Jurnal Kecerdasan Buatan dan Teknologi Informasi
Vol. 4, No. 3, September 2025, pp. 292-302
e-ISSN: 2964-2922, p-ISSN: 2963-6191
DOI : https://doi.org/10.69916/jkbti.v4i3.458

STATE RESPONSIBILITY IN PERSONAL DATA PROTECTION WITHIN THE ELECTRONIC-BASED GOVERNMENT SYSTEM

Muhammad Suhardi
Institut Pemerintahan Dalam Negeri, Indonesia
Email: muhammad@ipdn.ac.id

(Received: July 29, 2025; Revised: September 12, 2025; Accepted: September 17, 2025)

Abstract

This study examines the responsibility of the state in protecting personal data within Indonesia's Electronic-Based Government System. The objective is to analyze the legal obligations of government institutions as personal data controllers in digital public services and to formulate a normative framework that integrates the Personal Data Protection Law, SPBE governance, and the protection of citizens' constitutional rights. This research employs a qualitative legal method with a normative-juridical and conceptual approach. Data were collected through documentary study of Indonesian legal instruments concerning personal data protection, public services, government administration, electronic systems, and electronic-based government, supported by relevant scholarly literature on data governance and digital public administration. The findings show that Indonesia already has an important legal foundation for personal data protection and digital government, but the Personal Data Protection Law and SPBE framework have not yet been fully integrated. This regulatory fragmentation creates risks related to unclear institutional responsibility, excessive data processing, weak citizen notification, inaccurate data use, data breaches, and limited remedies. The study proposes the concept of the state as a constitutional data controller, meaning that government responsibility extends beyond technical compliance toward the protection of privacy, dignity, legal certainty, equality, and access to public services. This study contributes to strengthening a rights-based model of SPBE in Indonesia.

Keywords: constitutional data controller; digital government; electronic-based government system; personal data protection; state responsibility.

1. INTRODUCTION

The rapid expansion of digital government has transformed personal data into a core administrative resource. In electronic-based government systems, public institutions collect, store, exchange, verify, and process citizens' personal data to deliver services, manage population administration, distribute social assistance, issue licenses, provide health and education services, and support policy decisions. This transformation improves administrative efficiency, service integration, and data-driven governance, but it also creates serious legal risks when the state processes citizens' data without adequate safeguards. In Indonesia, this issue is particularly important because the Electronic-Based Government System, or *Sistem Pemerintahan Berbasis Elektronik* (SPBE), encourages interoperability and integrated digital services, while Law No. 27 of 2022 on Personal Data Protection regulates personal data processing, the rights of data subjects, and the obligations of personal data controllers and processors.

Personal data protection in digital government cannot be treated merely as an information-security issue. It is a constitutional and administrative law matter because personal data is closely connected to human dignity, privacy, legal identity, access to services, and protection from arbitrary state action. When citizens submit personal data to government platforms, they do not stand in an equal contractual relationship with the state. They are often legally required to provide data in order to obtain public services or exercise their rights. Therefore, the state has a higher duty of care than private entities. The government is not only a service provider, but also a public authority that holds constitutional obligations to respect, protect, and fulfil citizens' rights. This makes the state's position as a personal data controller in digital public services legally distinctive and normatively demanding [1]–[5].

In the Indonesian context, the problem becomes more complex because SPBE is designed to promote integrated government services, data sharing, interoperability, efficiency, and public-sector coordination. These objectives are legitimate and necessary for modern public administration. However, the more integrated government data systems become, the greater the risk of unauthorized access, excessive processing, data leakage, profiling, inaccurate data use, and unclear responsibility among public institutions. Previous research on the legal framework of personal data protection in SPBE has emphasized that the use of personal data in electronic government must accommodate the competing interests of the individual and the state, especially the individual interest in privacy and information security and the state interest in improving public service delivery [1]. This shows that the key issue is not whether

the government may process personal data, but how such processing can be made lawful, accountable, limited, secure, transparent, and rights-based.

The existing literature has developed several important discussions on personal data protection, digital government, and public-sector accountability. Rahman [1] examines the legal framework of personal data protection in the implementation of SPBE in Indonesia and identifies the need for stronger principles, data classification, access restrictions, and information-security standards. Syailendra, Lie, and Sudiro [2] analyze the challenges and opportunities of Indonesia's Personal Data Protection Law and argue that its enactment is an important step toward strengthening citizens' data protection. Badriah, Indiahono, and Sukarso [3] compare personal data protection accountability in Indonesia, South Korea, and Singapore and emphasize the importance of accountable policy innovation, institutional authority, and breach-reporting mechanisms. Wibowo [4] highlights the importance of personal data protection in Indonesia's digital economy, while Rahmawati and Wardana [5] relate privacy and personal data protection to constitutional guarantees in the era of government digitalization. These studies provide a strong foundation, but most of them still focus on general legal protection, policy comparison, or the implementation challenges of the Personal Data Protection Law.

