019). The comparison shows that both systems can complement each other conceptually: Indonesia highlights public participation, whereas Thailand highlights institutional responsibility. The main result of this study is that personal data protection education should be positioned as a preventive and enabling legal mechanism. It enables digital society to understand personal data rights, avoid digital risks, and participate more effectively in personal data protection governance.

DISCUSSION

Personal Data Protection Education as a Normative Requirement in Digital Society

The main finding of this study shows that personal data protection education has become a normative requirement in the digital transformation era, particularly in Indonesia and Thailand. This finding confirms that personal data protection is not only a matter of regulating data controllers, processors, consent, and sanctions, but also a matter of empowering citizens as data subjects. In legal theory, the effectiveness of rights depends not only on their recognition in written law, but also on the ability of legal subjects to understand and exercise those rights. This is consistent with Solove (2021), who argues that privacy problems cannot be reduced to individual choices because users often face information asymmetry, complex digital systems, and limited bargaining power. Therefore, education becomes essential because citizens cannot meaningfully protect their personal data if they do not understand the meaning of consent, data processing purposes, privacy notices, complaint mechanisms, and legal remedies.

The findings also support the concept that legal education functions as a bridge between formal legal norms and social behavior. Indonesia and Thailand have both established legal frameworks for personal data protection, but the existence of legal provisions alone does not automatically produce public awareness. This is relevant to Greenleaf (2023), who shows that the global growth of data privacy laws reflects the institutionalization of privacy protection, yet legal adoption must still be followed by implementation and public understanding. In the context of this study, personal data protection education becomes a mechanism for translating abstract legal rights into practical digital behavior. Thus, the results contribute to the development of personal data protection law by positioning education as a core legal element rather than a secondary public policy activity.

Comparative Meaning of the Indonesian and Thai Legal Frameworks

The comparison between Indonesia and Thailand shows that both countries recognize personal data protection education, but they construct it through different normative models. Indonesia emphasizes public participation through education, training, advocacy, socialization, and supervision under Law Number 27 of 2022 concerning Personal Data Protection. This model indicates that society is positioned as an active participant in personal data protection governance. Thailand, on the other hand, provides a more institutionally structured model through the Personal Data Protection Committee and the Office of the Personal Data Protection Committee under the Personal Data Protection Act, BE 2562 (2019). This structure places stronger responsibility on state institutions to promote public understanding, provide knowledge services, and develop training programs.

The consequence of this difference is significant. Indonesia's model is normatively participatory, but it requires stronger operational mechanisms to ensure that public participation becomes systematic and measurable. Thailand's model is institutionally clearer, but it must ensure that institutional education does not remain limited to organizational compliance or professional training. Ketmaneechairat et al. (2024) show that Thailand's personal data protection implementation is strongly connected to organizational compliance and data governance systems. This supports the finding that Thailand has a clearer institutional orientation, but it also reveals the need to expand education toward ordinary citizens as data subjects. Therefore, the Indonesian and Thai approaches can be seen as complementary: Indonesia offers a broader participatory orientation, while Thailand offers a clearer institutional basis for structured education.

Public Awareness and the Effectiveness of Data Subject Rights

Another important finding is that data subject rights will not be fully effective without public legal awareness. Both Indonesia and Thailand recognize rights such as access, correction, withdrawal of consent, objection, and complaint submission. However, these rights require citizens to know when their data is being processed, how consent is given, what risks may arise, and which legal remedies are available. Faisal and Zuliarti (2024) emphasize that Indonesia still faces an awareness gap in personal data privacy, meaning that citizens may be formally protected by law but practically unable to use that protection. This finding supports the argument that legal rights without legal literacy may become passive rights.

This result also has implications for digital consumer protection and public trust. Wibowo et al. (2024) show that personal data protection is closely related to Indonesia's economic development because data breaches and weak protection can reduce consumer trust in digital platforms. In this study, education is therefore interpreted as an enabling instrument that strengthens the practical use of legal rights and supports public confidence in electronic services. If citizens understand their rights, they are more likely to evaluate privacy notices, manage consent, avoid unsafe data-sharing practices, and report violations. Consequently, personal data protection education contributes not only to individual privacy, but also to the sustainability of the digital economy and public trust in digital governance.

Preventive Protection and the Limits of Sanction-Based Regulation

The findings indicate that personal data protection education has a preventive function. This preventive function is important because digital harms often occur before citizens realize that their rights have been violated. Data misuse, identity theft, phishing, unauthorized profiling, and unlawful data disclosure may happen quickly and may involve multiple platforms or cross-border processing. Soemitro et al. (2023) explain that personal data protection systems may differ between repressive models based on sanctions and preventive models based on education. The results of this study support the preventive model because education can reduce risk before legal violations occur.

The implication is that sanctions alone are insufficient to protect society in the digital era. Sanctions are important for accountability, but they usually operate after a violation has occurred. Education, by contrast, equips citizens with knowledge and practical skills before harm takes place. This includes understanding privacy notices, recognizing suspicious digital requests, protecting identity documents, managing one-time passwords, understanding biometric and financial data risks, and submitting complaints when violations occur. Therefore, education should be integrated into personal data protection governance as a preventive legal mechanism. This finding strengthens the argument that digital legal literacy should become part of national data protection policy in both Indonesia and Thailand.

