



Data Breaches in Government Digital Public Services: A Systematic Mapping of Research and Governance Challenges (2015–2025)

Indah Purwaningsih*

Universitas Muhammadiyah Yogyakarta,
Indonesia

Dian Eka Rahmawati

Universitas Muhammadiyah Yogyakarta,
Indonesia

***Corresponding author:**

Indah Purwaningsih,
Universitas Muhammadiyah Yogyakarta,
Indonesia. ✉indah.p.isip25@mail.umy.ac.id

Article Info:

Article history:

Received: September 15, 2026

Revised: October 14, 2026

Accepted: October 21, 2026

Available Online: October 28, 2026

Keywords:

Bibliometric and Scientometric
Analysis;
Data Breaches;
Digital Public Services;
Indonesia;
Public Sector Data Governance



This is an open access article under the
CC BY-SA license.

Copyright © 2026 by Author. Published by
Politeknik Siber Cerdika International

Abstract

Background: The rapid digital transformation of public services has increased the collection and use of citizens' personal data, intensifying concerns about data breaches in government-operated systems. However, existing research remains fragmented, with technical cybersecurity perspectives receiving greater attention than governance and public administration perspectives.

Objective: This study aims to systematically map global research on data breaches in digital public services from 2015 to 2025 and identify theoretical and governance gaps relevant to the Indonesian context.

Methods: A systematic literature review guided by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines was combined with bibliometric and scientometric analyses of publications indexed in Scopus. Descriptive bibliometric analysis and author keyword co-occurrence mapping using VOSviewer were conducted on 1,169 open-access documents, while 62 articles meeting the final eligibility criteria were examined through qualitative synthesis.

Results: The findings reveal an increase in research output and six thematic clusters. Cybersecurity and data security had the highest keyword occurrence (235), whereas privacy, ethics, and data protection exhibited the greatest total link strength (457). Governance, institutional accountability, organizational capacity, and public trust remain comparatively less integrated into technical cybersecurity research.

Conclusion: This study reconceptualizes data breaches in digital public services as sociotechnical governance challenges involving technological vulnerabilities, institutional capacity, regulatory arrangements, and public trust. The findings provide a conceptual foundation for strengthening public-sector data governance in Indonesia while highlighting the need for empirical validation and further comparative research.

To cite this article: Purwaningsih, I., & Rahmawati, D. E. (2026). Data breaches in government digital public services: A systematic mapping of research and governance challenges (2015–2025). *Journal of Business, Social and Technology*, 7(5), 2690-2708. <https://doi.org/10.59261/bustechno.v7i5.849>

INTRODUCTION

Digital transformation in public services is a key component of modern public sector reform, aimed at improving efficiency, accessibility, and transparency. Governments around the world increasingly rely on digital platforms to deliver essential services, including population administration, healthcare, taxation, social assistance, and immigration. Digital transformation streamlines bureaucratic processes, reduces administrative costs, and enhances service delivery efficiency (Anggara et al., 2024; Kayyali, 2025; moutamir & El Qour, 2025; Zakiuddin & Anggara, 2024). Although digital transformation in public services offers numerous benefits, including improved efficiency, accessibility, and transparency, it also introduces significant risks related to

data protection and inclusivity. The digitization of public services raises serious concerns about the protection of personal data, including the risks of data breaches, identity theft, and unauthorized access to sensitive information (Apostolos, 2021; Digay et al., 2025). The volume, sensitivity, and interconnectedness of the personal data managed by government institutions make digital public services particularly vulnerable to data breaches. International literature indicates that data breaches in the public sector are not caused solely by technical weaknesses in information systems but are also closely associated with governance failures, limited organizational capacity, inadequate coordination, and weak institutional accountability in the management of digital risks (Bannister & Connolly, 2015; Lodge & Wegrich, 2014; Mazzucato & Kattel, 2026). Data breaches affecting digital public services not only disrupt service continuity but also raise fundamental concerns about privacy protection, institutional legitimacy, and public trust in government, all of which are essential to the success of digital government initiatives (Grimmelikhuijsen et al., 2013; Tai, 2026).

