Jurnal Kecerdasan Buatan dan Teknologi Informasi
Vol. 4, No. 3, September 2025, pp. 303-311
e-ISSN: 2964-2922, p-ISSN: 2963-6191
DOI : https://doi.org/10.69916/jkbti.v4i3.462

CYBERSECURITY GOVERNANCE IN ELECTRONIC-BASED GOVERNMENT SYSTEMS: AN ANALYSIS OF THE GOVERNMENT'S LEGAL RESPONSIBILITY FOR PUBLIC DATA BREACHES

Erfan Wahyudi[1*], [2]Muhammad Suhardi[2]

[1,2]Institut Pemerintahan Dalam Negeri, Indonesia
Email: [1]erfan.wahyudie@gmail.com, [2]muhammad@ipdn.ac.id

(Received: July 29, 2025; Revised: September 12, 2025; Accepted: September 20, 2025)

Abstract

The increasing digitalisation of public administration has made cybersecurity governance a central issue in electronic-based government systems. Public data breaches in government digital platforms are no longer merely technical incidents, but also raise questions of administrative responsibility, public service continuity, and citizens' legal protection. This study examines the government's legal responsibility for public data breaches within the framework of cybersecurity governance and electronic-based government systems. Using a normative juridical method with statutory, conceptual, and analytical approaches, this article analyses cybersecurity as part of the state's duty to provide secure, reliable, and accountable digital public services. The findings show that government responsibility can be constructed through three layers: preventive responsibility, responsive responsibility, and restorative responsibility. Preventive responsibility requires risk-based cybersecurity standards, institutional coordination, security audits, and adequate backup systems. Responsive responsibility requires rapid incident detection, containment, reporting, and transparent public communication. Restorative responsibility requires service recovery, breach notification, institutional evaluation, and remedies for affected citizens. The novelty of this study lies in integrating cybersecurity governance, electronic-based government systems, and administrative-law responsibility into a single analytical framework. The study argues that public data protection is not only a technical obligation, but also a legal manifestation of due care, accountability, good administration, and public service responsibility. Therefore, cybersecurity governance must be positioned as an essential requirement for lawful, secure, and citizen-centred digital government.

Keywords: administrative responsibility; cybersecurity governance; electronic-based government system; public data breach; public data protection.

1. INTRODUCTION

The acceleration of digital government has transformed public administration into a data-intensive and technology-dependent system. Public services that were previously delivered through conventional bureaucratic procedures are now increasingly mediated by integrated platforms, digital identity systems, cloud infrastructure, electronic archives, and inter-agency data exchange mechanisms. This transformation has improved administrative efficiency, service accessibility, and policy coordination, but it has also expanded the state's exposure to cybersecurity risks. In an electronic-based government system, public data are no longer merely administrative records; they have become strategic assets that support decision-making, service delivery, population administration, health services, taxation, licensing, social assistance, immigration, and other public functions. Consequently, the failure to protect public data may directly affect citizens' rights, public trust, institutional legitimacy, and the continuity of government services [1], [2], [17].

Cybersecurity is therefore not only a technical issue but also a governance and legal responsibility issue. In the public sector, cyber incidents such as ransomware attacks, unauthorised access, data exfiltration, and service disruption may cause broader consequences than similar incidents in private organisations. A breach in government systems may expose sensitive citizen data, paralyse essential public services, weaken national digital infrastructure, and raise questions regarding the adequacy of institutional safeguards. Recent studies on government data breaches show that public-sector cyber incidents are increasingly connected to ransomware, weak security architecture, poor backup mechanisms, fragmented institutional coordination, and inadequate incident response capacity [2], [3], [6]. This demonstrates that cybersecurity governance must be understood as part of the state's duty to ensure reliable, secure, and accountable public administration.

In the Indonesian context, the issue is especially relevant because the Sistem Pemerintahan Berbasis Elektronik, or SPBE, is designed to integrate government administration and public services through digital systems. However, the increasing integration of government data also creates systemic risks. When government agencies centralise data,

connect services, and rely on shared infrastructure, a single vulnerability may produce cascading impacts across multiple institutions. The 2024 disruption of the Temporary National Data Centre illustrates that cybersecurity failure may no longer be treated as an isolated technical malfunction; it may become an administrative crisis involving public service continuity, institutional responsibility, data protection obligations, and citizens' legal rights. Therefore, the legal question is not only how a breach occurred, but also who must be held administratively responsible, what duties were neglected, and what remedies should be available to affected citizens.