A broader body of literature also discusses data governance and digital public administration. Schmeling, al Dakruni, and Mergel [6] show that data collaboration in digital government involves ecosystem, organizational, and individual dimensions, but research attention to standardization, privacy, security, and trust remains insufficient. Yukhno [7] argues that big-data governance requires a rethinking of public administration principles because digital government increasingly depends on large-scale data ecosystems. Degli Esposti, Ball, and Dibb [8] demonstrate that public-sector data use may be justified through public interest and national security arguments, yet such justification must still be balanced against individual rights. Meanwhile, studies on AI and public administration underline that digital government tools require transparency, accountability, institutional readiness, public trust, and human oversight [9]–[18]. These studies are relevant because personal data protection in SPBE is not only about data storage, but also about how state institutions use data to automate, integrate, and rationalize public governance.

Despite these contributions, there remains a specific gap in the literature: previous studies have not sufficiently integrated Indonesia's Personal Data Protection Law with SPBE governance and the constitutional protection of citizens' rights. Existing studies often discuss these issues separately. Personal data protection is examined as a privacy or cybersecurity issue, SPBE is examined as a digital government reform agenda, and constitutional rights are discussed as a broader normative guarantee. This article argues that these three dimensions must be integrated. The novelty of this study lies in its proposition that the state, when operating digital government services, must be legally understood as a constitutional data controller. This means that the government's obligation is not limited to technical security or regulatory compliance, but extends to the protection of citizens' constitutional rights in every stage of data processing within SPBE. Accordingly, this study aims to analyze the responsibility of the Indonesian state in protecting personal data within electronic-based government systems and to formulate a normative framework that integrates the Personal Data Protection Law, SPBE governance, and constitutional rights protection.

2. RESEARCH METHODS

This study employs a qualitative legal research method with a normative-juridical and conceptual approach. The qualitative method is appropriate because the object of this study is not statistical measurement, but the interpretation of legal norms, state obligations, institutional responsibilities, and constitutional rights in the protection of personal data within Indonesia's Electronic-Based Government System, or *Sistem Pemerintahan Berbasis Elektronik* (SPBE). Qualitative legal research enables the researcher to examine how legal texts, principles, and institutional practices interact in a particular regulatory context, especially when the issue concerns the relationship between the state, citizens, digital governance, and fundamental rights [28], [29].

The normative-juridical approach is used to analyze the legal obligations of the state as a personal data controller in digital government services. This approach examines statutory provisions, legal principles, and regulatory structures that govern personal data processing by public institutions. The study focuses on the integration of Law No. 27 of 2022 concerning Personal Data Protection, Presidential Regulation No. 95 of 2018 concerning the Electronic-Based Government System, Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, Law No. 30 of 2014 concerning Government Administration, and Law No. 25 of 2009 concerning Public Services. Law No. 27 of 2022 regulates principles of personal data protection, data-subject rights, personal data processing, obligations of personal data controllers and processors, data transfer, administrative sanctions, dispute settlement, and criminal provisions. Presidential Regulation No. 95 of 2018 provides the policy foundation for SPBE, while Government Regulation No. 71 of 2019 regulates electronic systems and transactions. These instruments are examined together to understand whether Indonesia's digital government framework has adequately positioned the state as a rights-based and accountable data controller.

This study is also designed as a single-case study of Indonesia. Indonesia is selected because it has formally developed SPBE as a national digital government framework, but the implementation of personal data protection within government digital services remains normatively and institutionally complex. The case study is limited to the

state's responsibility in processing citizens' personal data through public digital services, including the collection, storage, use, integration, exchange, security, and correction of personal data. The study does not examine private-sector data processing, except where private electronic system providers act as processors or technical partners of government institutions. This case boundary is important because the state's obligation in SPBE is legally different from private-sector data governance. The government does not process personal data merely as a market actor, but as a public authority that is constitutionally responsible for protecting citizens' rights.

The conceptual approach is used to construct the idea of the state as a constitutional data controller. This concept refers to the position of the state as a public authority that controls the purposes and means of personal data processing in digital government services, while also bearing constitutional responsibility to protect privacy, legal identity, access to public services, administrative fairness, and human dignity. The concept is necessary because the Personal Data Protection Law regulates the obligations of personal data controllers in general, but the state's responsibility in SPBE must be interpreted more broadly. As a public authority, the state is not only required to comply with data-processing rules, but also to ensure that personal data governance supports legality, transparency, proportionality, accountability, and constitutional rights protection.