In recent years, data breaches affecting digital public services have become a growing concern in terms of both frequency and scale. Governments face a wide range of threats, including cyberattacks, system misconfigurations, insider threats, and third-party security failures, which can result in unauthorized access to personal data. Cyberattacks have become increasingly sophisticated and frequent, targeting various sectors, including public services. These attacks may involve malware, phishing, denial-of-service attacks, and ransomware, potentially resulting in significant data breaches (Fouracres, 2023; Kumar & Singh, 2021; Sleem, 2022). Information security studies emphasize that the rapid digitization of the public sector is often not accompanied by corresponding improvements in institutional capacity, regulatory frameworks, and information security culture, thereby increasing vulnerability to large-scale data breaches (Janssen & Estevez, 2013; Saydi et al., 2025). In Indonesia, public-sector data breaches have intensified concerns about institutional readiness, digital infrastructure security, and the effectiveness of personal data governance. Such incidents highlight the broader challenge of protecting citizens' personal information amid rapid digital transformation and underscore the importance of institutional accountability and the effective implementation of data protection regulations. This situation has heightened public concern and intensified policy debates about institutional readiness, digital infrastructure security, and the effectiveness of government data protection governance.

Empirical analyses of large-scale incident data underscore the magnitude of this problem. A systematic examination of more than 12,000 cyber incidents found that breaches involving the loss of personal and sensitive records constituted a substantial and recurring proportion of reported incidents and that the public sector was among the most frequently affected domains (Lallie et al., 2025; Romanosky, 2016). Reviews of public digital infrastructures similarly indicate that security and privacy risks intensify as governments expand interconnected data systems, while the capacity to address these risks remains unevenly distributed across jurisdictions, with some better-resourced jurisdictions having greater capacity to manage them (Ismagilova et al., 2022). These findings suggest that data breaches affecting public services are neither isolated nor marginal incidents but constitute a structural and quantitatively significant governance challenge.

Unlike data breaches in the private sector, those affecting public services have distinctive implications because governments act as custodians of citizens' data, which they are legally required to collect and manage. Public administration literature emphasizes that government failures to protect public data can undermine institutional legitimacy and weaken public trust in the state's digital transformation agenda (Vatamanu & Tofan, 2025; Wirtz & Müller, 2018). Indonesia is undergoing rapid digital transformation, which presents significant risks when the pace of technology adoption outstrips the development of governance frameworks, system interoperability, and data management capacity. Data integration and synchronization across platforms remain major challenges. For example, in the health sector, insufficient interoperability among electronic health systems hampers efficient data exchange (Amin et al., 2020; Heryawan et al., 2025; Sonia Dewi et al., 2024).

Despite their scale and wide-ranging impacts, data breaches in Indonesia remain relatively underrepresented in indexed international academic literature. When discussed, these

incidents are often treated as isolated events rather than examined within a broader comparative and theoretical discourse on digital governance and public sector accountability. Most studies approach data breaches primarily from a technical or cybersecurity perspective, focusing on system vulnerabilities, encryption mechanisms, and network security. However, research indicates that organizational, regulatory, and governance dimensions are also critical to data protection in the public sector. Clear policy implementation, staff training, and robust accountability mechanisms are essential for regulatory compliance and data breach prevention (Garbaccio & Kischelewski, 2024; Jenson, 2008; Rahman, 2025). By contrast, public administration and e-government studies tend to focus on digital service adoption, performance, and citizen satisfaction but rarely treat data breaches as a central analytical concern. Consequently, the existing literature has yet to provide an integrated understanding of data breaches as socio-technical governance failures arising from interactions among technology, organizational practices, and institutional arrangements (Bannister & Connolly, 2015; Janssen & Estevez, 2013; Saydi et al., 2025).

To clarify how this study differs from prior research, three closely related strands of scholarship can be compared. First, Bannister and Connolly (2015) and Abdulkareem et al. (2022) examine the theoretical foundations of e-government and argue that the field contains numerous descriptive case studies but lacks integrative theory; however, their analysis does not specifically address data security or data breach incidents. Second, Janssen and Estevez (2013) and Saydi et al. (2025) analyze lean and platform-based digital government, emphasizing efficiency and interoperability while giving comparatively limited attention to information security risks. Third, Wirtz and Müller, (2018) and Vatamanu and Tofan (2025) propose an integrated framework for public sector technology governance but do not explicitly connect it to the empirical phenomenon of data breaches. Across these studies, the dominant focus is on governance capacity or digital service performance, the methods are primarily conceptual or case-based, and a shared limitation is the absence of a systematic, evidence-based mapping that positions data breaches as a governance problem. The present study addresses this gap.