Previous studies have examined cybersecurity in digital government from various perspectives. Ribeiro et al. assess the information security posture of online public service platforms worldwide and show that secure communication protocols, trustworthy certificates, and vulnerability exposure are central indicators of public service security [1]. Hamid and Huda map the scientific landscape of government data breaches and identify ransomware, cybercrime, and national security as dominant themes in recent literature [2]. Mushtaq and Shah demonstrate that cybercrime mitigation in e-government requires stronger internal processes, organisational preparedness, and security governance [3]. Hossain et al. identify financial limitations, technological vulnerabilities, human factors, and regulatory gaps as key challenges in local government cybersecurity [4], while Magnusson et al. emphasise that information security governance in the public sector requires risk management, accountability frameworks, and institutional alignment [5]. Figueroa et al. further propose a holistic cybersecurity framework for e-government that integrates regulatory compliance, risk management, secure data exchange, and citizen-oriented protection [6]. Nguyen-Duc et al. show that software security assessment in e-government projects requires not only technical tools but also human-driven security review [7]. These studies collectively indicate that cybersecurity governance must be embedded in public-sector management, not treated as a separate technological layer.

Other related works focus on digital governance, public-sector capability, and legal accountability. Ahn and Chen examine AI-augmented public administration and highlight the importance of public employees' perceptions and institutional readiness in adopting digital technologies [15]. Van Noordt and Misuraca show that AI and digital systems in government raise governance, ethical, and organisational challenges across public institutions [16]. Ruijer analyses data collaboratives from a governance perspective, demonstrating the importance of coordination, institutional design, and accountability in data-sharing arrangements [17]. Gasco-Hernandez et al. explain that inter-agency collaboration requires technology, leadership, governance, and collaborative capacity [18], while Wouters et al. argue that integrated digital public service delivery depends on inter-organisational cooperation and shared governance mechanisms [19]. At the legal level, Prictor discusses the growing importance of data breach notification laws in the Asia-Pacific region [12], Ba'abud and Heriyanto analyse extraterritorial jurisdiction in cross-border personal data breaches [13], and Poli and Sommario examine the complexities of state responsibility in cyberattacks [14]. These studies provide important foundations, but they do not specifically integrate cybersecurity governance, SPBE, and administrative-law responsibility in the context of public data breaches.

Based on this gap, this article positions cybersecurity governance as a legal requirement within electronic-based government systems. The novelty of this study lies in combining three dimensions that are often discussed separately: cybersecurity governance, SPBE-based digital administration, and the legal responsibility of government under administrative law. Unlike studies that focus primarily on technical security frameworks, cybercrime mitigation, or general data protection compliance, this article argues that public data breaches must be analysed as failures of administrative responsibility when they result from weak governance, inadequate risk management, poor institutional coordination, or negligence in fulfilling public duties. The study aims to examine how government responsibility should be constructed when public data breaches occur in digital public service systems, to identify the administrative-law principles that justify such responsibility, and to propose a normative framework for accountable cybersecurity governance in SPBE.

2. RESEARCH METHODS

This study employs a normative juridical research method with a doctrinal and conceptual orientation. This method is appropriate because the central issue examined in this article concerns the legal construction of government responsibility when public data breaches occur in electronic-based government systems. The study does not seek to measure the technical performance of cybersecurity infrastructure or conduct forensic analysis of specific cyber incidents. Instead, it analyses cybersecurity governance as a legal obligation of public authorities within the framework of electronic government, administrative law, public service accountability, and personal data protection. Through this method, the research examines how the state's duty to protect public data should be understood when digital public service systems fail to prevent, respond to, or recover from cybersecurity incidents.

This research applies three main approaches: the statutory approach, the conceptual approach, and the analytical approach**.** The statutory approach is used to examine legal norms related to electronic-based government systems, cybersecurity, public services, administrative responsibility, and personal data protection. This approach is important because public data breaches in government systems cannot be analysed only as technological failures; they must also be assessed in relation to the legal duties imposed on public institutions as data controllers, service providers, and administrative authorities. The conceptual approach is used to clarify key concepts such as cybersecurity governance,

public data breach, electronic-based government system, state responsibility, administrative negligence, risk management, and public-sector accountability. Meanwhile, the analytical approach is applied to examine the relationship between cybersecurity failure and administrative-law responsibility, particularly when a breach results from weak institutional coordination, inadequate security standards, poor risk mitigation, or failure to provide effective remedies for affected citizens.

The legal materials used in this study consist of primary, secondary, and tertiary legal materials. Primary legal materials include laws and regulations governing electronic government, public administration, public services, cybersecurity, information governance, and personal data protection. These materials are used to identify the normative basis of government obligations in securing digital public service systems and protecting public data. Secondary legal materials include peer-reviewed journal articles, academic books, research reports, and scholarly commentaries discussing cybersecurity governance, e-government, data breaches, administrative responsibility, and state accountability in the digital era. The study prioritises recent academic literature published within the last five years to ensure that the analysis reflects current developments in cybersecurity threats, digital government transformation, and legal accountability [1]–[10], [12]–[14]. Tertiary legal materials, such as legal dictionaries, institutional glossaries, and cybersecurity terminology references, are used to support conceptual clarification.