The data used in this study consist of primary legal materials, secondary legal materials, and supporting policy documents. Primary legal materials include the 1945 Constitution of the Republic of Indonesia, Law No. 27 of 2022 concerning Personal Data Protection, Law No. 25 of 2009 concerning Public Services, Law No. 30 of 2014 concerning Government Administration, Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, and Presidential Regulation No. 95 of 2018 concerning the Electronic-Based Government System. Secondary legal materials include peer-reviewed journal articles on personal data protection, digital government, SPBE, data governance, privacy rights, administrative law, and AI or automated decision-making in public administration. Supporting policy documents include official regulatory databases, government policy materials, and institutional documents related to SPBE and public-sector data governance.

Data were collected through library research and documentary study. Library research was conducted by tracing scholarly literature from reputable journals, prioritizing recent articles with active DOI links and direct relevance to personal data protection, digital government, public administration, and state accountability. Documentary study was conducted by examining statutory regulations, policy documents, and official legal materials. Documentary analysis is relevant because legal and policy documents are the main sources for identifying the state's obligations, the scope of citizens' rights, and the regulatory relationship between the Personal Data Protection Law and SPBE governance [29]. This technique allows the research to systematically identify legal norms and institutional responsibilities embedded in Indonesian digital government regulation.

The collected data were analyzed using qualitative content analysis and legal interpretation. Qualitative content analysis was used to classify the materials into several analytical themes: the state as personal data controller, citizens as data subjects, lawful basis of data processing, purpose limitation, data minimization, consent and public interest, data security, inter-agency data sharing, data accuracy, breach notification, administrative responsibility, and constitutional rights protection. Legal interpretation was then applied to examine how these themes should be understood within Indonesia's administrative and constitutional law framework. Statutory interpretation was used to analyze the meaning of relevant legal provisions, conceptual interpretation was used to clarify the legal meaning of state responsibility as data controller, and systematic interpretation was used to connect the Personal Data Protection Law with SPBE governance, public service obligations, and government administration principles.

The analytical process was conducted in four stages. First, the study identified the legal norms governing personal data protection in Indonesia, especially the rights of data subjects and obligations of data controllers under Law No. 27 of 2022. Second, it examined the SPBE framework to understand how digital government encourages integration, interoperability, and data exchange among public institutions. Third, the study analyzed the legal risks that arise when government institutions process personal data through integrated digital systems, including excessive data processing, unclear institutional responsibility, inaccurate data use, weak consent mechanisms, unauthorized access, data breaches, and insufficient remedies. Fourth, the study formulated a normative framework for integrating personal data protection, SPBE governance, and constitutional rights.

To strengthen the credibility of the analysis, this study applies source triangulation by comparing statutory regulations, scholarly literature, and official policy documents. The study also applies a rights-based perspective, meaning that SPBE is not assessed solely as an administrative-efficiency instrument, but as a digital governance system that must respect and protect citizens' constitutional rights. Therefore, the legality of personal data processing by the state is assessed through several standards: clear legal basis, legitimate public purpose, proportionality, transparency, data accuracy, security, accountability, access to correction, and effective remedies.

The limitation of this method is that it does not empirically assess the technical security performance of specific government platforms or measure public perception of data protection in SPBE services. It also does not conduct interviews with government officials, system developers, data protection officers, or citizens. The study is limited to normative legal reconstruction based on legal materials, policy documents, and scholarly literature. Nevertheless, this method is appropriate for the purpose of the article because the study aims to formulate a legal framework for state

responsibility in personal data protection within SPBE, rather than to conduct a technical audit of a particular digital government system.

3. RESULTS AND DISCUSSION

3.1. The State as a Constitutional Data Controller in Electronic-Based Government Systems

The findings of this study show that the Indonesian state, when operating digital public services through the Electronic-Based Government System, cannot be understood merely as an ordinary data-processing institution. In the context of SPBE, the state collects, stores, integrates, exchanges, verifies, and uses citizens' personal data for the purpose of delivering public services and exercising governmental authority. This position makes the state a **personal data controller** because public institutions determine the purpose and means of personal data processing in digital government services. However, unlike private data controllers, the state exercises this role based on public authority and constitutional responsibility. Therefore, the state should be understood as a **constitutional data controller**, namely a public authority that controls personal data processing while being legally bound to protect citizens' constitutional rights.

This finding is important because personal data processing in government services is often mandatory in practice. Citizens usually cannot refuse to provide personal data when accessing population administration, health services, education services, taxation, licensing, social assistance, immigration, or other public services. This creates an unequal relationship between citizens and the state. In the private sector, personal data processing is often based on consent or contractual relations, although such consent may also be problematic. In government services, however, citizens' personal data is often processed because of statutory obligation, public interest, or the exercise of public authority. Therefore, the state has a higher duty to ensure that data processing is lawful, limited, transparent, secure, accurate, and accountable.