Relationship Between Findings and Previous Studies

The findings of this study both support and differ from previous studies. They support Syailendra et al. (2024), who found that Indonesia's Personal Data Protection Law creates important opportunities but also faces implementation challenges. This study confirms that one of those implementation challenges is the need for systematic public education. The findings also support Faisal and Zuliarti (2024), who emphasize the awareness gap in Indonesia's cyberspace. However, this study extends their argument by comparing Indonesia with Thailand and by showing that public awareness is not only a social problem, but also a normative issue that should be addressed through legal design.

The study differs from Ketmaneechairat et al. (2024), whose analysis focuses more strongly on data governance and organizational compliance in Thailand. While their study is important for understanding institutional and organizational readiness, the present study places society as the central subject of legal education. The study also differs from Wibowo et al. (2024), who connect personal data protection with economic development and consumer trust. This research accepts that economic trust is important, but it broadens the analysis by arguing that legal education is a prerequisite for the effective exercise of privacy rights and public participation. Therefore, the contribution of this study lies in shifting the focus from mere legal compliance and economic protection toward education as a normative and preventive element of personal data protection law.

Factors Influencing the Research Findings

Several factors influence the findings of this study. The first factor is the maturity of each country's institutional framework. Thailand's Personal Data Protection Act provides clearer institutional mandates for promoting public understanding and training, while Indonesia's Personal Data Protection Law recognizes public participation but still requires more detailed operational implementation. The second factor is the level of digital transformation in both countries. High internet penetration and dependence on digital services increase the urgency of personal data protection education because more citizens are exposed to digital risks. The third factor is the complexity of digital platforms, which makes it difficult for ordinary users to understand data processing practices without continuous education.

The fourth factor is the relationship between legal literacy and digital literacy. Citizens may know how to use digital services but may not understand the legal consequences of sharing personal data. This creates a gap between technological participation and legal awareness. The Organisation for Economic Co-operation and Development (2024) emphasizes that privacy concerns and lack of control over data can affect trust in digital environments. This supports the finding that education must not only explain legal provisions, but also develop practical skills for safe digital behavior. Therefore, the factors influencing the findings are legal, institutional, technological, and social at the same time.

Scientific Contribution of the Study

This study contributes to the development of personal data protection law by positioning education as a central component of legal effectiveness. Theoretically, it expands the understanding of privacy law by showing that the protection of personal data depends not only on legal recognition, but also on citizens' ability to understand and exercise their rights. This contributes to legal scholarship by integrating personal data protection, public legal education, and digital literacy within a single normative-comparative framework. The study also strengthens the concept that legal education can function as preventive protection in the digital era. In this way, the research contributes to a broader understanding of how law can respond to the risks of digital transformation.

Practically, this study provides insights for policymakers, supervisory authorities, educational institutions, and electronic system providers. For Indonesia, the findings suggest the need to operationalize public participation under Law Number 27 of 2022 through structured national education programs, sectoral guidelines, and public-facing complaint literacy. For Thailand, the findings suggest the need to ensure that institutional training under the Personal Data Protection Act reaches not only organizations and professionals, but also ordinary citizens as data subjects. The study also suggests that public education should include practical materials on consent, privacy notices, data subject rights, complaint procedures, digital identity protection, and cross-border data risks. Therefore, the study has both theoretical and practical relevance for strengthening digital society.

CONCLUSIONS AND RECOMMENDATIONS

This study concludes that Indonesia and Thailand have established normative legal frameworks for personal data protection in response to the risks of digital transformation. Indonesia regulates personal data protection through Law Number 27 of 2022, which recognizes public participation through education, training, advocacy, socialization, and supervision. Thailand, through the Personal Data Protection Act, BE 2562 (2019), provides a more institutionally structured mandate by assigning educational and training functions to the Personal Data Protection Committee and the Office of the Personal Data Protection Committee. The main finding of this study shows that personal data protection education is not merely a supporting activity, but an essential preventive legal instrument for strengthening digital legal literacy, improving public awareness, and enabling citizens to exercise their rights as data subjects.

Based on these findings, this study recommends that Indonesia strengthen the operational implementation of public education under its personal data protection framework through structured national programs, sectoral guidelines, and accessible public complaint literacy. Thailand is also recommended to expand its institutional education model so that training and public understanding programs reach not only data controllers, data processors, and professionals, but also ordinary citizens as data subjects. Both countries should integrate personal data protection education into schools, universities, public institutions, digital platforms, and community-based literacy programs. Such efforts are necessary to ensure that personal data protection is not limited to formal legal compliance, but becomes a practical mechanism for protecting digital society.