Data collection is conducted through library research by identifying, selecting, and reviewing legal instruments and academic literature relevant to cybersecurity governance in electronic-based government systems. The selected materials are classified into several thematic categories: first, literature on cybersecurity risks and data breaches in government systems; second, studies on e-government governance and public-sector digital transformation; third, legal scholarship on data protection, breach notification, and state responsibility; and fourth, administrative-law literature concerning legality, accountability, duty of care, public service continuity, and government liability. This classification allows the study to connect technological vulnerability with legal responsibility in a systematic manner.

The analysis is conducted using qualitative legal analysis. First, the study interprets relevant legal norms to identify the government's duties in preventing, managing, and responding to public data breaches. Second, it systematises the relationship between cybersecurity governance and administrative-law principles, particularly the principles of legality, accountability, prudence, proportionality, due care, public service continuity, and good administration. Third, it evaluates whether cybersecurity failure in government systems may be understood as a form of administrative failure when it results from negligence, lack of risk management, institutional fragmentation, or failure to provide adequate protection for public data. This analytical process enables the study to construct public data breaches not merely as cyber incidents, but as potential failures of public administration.

To strengthen the validity of the analysis, this study applies source triangulation by comparing legal norms, doctrinal arguments, and contemporary scholarly findings. This is necessary because cybersecurity governance is an interdisciplinary issue involving law, public administration, information security, digital governance, and institutional management. The study therefore does not rely only on cybersecurity literature, but places such literature within the normative structure of administrative law. By doing so, the research evaluates whether government cybersecurity obligations should be treated as part of administrative accountability, especially when breaches affect citizens' personal data, access to public services, and trust in government institutions.

The scope of this research is limited to the normative construction of government legal responsibility in cases of public data breaches within electronic-based government systems. It does not conduct empirical interviews with government officials, citizens, or cybersecurity practitioners. It also does not perform technical testing of specific digital platforms, penetration testing, or incident forensics. This limitation is intentional because the main objective of the study is to develop a legal and conceptual framework for understanding cybersecurity governance as an administrative-law responsibility. By focusing on the normative dimension, this research contributes to the development of a legal model in which public data protection, cybersecurity preparedness, incident response, and citizen remedies are treated as essential components of accountable digital government.

3. RESULTS AND DISCUSSION

3.1. Cybersecurity Governance as an Administrative-Law Obligation in SPBE

The results of this study indicate that cybersecurity governance in electronic-based government systems must be understood as an administrative-law obligation, not merely as a technical function managed by information technology units. In the context of SPBE, digital infrastructure is used to support public administration, public service delivery, inter-agency coordination, data exchange, and decision-making. Therefore, when government institutions collect, process, store, and distribute public data through digital systems, they assume a legal duty to ensure that such systems are secure, reliable, accountable, and capable of protecting citizens' rights. In Indonesia, SPBE is formally regulated through Presidential Regulation No. 95 of 2018, which frames electronic-based government as a system intended to support integrated, effective, transparent, and accountable governance. This regulatory basis shows that cybersecurity cannot be separated from the broader obligation to organise good digital administration.

The study finds that cybersecurity governance in SPBE consists of at least four interrelated dimensions: preventive governance, institutional governance, procedural governance, and remedial governance. Preventive governance refers to the government's obligation to anticipate cyber risks through risk assessment, security standards, backup systems, access control, encryption, system monitoring, and periodic audits. Institutional governance refers to the distribution of authority and responsibility among ministries, agencies, local governments, data centre operators, and cybersecurity institutions. Procedural governance concerns incident response mechanisms, reporting channels, breach notification, service recovery, and documentation. Remedial governance refers to the availability of administrative, legal, and institutional remedies for citizens whose data or access to public services are affected by a breach.

This finding is consistent with Ribeiro et al., who argue that the security posture of online public services must be assessed through technical indicators such as secure communication protocols, certificates, and exposure to vulnerabilities [1]. However, this study extends that argument by emphasising that technical security indicators are insufficient without administrative accountability. A government website or digital platform may appear technically functional, but it remains legally problematic if the institution lacks clear responsibility, risk governance, audit procedures, and mechanisms to notify or protect affected citizens. In this sense, cybersecurity governance is not only about protecting systems from attack, but also about ensuring that digital public administration remains lawful and trustworthy.

The findings also support Magnusson et al., who show that information security governance in the public sector requires risk management, accountability frameworks, and institutional alignment [5]. Similarly, Figueroa et al. argue that a holistic cybersecurity framework for e-government must combine regulatory compliance, risk management, secure data exchange, and citizen protection [6]. These studies confirm that cybersecurity governance must be embedded in the structure of public administration. Nevertheless, this article differs from previous cybersecurity studies by placing such governance within the doctrinal framework of administrative law. The failure to protect public data is not merely an operational weakness; it may constitute a failure of public duty when it results from negligence, weak supervision, inadequate coordination, or the absence of reasonable preventive measures.