Law No. 27 of 2022 concerning Personal Data Protection provides the legal basis for data-subject rights, the obligations of personal data controllers and processors, lawful data processing, data transfer, administrative sanctions, dispute settlement, and criminal provisions. Nevertheless, the implementation of this law in SPBE requires a specific administrative-law interpretation. In digital government, personal data protection is not only about preventing data leakage, but also about ensuring that citizens' data is processed fairly and proportionately by public institutions. This finding strengthens Rahman's argument that personal data protection in SPBE must be supported by clear legal principles, data classification, access restrictions, and information-security standards [1]. It also confirms Syailendra, Lie, and Sudiro's view that the Personal Data Protection Law is a significant legal development, but its implementation requires stronger institutional readiness and enforcement mechanisms [2].

The study further finds that the state's responsibility as a data controller must be connected to the principles of government administration and public service. Law No. 30 of 2014 concerning Government Administration requires governmental actions and decisions to be based on legality, authority, good governance, and accountability. Law No. 25 of 2009 concerning Public Services requires public institutions to provide services in accordance with citizens' rights, service standards, complaint mechanisms, and institutional responsibility. Therefore, when public services are delivered through SPBE, personal data protection should not be treated separately from public service accountability. A government institution that processes personal data unlawfully, excessively, or insecurely does not only violate data protection principles; it may also violate the principles of good governance and public service responsibility.

3.2. Regulatory Fragmentation between the Personal Data Protection Law and SPBE Governance

The second finding of this study is that Indonesia already has important legal instruments for digital government and personal data protection, but these instruments remain fragmented when applied to the daily operation of SPBE. Presidential Regulation No. 95 of 2018 concerning SPBE emphasizes integration, interoperability, efficiency, public service improvement, and digital transformation of government administration. Meanwhile, Law No. 27 of 2022 concerning Personal Data Protection emphasizes the rights of data subjects, obligations of controllers and processors, personal data processing principles, data security, dispute settlement, and sanctions. Both instruments are relevant, but they do not yet form a fully integrated framework for rights-based data governance in digital government.

This fragmentation creates several legal risks. First, the expansion of inter-agency data sharing may produce uncertainty over which public institution acts as the main controller, joint controller, or processor. Second, data integration may increase the possibility of excessive processing when data collected for one public service purpose is reused for another purpose without adequate legal limitation. Third, citizens may face difficulty in identifying which institution is responsible when their data is inaccurate, misused, leaked, or used to deny access to public services. Fourth, SPBE may prioritize interoperability and administrative efficiency without sufficient procedural safeguards for citizens as data subjects.

This finding is consistent with Schmeling, al Dakruni, and Mergel, who argue that data collaboration in digital government involves ecosystem, organizational, and individual dimensions, but issues of privacy, security, standardization, and trust remain underdeveloped in public-sector data collaboration research [6]. It also aligns with

Yukhno's argument that big-data governance requires public administration to rethink its principles because digital government increasingly depends on large-scale data ecosystems [7]. In the Indonesian context, this means that SPBE governance must move beyond technical integration and toward accountable data governance.

The fragmentation between the Personal Data Protection Law and SPBE governance also affects the protection of constitutional rights. Personal data is closely related to privacy, human dignity, legal identity, equality before the law, and access to public services. When government data systems are inaccurate or insecure, citizens may suffer concrete harm, such as exclusion from social assistance, difficulty accessing public services, identity misuse, administrative discrimination, or exposure of sensitive personal information. Rahmawati and Wardana emphasize that privacy and personal data protection are linked to constitutional guarantees in the era of government digitalization [5]. This study extends that argument by showing that constitutional protection must be embedded directly into SPBE governance, not treated only as a general constitutional principle.

The comparison with prior research indicates that Indonesia's regulatory challenge is not merely the absence of a Personal Data Protection Law, because such a law already exists. The deeper issue is the need to operationalize the law within the institutional structure of digital government. Badriah, Indiahono, and Sukarso show that accountability in personal data protection requires institutional clarity, breach-reporting mechanisms, and learning from comparative governance models such as South Korea and Singapore [3]. This study confirms that point but adds that, in Indonesia, accountability must be developed specifically within the SPBE architecture because government data processing involves public authority, public service obligations, and constitutional rights.

3.3. State Obligations in Protecting Citizens' Personal Data in Digital Government Services

The third finding of this study is that the state's responsibility in protecting personal data within SPBE should be formulated through several core obligations. The first obligation is lawfulness and purpose limitation. Every act of personal data processing by public institutions must have a clear legal basis and legitimate public purpose. Government institutions should not collect or process personal data merely because technology allows it. Data processing must be necessary for a specific public service or governmental function, and the purpose must be clearly communicated to citizens.