ADVANCED RESEARCH

Future research should examine the practical implementation and effectiveness of personal data protection education in Indonesia and Thailand through empirical methods. Surveys, interviews, or mixed-method studies may be conducted to measure citizens' understanding of consent, privacy notices, data subject rights, complaint mechanisms, and digital security risks. Further studies may also compare Indonesia and Thailand with other Southeast Asian countries to identify regional patterns of digital legal literacy and personal data protection governance. In addition, future research can develop an educational model or curriculum for personal data protection that can be applied in formal education, public institutions, and digital service platforms.

ACKNOWLEDGMENT

The authors would like to express their sincere appreciation to Ngudi Waluyo University, Indonesia, and Thai Global Business Administration Technological College for their academic support in the preparation of this study. The authors also extend their gratitude to colleagues and academic contributors who provided constructive suggestions during the development of this article. This acknowledgment is addressed to all parties who supported the completion of the research, particularly in strengthening the legal, comparative, and academic dimensions of personal data protection education in Indonesia and Thailand.

REFERENCES

- Al Amaren, E. M., Hamad, A. M. A., Al Mashhour, O. F., & Al Mashni, M. I. (2020). An introduction to the legal research method: To clear the blurred image on how students understand the method of the legal science research. *International Journal of Multidisciplinary Sciences and Advanced Technology*, 1(9), 50–55.
- Association of Southeast Asian Nations. (2021a). *Association of Southeast Asian Nations data management framework*.
- Association of Southeast Asian Nations. (2021b). *Association of Southeast Asian Nations digital masterplan 2025*.
- Association of Southeast Asian Nations. (2021c). *Association of Southeast Asian Nations model contractual clauses for cross-border data flows*.

- Dalglish, S. L., Khalid, H., & McMahon, S. A. (2020). Document analysis in health policy research: The READ approach. *Health Policy and Planning*, 35(10), 1424–1431. <https://doi.org/10.1093/heapol/czaa064>.
- Faisal, F., & Zuliarti, W. O. (2024). The awareness gap in personal data privacy in Indonesia's cyberspace. *International Journal of Social Science and Human Research*, 7(7), 5358–5362. <https://doi.org/10.47191/ijsshr/v7-i07-84>.
- Greenleaf, G. (2023). Global data privacy laws 2023: 162 national laws and 20 bills. *Privacy Laws & Business International Report*, 181, 1–4. <https://doi.org/10.2139/ssrn.4426146>.
- International Telecommunication Union. (2024). *Facts and figures 2024: Internet use*.
- Kemp, S. (2024a). *Digital 2024: Global overview report*. DataReportal.
- Kemp, S. (2024b). *Digital 2024: Indonesia*. DataReportal.
- Kemp, S. (2024c). *Digital 2024: Thailand*. DataReportal.
- Ketmaneechairat, H., Maliyaem, M., & Puttawattanakul, P. (2024). Towards a management system framework for the integration of personal data protection and data governance: A case study of Thai laws and practices. *International Journal of Technology*, 15(1), 219–229. <https://doi.org/10.14716/ijtech.v15i1.5885>.
- Kingdom of Thailand. (2017). *Constitution of the Kingdom of Thailand Buddhist Era 2560* (2017).
- Kingdom of Thailand. (2019). *Personal Data Protection Act, Buddhist Era 2562* (2019).
- Majeed, N., Hilal, A., & Khan, A. N. (2023). Doctrinal research in law: Meaning, scope and methodology. *Bulletin of Business and Economics*, 12(4), 559–563.
- Nyathi, M. (2023). Re-asserting the doctrinal legal research methodology in the South African academy: Navigating the maze. *South African Law Journal*, 140(2), 365–386. <https://doi.org/10.47348/SALJ/v140/i2a5>.
- Organisation for Economic Co-operation and Development. (2024). *Organisation for Economic Co-operation and Development digital economy outlook 2024, volume 2: Media consumption and privacy*.
- Republic of Indonesia. (1945). *The Constitution of the Republic of Indonesia of 1945*.
- Republic of Indonesia. (2008). *Law Number 11 of 2008 concerning Electronic Information and Transactions*.
- Republic of Indonesia. (2019). *Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions*.
- Republic of Indonesia. (2022). *Law Number 27 of 2022 concerning Personal Data Protection*.
- Soemitro, D. P., Wicaksono, M. A., & Putri, N. A. (2023). Penal provisions in the personal data protection law: A comparative legal study between Indonesia and Singapore. *SIGn Jurnal Hukum*, 5(1), 155–167. <https://doi.org/10.37276/sjh.v5i1.272>.
- Solove, D. J. (2021). The myth of the privacy paradox. *The George Washington Law Review*, 89(1), 1–51.
- Statistics Indonesia. (2025). *Telecommunication statistics in Indonesia 2024*. Statistics Indonesia.
- Syailendra, M. R., Lie, G., & Sudiro, A. (2024). Personal data protection law in Indonesia: Challenges and opportunities. *Indonesia Law Review*, 14(2), Article 4. <https://doi.org/10.15742/ilrev.v14n2.4>.
- Varuhas, J. N. E. (2023). Mapping doctrinal methods. In P. Daly & J. Tomlinson (Eds.), *Researching public law in common law systems* (pp. 101–128). Edward Elgar Publishing. <https://doi.org/10.2139/ssrn.4087836>.