The Indonesian case further demonstrates the urgency of this issue. The ransomware attack on the Temporary National Data Centre, or PDNS 2, in June 2024 affected immigration and other government services, and later reports stated that more than 230 public agencies were affected and that the President ordered an audit of government data centres. This incident illustrates that cybersecurity failure in SPBE can disrupt essential services and expose weaknesses in data governance, backup policy, institutional preparedness, and public accountability. Therefore, public data breaches should not be viewed only as cyber incidents; they should also be analysed as administrative events that trigger questions of legality, responsibility, supervision, and citizen protection.

From an administrative-law perspective, the government has a duty of care to manage public data responsibly. This duty includes the obligation to design secure systems, supervise third-party providers, ensure data backup, prepare incident response mechanisms, and maintain service continuity. If a public data breach occurs because the government fails to adopt reasonable cybersecurity measures, then the breach may indicate administrative negligence. This does not mean that the state is automatically liable for every cyberattack, because not all attacks can be fully prevented. However, the government may be held responsible when the breach is connected to preventable weaknesses, poor governance, inadequate institutional coordination, or failure to respond properly after the incident.

3.2. Public Data Breaches and the Legal Responsibility of Government

The second result of this study is that government responsibility for public data breaches must be analysed through three forms of responsibility: preventive responsibility, responsive responsibility, and restorative responsibility. Preventive responsibility refers to the obligation of public institutions to reduce cybersecurity risks before an incident occurs. Responsive responsibility refers to the obligation to act immediately when a breach occurs, including identifying the incident, containing damage, notifying relevant parties, and restoring public services. Restorative responsibility refers to the obligation to repair the consequences of the breach, including data recovery, institutional evaluation, administrative sanctions where necessary, and remedies for affected citizens.

This three-layer model is important because public data breaches usually do not occur in a legal vacuum. A breach may result from technical attack, but its legal consequences depend on how the government prepared for, responded to, and recovered from the incident. If a government agency has adopted reasonable cybersecurity standards, conducted regular audits, maintained backups, and responded quickly, the legal assessment may differ from a case in which the agency ignored known vulnerabilities or failed to maintain basic safeguards. Therefore, administrative responsibility must be assessed by examining whether public authorities fulfilled their duty of prudence, duty of supervision, duty of risk management, and duty to provide public service continuity.

The findings are consistent with Hossain et al., who identify financial limitations, technological weaknesses, human factors, policy gaps, and organisational challenges as key barriers in local government cybersecurity [4], [8], [9]. This study adds that such barriers are not merely managerial problems; they may become legal problems when they lead to the failure of public institutions to protect public data. Mushtaq and Shah also emphasise that cybercrime

mitigation in e-government requires stronger internal processes and organisational preparedness [3]. In administrative-law terms, organisational preparedness is part of the government's due care obligation. A state institution cannot justify weak cybersecurity merely by arguing that cyber threats are external, because the state itself has chosen to digitise public services and centralise public data.

Government responsibility is also closely related to the position of public institutions as controllers or custodians of citizens' data. In Indonesia, Law No. 27 of 2022 on Personal Data Protection provides the general legal framework for personal data protection. Although the implementation of public-sector data protection still requires institutional development, the law strengthens the principle that data controllers have obligations to process and protect personal data lawfully. The existence of this legal framework indicates that public institutions cannot treat citizen data as ordinary administrative material; they must manage it as protected legal interests. In the SPBE context, this means that cybersecurity governance and personal data protection must be integrated.

The study also finds that public data breaches affect more than privacy. They may disrupt public services, weaken access to administrative rights, create identity fraud risks, and reduce citizens' trust in digital government. Cremer et al. show that cyber risk is difficult to manage because data availability, incident measurement, and risk assessment remain fragmented across sectors [10]. Li et al. further show that data breaches are related not only to technology investment but also to organisational awareness and security management [11]. These findings support the argument that government responsibility cannot be reduced to the procurement of cybersecurity tools. Legal responsibility must also include human capacity, institutional awareness, risk culture, documentation, and continuous evaluation.

The legal responsibility of government must also include breach notification and public communication. Prictor notes that data breach notification laws have gained momentum across the Asia-Pacific region because notification is central to protecting affected individuals [12]. In public administration, notification has a broader function: it enables citizens to take protective measures, strengthens institutional transparency, and prevents the state from concealing administrative failure. If a public institution fails to inform citizens about a breach that affects their data, it undermines accountability and weakens the public's ability to seek remedies. Therefore, breach notification should be treated as part of good administration.

At the same time, this study recognises that responsibility for cyber incidents may involve complex institutional relations. Some systems are managed by central agencies, some by local governments, and others by third-party service providers or state-owned enterprises. This creates a risk of fragmented responsibility, where each institution may shift blame to another actor. Poli and Sommario show that the attribution of responsibility in cyberattacks is legally complex, particularly when incidents involve cross-border actors or uncertain origins [14]. However, in the context of domestic administrative law, the complexity of attribution should not eliminate government responsibility toward citizens. Even when the attacker is external, the public institution remains responsible for governance failures within its authority, especially if the breach was aggravated by weak security, lack of backup, or poor incident response.