The second obligation is data minimization and proportionality. Public institutions should only collect and process data that is necessary for the stated purpose. Excessive collection of personal data creates risks of misuse, unauthorized access, profiling, and institutional overreach. In SPBE, where data integration is a central objective, proportionality becomes essential because integrated systems may encourage the accumulation of large amounts of personal data across institutions. This finding is consistent with broader studies on digital government and surveillance, which warn that public-sector data use may be justified by public interest or national security, but such justification must still be balanced against individual rights [8].

The third obligation is transparency and citizen notification. Citizens must be informed about how their personal data is collected, used, shared, stored, protected, and deleted. Transparency is not only a technical privacy notice; it is a democratic requirement in digital public administration. Without transparency, citizens cannot exercise their rights as data subjects, including the right to access, correct, or challenge the use of their personal data. In this respect, SPBE platforms should provide clear information about data-processing purposes, responsible institutions, data-sharing mechanisms, retention periods, and complaint channels.

The fourth obligation is data accuracy and correction. Personal data used in digital public services must be accurate, updated, and relevant. This obligation is particularly important because inaccurate government data may directly affect citizens' access to public services. For example, inaccurate population data, welfare data, tax data, or education data may result in exclusion from benefits or administrative obstacles. Therefore, SPBE must provide accessible mechanisms for citizens to correct inaccurate data and ensure that corrected data is reflected across relevant government systems.

The fifth obligation is security and breach accountability. Public institutions must implement appropriate technical and organizational measures to prevent unauthorized access, data leakage, unlawful disclosure, manipulation, and cyberattacks. However, security should not be understood narrowly as an IT function. It is also a legal responsibility. When a breach occurs, government institutions must be able to identify the responsible actor, notify affected citizens, mitigate harm, investigate the cause, and impose institutional accountability. This supports Wibowo's argument that personal data protection is increasingly important for Indonesia's digital development because trust in digital systems depends on the protection of citizens' personal information [4].

The sixth obligation is effective remedies. Citizens must have accessible complaint, correction, objection, and dispute-settlement mechanisms when their personal data is misused, leaked, processed unlawfully, or used to produce harmful administrative consequences. Without remedies, personal data protection becomes declaratory rather than enforceable. In the SPBE context, remedies should be integrated into public service complaint mechanisms, administrative review, data protection supervision, and judicial remedies. This is essential because digital government may produce harm that is difficult for citizens to trace without institutional assistance.

3.4. Integrating Personal Data Protection, SPBE Governance, and Constitutional Rights

The central contribution of this study is the formulation of an integrated framework for state responsibility in personal data protection within SPBE. This framework is based on the argument that the state must be treated as a constitutional data controller. This concept combines three legal dimensions. First, the state is a data controller under the Personal Data Protection Law because it determines the purpose and means of data processing. Second, the state is an SPBE organizer because it designs, operates, integrates, and manages digital public services. Third, the state is a constitutional duty bearer because it is responsible for protecting citizens' fundamental rights.

This integrated framework requires that SPBE governance be evaluated through both administrative efficiency and rights protection. Digital government cannot be considered successful merely because it accelerates services, integrates databases, or reduces bureaucratic procedures. It must also ensure that citizens' personal data is processed lawfully, transparently, securely, proportionately, and accountably. In other words, the legitimacy of SPBE depends not only on technological performance, but also on its ability to protect constitutional rights.

This finding has implications for previous studies on AI and digital government. Research on AI adoption in public administration shows that digital technologies can improve public-sector capacity but may also create risks related to fairness, transparency, privacy, and institutional accountability [9]–[15]. Busuioc argues that accountable AI requires identifiable responsibility and mechanisms for holding institutions to account [16]. Bignami emphasizes the importance of public administration accountability in AI governance [17]. Williams argues that algorithmic decision-making challenges administrative law doctrines such as legality, discretion, reason-giving, and reviewability [18]. Although these studies focus largely on AI and automated decision-making, their arguments are also relevant to SPBE because AI and automation depend heavily on personal data. Without strong data governance, AI-based or automated government systems may reproduce inaccurate, biased, or unlawful data practices.

The integrated framework proposed in this study consists of seven principles. First, legal basis, meaning every personal data processing activity in SPBE must be grounded in law. Second, public purpose, meaning data processing must be connected to a legitimate governmental function or public service. Third, proportionality, meaning the scope of data processing must be limited to what is necessary. Fourth, transparency, meaning citizens must be informed about data use and institutional responsibility. Fifth, security, meaning the state must protect personal data through technical and organizational safeguards. Sixth, accountability, meaning public institutions must be responsible for unlawful processing, data leakage, inaccurate data use, and failure to provide remedies. Seventh, constitutional protection, meaning SPBE must be designed and implemented in a way that respects privacy, human dignity, equality, legal certainty, and access to public services.