Therefore, the main legal issue is not only who committed the cyberattack, but whether the government fulfilled its administrative duties before, during, and after the breach. This shifts the analysis from a narrow criminal-law perspective toward administrative accountability. Cybercrime law may address the perpetrator, but administrative law must address the responsibility of public authorities that manage the affected systems. In this sense, public data breaches in SPBE require a dual response: enforcement against attackers and accountability of institutions responsible for protecting public data.

3.3. Toward an Accountable Cybersecurity Governance Framework for Digital Government

The third result of this study is the need for an accountable cybersecurity governance framework that integrates SPBE governance, data protection, and administrative responsibility. Such a framework should not only focus on technical prevention, but also establish clear legal standards for institutional responsibility, incident response, citizen notification, audit, and remedies. Based on the normative analysis, this study proposes six core elements of accountable cybersecurity governance in SPBE. First, public institutions must adopt a risk-based cybersecurity obligation**.** This means that every government agency operating digital public services must identify the sensitivity of the data it manages, the criticality of the service it provides, and the potential impact of system disruption. The higher the risk to citizens and public service continuity, the stronger the security obligations should be. This principle is consistent with Figueroa et al., who argue that e-government cybersecurity frameworks must include systematic risk management and regulatory compliance [6].

Second, government agencies must establish clear institutional responsibility. Cybersecurity governance requires a defined chain of responsibility among system owners, data controllers, platform operators, data centre managers, cybersecurity officers, and supervisory institutions. Without clear responsibility, public data breaches may lead to bureaucratic blame-shifting. Gasco-Hernandez et al. show that inter-agency collaboration depends on technology, leadership, governance, and collaborative capacity [18]. Wouters et al. similarly argue that integrated digital public services require inter-organisational cooperation and shared governance mechanisms [19]. These

findings are highly relevant to SPBE, because digital government operates through interconnected systems and cross-agency data exchange.

Third, the government must maintain security-by-design and accountability-by-design in digital public service systems. Security-by-design requires that cybersecurity safeguards are embedded from the planning stage of digital systems, not added only after incidents occur. Accountability-by-design requires that every digital system includes documentation, audit trails, access logs, reporting mechanisms, and review procedures. Nguyen-Duc et al. show that software security assessment in e-government projects requires both technical tools and human-driven review [7]. This supports the view that secure public systems must combine technology, human oversight, and institutional accountability.

Fourth, the government must guarantee incident response and public service continuity. A cyber incident becomes an administrative crisis when it paralyses essential services or prevents citizens from accessing their rights. Therefore, public institutions must maintain backup systems, disaster recovery plans, alternative service channels, and clear escalation procedures. The PDNS 2 incident shows that the absence or weakness of backup arrangements can intensify the public impact of a cyberattack. From an administrative-law perspective, service continuity is part of the government's obligation to provide reliable public services, especially when the state has made digital systems central to administrative access.

Fifth, affected citizens must receive notification, explanation, and remedies. Breach notification should explain what happened, what data may have been affected, what risks citizens may face, what measures the government has taken, and what remedies are available. Remedies may include correction of compromised data, identity protection measures, administrative complaint channels, compensation mechanisms where legally justified, and access to review when the breach affects administrative rights. This element distinguishes accountable cybersecurity governance from purely technical incident management.

Sixth, there must be independent audit and institutional learning. Cybersecurity governance must include regular audits, post-incident evaluation, publication of non-sensitive findings, and administrative sanctions for negligence. Audit is important not only to identify technical vulnerabilities but also to assess whether institutions followed legal duties, risk procedures, and internal controls. Ruijer's work on data collaboratives shows that data governance requires institutional design and accountability mechanisms [17]. This study extends that insight by arguing that SPBE cybersecurity governance must include post-breach accountability and organisational learning.

The proposed framework contributes to previous studies by integrating cybersecurity governance with administrative-law responsibility. Earlier research has discussed cyber risk, data breaches, e-government security, and public-sector cybersecurity challenges [1]–[10]. Other studies have examined digital governance, inter-agency collaboration, and public-sector capability [17]–[19], [25]. However, these studies generally do not formulate public data breaches as failures of administrative responsibility. This article fills that gap by arguing that cybersecurity governance in SPBE should be treated as part of the state's legal duty to provide secure, reliable, and accountable digital public services.

Overall, the discussion shows that government responsibility for public data breaches must be assessed beyond the existence of a cyberattack. The relevant legal question is whether the government had taken reasonable measures to prevent the breach, whether it responded properly when the breach occurred, and whether it provided remedies to affected citizens. In this way, cybersecurity governance becomes a concrete expression of administrative legality, duty of care, public accountability, and good governance in the digital era. Digital government can only be legitimate if the state is not merely capable of collecting and processing public data, but also legally responsible for protecting it. The third finding of this study is that algorithmic transparency and the right to explanation require an integrated normative framework. AI-based public services cannot be governed only through technical standards or ethical guidelines. They require clear legal obligations, institutional responsibility, procedural safeguards, and mechanisms for citizen remedies. Without such a framework, the use of AI in public administration may produce black-box governance, where public decisions are formally issued by government institutions but substantively shaped by opaque systems.

This study proposes six core obligations for accountable AI-based public services. First, the government must disclose the use of AI or automated decision-making systems in public service delivery. Second, the government must provide general information about the purpose, function, and scope of the system. Third, public institutions must explain the main criteria, data categories, and decision logic used in the administrative process. Fourth, affected citizens must receive an individualised explanation of the factors that influenced the decision. Fifth, citizens must have access to correction, objection, appeal, or human review. Sixth, government agencies must maintain documentation, audit trails, and accountability mechanisms to support administrative and judicial review.

This framework may be organised into three levels of transparency. The first is institutional transparency, which concerns public disclosure of the existence, purpose, and governance of AI systems used by public authorities. The second is procedural transparency, which concerns how algorithmic systems are integrated into administrative decision-making, including human oversight, documentation, and review procedures. The third is individual transparency, which concerns the explanation provided to a specific citizen affected by a particular decision. These

three levels are interconnected. Institutional transparency supports public trust, procedural transparency strengthens legality, and individual transparency protects due process.

The framework also requires meaningful human responsibility. Public officials must not merely approve algorithmic outputs without understanding their basis. Human oversight must be substantive, not symbolic. A public official should be able to review the data used, assess the relevance of algorithmic recommendations, identify potential errors, and override the system when necessary. If human oversight is reduced to automatic approval, it fails to protect citizens from arbitrary or erroneous algorithmic decisions. This finding is consistent with Meijer, Lorenz, and Wessels, who show that algorithmisation reshapes bureaucratic routines and organisational practices [10]. Ahn and Chen also show that AI adoption in government depends on public employees' perceptions, capacity, and institutional readiness [6].

Organisational capacity is therefore a central part of accountable AI governance. Selten and Klievink argue that public-sector AI adoption requires institutional arrangements that balance separation and integration of AI capabilities [8]. Van Noordt and Misuraca also show that AI use in the public sector raises governance, ethical, and organisational challenges across government institutions [7]. Similarly, Mikalef et al. emphasise that AI capability in government agencies depends on organisational, technological, and human determinants [23]. These studies support the finding that algorithmic transparency cannot be implemented effectively without trained officials, clear procedures, documentation systems, audit mechanisms, and citizen complaint channels.

Compared with previous studies, the contribution of this research lies in translating the abstract idea of explainable AI into administrative-law obligations. Previous research has discussed AI adoption, citizen trust, public-sector capability, and explainable AI [1], [3], [5], [7], [23]. Other studies have examined the philosophical and ethical foundation of the right to explanation [14]–[17]. However, this study places the right to explanation specifically within the structure of administrative law. It argues that algorithmic transparency should be treated as part of the government's duty to give reasons, ensure due process, and maintain accountability in public service decisions.

Overall, the analysis shows that AI-based public services can improve efficiency, consistency, and administrative capacity, but they also create risks of opacity, bias, and weakened procedural protection. Therefore, digital innovation in public administration must be accompanied by legal safeguards. The right to explanation provides such a safeguard by ensuring that citizens are not merely objects of automated governance, but remain legal subjects who are entitled to understand and challenge decisions affecting them. In this sense, algorithmic transparency is not only a matter of technological governance; it is a requirement of lawful, accountable, and citizen-centred public administration.

4. CONCLUSION

This study concludes that cybersecurity governance in electronic-based government systems must be understood as an integral part of administrative-law responsibility. In the context of SPBE, the government does not merely act as a user of digital technology, but also as a public authority that collects, manages, processes, stores, and distributes citizens' data for administrative and public service purposes. Therefore, when public data breaches occur in government digital systems, the issue cannot be reduced to a technical failure or cybercrime incident alone. It must also be assessed as a possible failure of public administration, especially when the breach is connected to weak risk management, inadequate security standards, poor institutional coordination, insufficient backup systems, or ineffective incident response.

The main finding of this study is that government responsibility for public data breaches can be constructed through three layers: preventive responsibility, responsive responsibility, and restorative responsibility. Preventive responsibility requires public institutions to adopt risk-based cybersecurity standards, conduct regular audits, protect digital infrastructure, and ensure adequate data backup. Responsive responsibility requires the government to detect, contain, report, and respond to cyber incidents quickly and transparently. Restorative responsibility requires the government to restore public services, notify affected citizens, evaluate institutional weaknesses, impose accountability where negligence exists, and provide appropriate remedies for citizens whose data or rights are affected. These three layers show that state responsibility does not arise only after a breach occurs, but begins from the moment the government decides to digitise public services and centralise public data.