The novelty of this study lies in its effort to integrate the Personal Data Protection Law with SPBE governance and constitutional rights protection. Previous studies have generally discussed these issues separately: data protection as a privacy issue, SPBE as a digital government reform agenda, and constitutional rights as a broad normative guarantee. This study argues that these three dimensions must be treated as one interconnected framework. The state's responsibility in SPBE is not fulfilled merely by adopting digital platforms or complying formally with data protection provisions. It must ensure that every stage of personal data processing in digital government services is legally justified, institutionally accountable, and constitutionally oriented.

Overall, the findings show that Indonesia's digital government transformation requires a shift from platform-based SPBE to rights-based SPBE. Platform-based SPBE emphasizes digital integration, interoperability, and service efficiency. Rights-based SPBE goes further by ensuring that citizens remain protected as legal subjects and data subjects within government digital systems. This shift is essential because public trust in digital government depends not only on service speed, but also on the assurance that the state will not misuse, neglect, or expose citizens' personal data. Therefore, the protection of personal data in SPBE should be understood as a core element of constitutional governance in the digital age.

4. CONCLUSION

This study concludes that the protection of personal data in Indonesia's Electronic-Based Government System cannot be understood merely as a technical matter of cybersecurity or administrative data management. It is a constitutional responsibility of the state. When government institutions collect, store, integrate, exchange, and process citizens' personal data through digital public services, the state acts not only as a service provider but also as a public authority that determines the purpose and means of personal data processing. Therefore, the state must be positioned as a **constitutional data controller** whose obligations extend beyond formal compliance with data protection rules toward the protection of privacy, human dignity, legal certainty, equality, and access to public services.

The main finding of this study shows that Indonesia already has an important legal foundation for personal data protection and digital government, particularly through Law No. 27 of 2022 concerning Personal Data Protection and Presidential Regulation No. 95 of 2018 concerning the Electronic-Based Government System. However, these two regulatory frameworks have not yet been fully integrated. The Personal Data Protection Law regulates the rights of data subjects and the obligations of personal data controllers and processors, while the SPBE framework

emphasizes digital integration, interoperability, efficiency, and public service transformation. The problem is that SPBE governance may encourage extensive data sharing and inter-agency integration without a sufficiently detailed framework for determining institutional responsibility, data-processing limits, citizen notification, correction mechanisms, breach accountability, and effective remedies.

The novelty of this study lies in its effort to integrate three dimensions that are often discussed separately: personal data protection, SPBE governance, and constitutional rights. This study argues that the state's responsibility in digital government must be reconstructed through a rights-based SPBE framework. Such a framework requires every public institution to ensure that personal data processing is based on clear legal authority, legitimate public purpose, proportionality, transparency, security, accountability, and constitutional protection. In this sense, the success of SPBE should not be measured only by service speed, platform integration, or administrative efficiency, but also by the extent to which citizens' personal data is protected from misuse, excessive processing, unauthorized access, inaccurate use, and institutional neglect.

This study contributes to previous research on data protection and digital government by emphasizing that the state has a higher level of responsibility than private data controllers. Citizens often cannot freely refuse data processing in public services because personal data submission is required to obtain identity documents, social assistance, licensing, education, health services, taxation services, immigration services, and other administrative benefits. This unequal relationship requires stronger safeguards. Therefore, the government must provide clear mechanisms for notification, data access, correction, complaint submission, breach notification, institutional review, and legal remedies. Without these mechanisms, personal data protection in SPBE risks becoming a formal legal promise rather than an enforceable right.

The findings also imply that Indonesia needs a more operational regulatory framework for personal data protection in the public sector. Such a framework should clarify the status of government institutions as data controllers, joint controllers, or processors in inter-agency data sharing. It should also regulate standards for data minimization, purpose limitation, consent or lawful basis in public services, retention periods, data security, accountability logs, breach response, and remedies for citizens. In addition, each government institution operating digital public services should develop internal data governance standards, appoint responsible officials, conduct data protection impact assessments, and ensure that SPBE platforms are designed according to privacy-by-design and rights-by-design principles.

This study has several limitations. It is based on qualitative legal research and documentary analysis, so it does not empirically examine the technical security of specific government platforms or the actual implementation of data protection practices within public institutions. It also does not involve interviews with citizens, government officials, data protection officers, system developers, or oversight institutions. Therefore, the conclusions of this study are primarily normative and conceptual, aimed at formulating a legal framework for state responsibility in personal data protection within SPBE.

Future research should examine the implementation of personal data protection in specific Indonesian digital government services, such as population administration, social assistance, online licensing, taxation, health services, education platforms, immigration, and digital identity systems. Empirical studies are also needed to assess citizens' awareness of their data rights, the readiness of government institutions to comply with the Personal Data Protection Law, and the effectiveness of complaint and remedy mechanisms. Comparative studies with countries that have stronger public-sector data governance frameworks, such as the European Union member states, Singapore, South Korea, Australia, or Canada, may also provide valuable lessons for strengthening Indonesia's SPBE governance.