The novelty of this study lies in its effort to combine cybersecurity governance, SPBE, and administrative-law responsibility within a single analytical framework. Previous studies have largely examined cybersecurity in e-government through technical, managerial, institutional, or data protection perspectives. This study extends those discussions by arguing that cybersecurity governance should be treated as a legal obligation of public administration. The protection of public data is not only a matter of system security, but also a manifestation of legality, duty of care, accountability, public service continuity, and good administration. In this regard, a public data breach may become an administrative-law issue when it reveals negligence or failure by public authorities to fulfil reasonable obligations in securing digital public services.

The findings also have implications for previous research on cybersecurity and digital government. Studies on government data breaches, e-government security, and public-sector cybersecurity governance have shown that cyber risks are shaped by technical vulnerability, organisational capacity, human factors, and regulatory gaps. This study

reinforces those findings, but adds that such weaknesses must be translated into legal accountability standards. It also complements studies on inter-agency collaboration in digital government by showing that fragmented institutional responsibility may worsen the impact of cyber incidents. Therefore, cybersecurity governance in SPBE requires not only better technology, but also clearer legal mandates, stronger coordination, documented risk management, transparent breach notification, and accessible remedies for affected citizens.

Nevertheless, this study has limitations. As a normative juridical study, it does not conduct empirical investigation into the internal cybersecurity practices of specific government institutions. It also does not perform technical forensic analysis of particular cyber incidents or evaluate the effectiveness of existing government security systems. The analysis is focused on the legal and conceptual construction of responsibility. Therefore, the findings should be read as a normative framework that still requires empirical testing in real institutional settings.

Future research should examine how government agencies implement cybersecurity governance in practice, particularly in relation to risk assessment, data backup, incident response, breach notification, and citizen remedies. Empirical studies involving public officials, cybersecurity practitioners, data protection officers, and affected citizens would help explain the gap between legal norms and administrative practice. Comparative research is also needed to analyse how different jurisdictions regulate government responsibility for public data breaches and how such models may inform the development of SPBE governance in Indonesia. Further interdisciplinary studies involving law, public administration, and cybersecurity are essential to ensure that digital government remains not only efficient and integrated, but also secure, accountable, and legally responsible.

5. REFERENCES

[1] D. Ribeiro, J. Fonte, and L. Antunes, "Assessing the information security posture of online public services worldwide: Technical insights, trends and policy implications," *Government Information Quarterly*, vol. 42, no. 3, Art. no. 102031, 2025, doi: https://doi.org/10.1016/j.giq.2025.102031.

[2] S. Hamid and M. N. Huda, "Mapping the landscape of government data breaches: A bibliometric analysis of literature from 2006 to 2023," *Social Sciences & Humanities Open*, vol. 11, Art. no. 101234, 2025, doi: https://doi.org/10.1016/j.ssaho.2024.101234.

[3] S. Mushtaq and M. Shah, "Mitigating cybercrimes in e-government services: A systematic review and bibliometric analysis," *Digital*, vol. 5, no. 1, Art. no. 3, 2025, doi: 10.3390/digital5010003.

[4] S. T. Hossain, T. Yigitcanlar, K. Nguyen, and Y. Xu, "Cybersecurity in local governments: A systematic review and framework of key challenges," *Urban Governance*, vol. 5, no. 1, pp. 1–19, 2025, doi: https://doi.org/10.1016/j.ugj.2024.12.010.

[5] L. Magnusson, S. Iqbal, and F. Dalipi, "Information security governance in the public sector: Investigations, approaches, measures, and trends," *International Journal of Information Security*, vol. 24, Art. no. 177, 2025, doi: https://doi.org/10.1007/s10207-025-01097-x.

[6] V. Figueroa, L. E. Sánchez Crespo, A. Santos-Olmo, D. G. Rosado, and E. Fernández-Medina, "Building a holistic cybersecurity framework for e-Government based on a systematic analysis of proposals," *International Journal of Information Security*, vol. 24, Art. no. 121, 2025, doi: https://doi.org/10.1007/s10207-025-01024-0.

[7] A. Nguyen-Duc, M. V. Do, Q. L. Hong, K. N. Khac, and A. N. Quang, "On the adoption of static analysis for software security assessment: A case study of an open-source e-government project," *Computers & Security*, vol. 111, Art. no. 102470, 2021, doi: https://doi.org/10.1016/j.cose.2021.102470.

[8] S. T. Hossain, T. Yigitcanlar, K. Nguyen, and Y. Xu, "Understanding local government cybersecurity policy: A concept map and framework," *Information*, vol. 15, no. 6, Art. no. 342, 2024, doi: https://doi.org/10.3390/info15060342.

[9] S. T. Hossain, T. Yigitcanlar, K. Nguyen, and Y. Xu, "Local government cybersecurity landscape: A systematic review and conceptual framework," *Applied Sciences*, vol. 14, no. 13, Art. no. 5501, 2024, doi: https://doi.org/10.3390/app14135501.

[10] F. Cremer, B. Sheehan, M. Fortmann, A. N. Kia, M. Mullins, F. Murphy, and S. Materne, "Cyber risk and cybersecurity: A systematic review of data availability," *The Geneva Papers on Risk and Insurance—Issues and Practice*, vol. 47, pp. 698–736, 2022, doi: https://doi.org/10.1057/s41288-022-00266-6.

[11] W. W. Li, A. C. M. Leung, and W. T. Yue, "Where is IT in information security? The interrelationship among IT investment, security awareness, and data breaches," *MIS Quarterly*, vol. 47, no. 1, pp. 317–342, 2023, doi: https://doi.org/10.25300/MISQ/2022/15713.

[12] M. Prictor, "Data breach notification laws—Momentum across the Asia-Pacific region," *Journal of Bioethical Inquiry*, vol. 20, no. 4, pp. 1–7, 2023, doi: https://doi.org/10.1007/s11673-023-10324-w.

[13] M. F. R. Ba'abud and D. S. N. Heriyanto, "Application of the principles of extraterritorial jurisdiction towards personal data breach committed cross-country borders," *Uti Possidetis: Journal of International Law*, vol. 5, no. 1, pp. 106–137, 2024, doi: https://doi.org/10.22437/up.v5i1.28300.

[14] S. Poli and E. Sommario, "The rationale and the perils of failing to invoke state responsibility for cyber-attacks: The case of the EU cyber sanctions," *German Law Journal*, vol. 24, no. 3, pp. 522–536, 2023, doi: https://doi.org/10.1017/glj.2023.25.
[15] M. J. Ahn and Y.-C. Chen, "Digital transformation toward AI-augmented public administration: The perception of government employees and the willingness to use AI in government," *Government Information Quarterly*, vol. 39, no. 2, Art. no. 101664, 2022, doi: https://doi.org/10.1016/j.giq.2021.101664.
[16] C. van Noordt and G. Misuraca, "Artificial intelligence for the public sector: Results of landscaping the use of AI in government across the European Union," *Government Information Quarterly*, vol. 39, no. 3, Art. no. 101714, 2022, doi: https://doi.org/10.1016/j.giq.2022.101714.
[17] E. Ruijer, "Designing and implementing data collaboratives: A governance perspective," *Government Information Quarterly*, vol. 38, no. 4, Art. no. 101612, 2021, doi: https://doi.org/10.1016/j.giq.2021.101612.
[18] M. Gasco-Hernandez, J. R. Gil-Garcia, and L. F. Luna-Reyes, "Unpacking the role of technology, leadership, governance and collaborative capacities in inter-agency collaborations," *Government Information Quarterly*, vol. 39, no. 3, Art. no. 101710, 2022, doi: https://doi.org/10.1016/j.giq.2022.101710.
[19] S. Wouters, M. Janssen, V. Lember, and J. Crompvoets, "Strategies to advance the dream of integrated digital public service delivery in inter-organizational collaboration networks," *Government Information Quarterly*, vol. 40, no. 1, Art. no. 101779, 2023, doi: https://doi.org/10.1016/j.giq.2022.101779.
[20] S. K. Sharma, B. Metri, Y. K. Dwivedi, and N. P. Rana, "Challenges common service centers face in delivering e-government services in rural India," *Government Information Quarterly*, vol. 38, no. 2, Art. no. 101573, 2021, doi: https://doi.org/10.1016/j.giq.2021.101573.
[21] S. Malodia, A. Dhir, M. Mishra, and Z. A. Bhatti, "Future of e-government: An integrated conceptual framework," *Technological Forecasting and Social Change*, vol. 173, Art. no. 121102, 2021, doi: https://doi.org/10.1016/j.techfore.2021.121102.
[22] R. Kumar, A. Mukherjee, and A. Sachan, "Factors influencing indirect adoption of e-Government services: A qualitative study," *Information Systems and e-Business Management*, vol. 21, pp. 471–504, 2023, doi: https://doi.org/10.1007/s10257-023-00637-z.
[23] I. Savveli, M. Rigou, and S. Balaskas, "From e-government to AI e-government: A systematic review of citizen attitudes," *Informatics*, vol. 12, no. 3, Art. no. 98, 2025, doi: https://doi.org/10.3390/informatics12030098.
[24] T. Haesevoets, B. Verschuere, R. Van Severen, and A. Roets, "How do citizens perceive the use of artificial intelligence in public sector decisions?," *Government Information Quarterly*, vol. 41, no. 1, Art. no. 101906, 2024, doi: https://doi.org/10.1016/j.giq.2023.101906.
[25] P. Mikalef, K. Lemmer, C. Schaefer, M. Ylinen, S. O. Fjørtoft, H. Y. Torvatn, M. Gupta, and B. Niehaves, "Enabling AI capabilities in government agencies: A study of determinants for European municipalities," *Government Information Quarterly*, vol. 39, no. 4, Art. no. 101596, 2022, doi: https://doi.org/10.1016/j.giq.2021.101596.