Overall, this study affirms that digital government must be built not only on efficiency and interoperability, but also on constitutional responsibility. SPBE will gain public legitimacy only when citizens can trust that their personal data is processed lawfully, transparently, securely, proportionately, and accountably. Therefore, Indonesia's digital government transformation should move from a platform-based model toward a rights-based model of SPBE, where personal data protection becomes a core element of democratic, accountable, and constitutionally oriented public administration.

5. REFERENCES

[1] F. Rahman, "Kerangka hukum perlindungan data pribadi dalam penerapan Sistem Pemerintahan Berbasis Elektronik di Indonesia," *Jurnal Legislasi Indonesia*, vol. 18, no. 1, pp. 81–102, 2021. https://doi.org/10.54629/jli.v18i1.736

[2] M. R. Syailendra, G. Lie, and A. Sudiro, "Personal data protection law in Indonesia: Challenges and opportunities," *Indonesia Law Review*, vol. 14, no. 2, article 4, 2024. https://doi.org/10.15742/ilrev.v14n2.4

[3] L. Badriah, D. Indiahono, and Sukarso, "Accountability in personal data protection policy in Indonesia: Learning from South Korea and Singapore," *Matra Pembaruan: Jurnal Inovasi Kebijakan*, vol. 8, no. 2, pp. 89–102, 2024. https://doi.org/10.21787/mp.8.2.2024.89-102

[4] A. Wibowo, "The importance of personal data protection in Indonesia's economic development," *Cogent Social Sciences*, vol. 10, no. 1, 2024. https://doi.org/10.1080/23311886.2024.2306751

[5] A. D. Rahmawati and D. J. Wardana, "Constitutional guarantees of the right to privacy of personal data of citizens in the era of government digitalization," *Journal of Law, Politic and Humanities*, vol. 6, no. 2, pp. 1052–1063, 2025. https://doi.org/10.38035/jlph.v6i2.2664
[6] J. Schmeling, S. al Dakruni, and I. Mergel, "Data collaboration in digital government research: A literature review and research agenda," *Government Information Quarterly*, vol. 42, no. 3, article 102063, 2025. https://doi.org/10.1016/j.giq.2025.102063
[7] A. Yukhno, "Digital transformation: Exploring big data governance in public administration," *Public Organization Review*, vol. 24, no. 1, pp. 335–349, 2024. https://doi.org/10.1007/s11115-022-00694-x
[8] S. Degli Esposti, K. Ball, and S. Dibb, "What's in it for us? Benevolence, national security, and digital surveillance," *Public Administration Review*, vol. 81, no. 5, pp. 862–873, 2021. https://doi.org/10.1111/puar.13362
[9] B. W. Wirtz, P. F. Langer, and C. Fenner, "Artificial intelligence in the public sector: A research agenda," *International Journal of Public Administration*, vol. 44, no. 13, pp. 1103–1128, 2021. https://doi.org/10.1080/01900692.2021.1947319
[10] A. Zuiderwijk, Y.-C. Chen, and F. Salem, "Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda," *Government Information Quarterly*, vol. 38, no. 3, article 101577, 2021. https://doi.org/10.1016/j.giq.2021.101577
[11] R. Madan and M. Ashok, "AI adoption and diffusion in public administration: A systematic literature review and future research agenda," *Government Information Quarterly*, vol. 40, no. 1, article 101774, 2023. https://doi.org/10.1016/j.giq.2022.101774
[12] I. Mergel, H. Dickinson, J. Stenvall, and M. Gascó, "Implementing AI in the public sector," *Public Management Review*, 2023. https://doi.org/10.1080/14719037.2023.2231950
[13] C. van Noordt and L. Tangi, "The dynamics of AI capability and its influence on public value creation of AI within public administration," *Government Information Quarterly*, vol. 40, no. 4, article 101860, 2023. https://doi.org/10.1016/j.giq.2023.101860
[14] G. Maragno, L. Tangi, L. Gastaldi, and M. Benedetti, "Exploring the factors, affordances and constraints outlining the implementation of artificial intelligence in public sector organizations," *International Journal of Information Management*, vol. 73, article 102686, 2023. https://doi.org/10.1016/j.ijinfomgt.2023.102686
[15] R. Medaglia, J. R. Gil-Garcia, and T. A. Pardo, "Artificial intelligence in government: Taking stock and moving forward," *Social Science Computer Review*, vol. 41, no. 1, pp. 123–140, 2023. https://doi.org/10.1177/08944393211034087
[16] M. Busuioc, "Accountable artificial intelligence: Holding algorithms to account," *Public Administration Review*, vol. 81, no. 5, pp. 825–836, 2021. https://doi.org/10.1111/puar.13293
[17] F. Bignami, "Artificial intelligence accountability of public administration," *The American Journal of Comparative Law*, vol. 70, Supplement_1, pp. i312–i346, 2022. https://doi.org/10.1093/ajcl/avac012
[18] R. Williams, "Rethinking administrative law for algorithmic decision making," *Oxford Journal of Legal Studies*, vol. 42, no. 2, pp. 468–494, 2022. https://doi.org/10.1093/ojls/gqab032
[19] M. Suksi, "Administrative due process when using automated decision-making in public administration: Some notes from a Finnish perspective," *Artificial Intelligence and Law*, vol. 29, no. 1, pp. 87–110, 2021. https://doi.org/10.1007/s10506-020-09269-x
[20] N. Aoki, "The importance of the assurance that 'humans are still in the decision loop' for public trust in artificial intelligence: Evidence from an online experiment," *Computers in Human Behavior*, vol. 114, article 106572, 2021. https://doi.org/10.1016/j.chb.2020.106572
[21] N. Aoki, T. Tatsumi, G. Naruse, and K. Maeda, "Explainable AI for government: Does the type of explanation matter to the accuracy, fairness, and trustworthiness of an algorithmic decision as perceived by those who are affected?" *Government Information Quarterly*, vol. 41, no. 4, article 101965, 2024. https://doi.org/10.1016/j.giq.2024.101965
[22] S. Grimmelikhuijsen, "Explaining why the computer says no: Algorithmic transparency affects the perceived trustworthiness of automated decision-making," *Public Administration Review*, vol. 83, no. 2, pp. 241–262, 2023. https://doi.org/10.1111/puar.13483
[23] D. S. Schiff, K. J. Schiff, and P. Pierson, "Assessing public value failure in government adoption of artificial intelligence," *Public Administration*, vol. 100, no. 3, pp. 653–673, 2022. https://doi.org/10.1111/padm.12742
[24] O. Agbabiaka, A. Ojo, and N. Connolly, "Requirements for trustworthy AI-enabled automated decision-making in the public sector: A systematic review," *Technological Forecasting and Social Change*, vol. 215, article 124076, 2025. https://doi.org/10.1016/j.techfore.2025.124076
[25] A. Rizk and I. Lindgren, "Automated decision-making in public administration: Changing the decision space between public officials and citizens," *Government Information Quarterly*, vol. 42, no. 4, article 102061, 2025. https://doi.org/10.1016/j.giq.2025.102061

[26] A. Kouroutakis, "Rule of law in the AI era: Addressing accountability and the governance of artificial intelligence," *Discover Artificial Intelligence*, vol. 4, article 91, 2024. https://doi.org/10.1007/s44163-024-00191-8
[27] J. Mišić, R. van Est, and L. Kool, "Good governance of public sector AI: A combined value framework for good order and a good society," *AI and Ethics*, vol. 5, pp. 4875–4889, 2025. https://doi.org/10.1007/s43681-025-00751-3
[28] M. Mitchell, "Analyzing the law qualitatively," *Qualitative Research Journal*, vol. 23, no. 1, pp. 102–113, 2022. https://doi.org/10.1108/QRJ-04-2022-0061
[29] H. Morgan, "Conducting a qualitative document analysis," *The Qualitative Report*, vol. 27, no. 1, pp. 64–77, 2022. https://doi.org/10.46743/2160-3715/2022.5044
[30] W. M. Lim, "What is qualitative research? An overview and guidelines," *Australasian Marketing Journal*, vol. 33, no. 5, pp. 199–229, 2025. https://doi.org/10.1177/14413582241264619
[31] A. Blackham, "When law and data collide: The methodological challenge of conducting mixed methods research in law," *Journal of Law and Society*, vol. 49, no. S1, pp. S87–S104, 2022. https://doi.org/10.1111/jols.12373

Legal Materials

Republic of Indonesia, Law No. 27 of 2022 concerning Personal Data Protection.
Republic of Indonesia, Law No. 25 of 2009 concerning Public Services.
Republic of Indonesia, Law No. 30 of 2014 concerning Government Administration.
Republic of Indonesia, Presidential Regulation No. 95 of 2018 concerning the Electronic-Based Government System.
Republic of Indonesia, Law No. 27 of 2022 concerning Personal Data Protection.
Republic of Indonesia, Law No. 25 of 2009 concerning Public Services.
Republic of Indonesia, Law No. 30 of 2014 concerning Government Administration.
Republic of Indonesia, Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions.
Republic of Indonesia, Presidential Regulation No. 95 of 2018 concerning the Electronic-Based Government System.