These conditions indicate a clear gap between normative frameworks and empirical practice. Conceptually, the governance of digital public services requires the protection of personal data, institutional accountability, and the safeguarding of citizens' rights as fundamental principles. However, the Indonesian context suggests that data breaches continue to occur, indicating that these principles may not yet be adequately embedded in public sector governance practices. Although Law No. 27 of 2022 on Personal Data Protection (the PDP Law) has been enacted, its implementation faces challenges related to inadequate digital infrastructure and limited institutional accountability (Rahman, 2025; Syifa et al., 2025). This underscores the need to understand data breaches not merely as technological failures but as broader governance and public administration problems involving interactions among organizational capacity, regulatory arrangements, and social dynamics, particularly public trust.

Accordingly, the novelty of this study lies not merely in asserting that data breaches are governance failures but in demonstrating, through a systematic bibliometric and scientometric mapping of a decade of global scholarship, that the existing literature is structurally fragmented across technical, legal, ethical, and administrative domains. Previous research has neither quantified this fragmentation nor synthesized the findings into a single analytical framework. This study therefore contributes an evidence-based reconceptualization of data breaches as socio-technical governance failures and develops an integrative framework connecting technological vulnerabilities, organizational capacity, regulatory arrangements, and public trust.

Against this background, this study aims to systematically map and analyze the development of global research on data breaches affecting digital public services and identify governance and theoretical gaps relevant to the Indonesian context. Specifically, the study examines research trends, dominant themes, and the intellectual structure shaping scholarly discourse on data breaches while identifying gaps between technical cybersecurity approaches and public administration perspectives on governance. In addition, the study develops a conceptual synthesis linking data breaches to technological vulnerabilities, organizational capacity, governance and regulatory frameworks, and social impacts, particularly public trust. The Indonesian context, including the implementation of the Personal Data Protection Law and the

Electronic-Based Government System (Sistem Pemerintahan Berbasis Elektronik, SPBE) policy, serves as an analytical reference for strengthening the study's theoretical relevance and policy implications. Importantly, this study does not empirically investigate individual data breach incidents in Indonesia. Instead, it systematically maps the global academic literature and interprets the identified theoretical and governance gaps in relation to Indonesia's digital public services and data governance context.

This study offers both theoretical and practical contributions. Theoretically, it advances public administration and digital governance scholarship by bridging the longstanding divide between technical cybersecurity research and e-government studies and by providing an integrative conceptual vocabulary for analyzing public-sector data breaches. Practically, it provides public data managers and policymakers in Indonesia with an evidence-informed basis for strengthening institutional accountability, interagency coordination, and post-incident response under the Personal Data Protection Law and the Electronic-Based Government System (SPBE) policy. The broader implication is that reducing data breach risks requires governance reform—including clear mandates, effective oversight, and capacity building—rather than technological investment alone.

METHOD

This study applies a systematic literature review combined with bibliometric and scientometric analyses to map and synthesize research on data breaches in digital public services. The review process follows PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines to ensure transparency, reproducibility, and rigor in literature identification, screening, eligibility assessment, and inclusion (Page et al., 2022), thereby minimizing selection bias and ensuring that the analysis is based on relevant, high-quality publications.

Following literature selection, the study employs bibliometric and scientometric analyses to examine knowledge structures, thematic patterns, and conceptual relationships through publication trends, keyword co-occurrence, co-citation, and author collaboration networks (Aria & Cuccurullo, 2017; Donthu et al., 2021; Klarin, 2024). Integrating PRISMA with scientific mapping, this approach provides both a quantitative overview of the literature and a robust basis for identifying research gaps and future directions, in line with best practices for analyzing conceptual fragmentation and knowledge evolution in multidisciplinary fields such as digital government and data security (Janssen & Estevez, 2013; Ogutu et al., 2023; Zupic & Čater, 2015). This methodological design ensures analytical rigor while positioning the study within governance-oriented digital government research.

Bibliometric analysis is used to examine the quantitative characteristics of research on data breaches in digital public services by mapping publication patterns, temporal trends, and thematic distributions based on document metadata (titles, abstracts, keywords, citations, and affiliations). This method enables objective and replicable identification of the intellectual structure and evolution of a multidisciplinary and rapidly developing field (Donthu et al., 2021; Ogutu et al., 2023; Zupic & Čater, 2015). Bibliographic data were sourced from Scopus due to its broad multidisciplinary coverage, indexing quality, and relevance to public administration, e-government, information systems, and cybersecurity studies.

Scopus was selected as the sole data source due to its consistent metadata and strong support for comprehensive scientific mapping, ensuring data comparability in large-scale bibliometric analyses (Aria & Cuccurullo, 2017; Donthu et al., 2021; Klarin, 2024). A systematic search was conducted using the Scopus advanced search function. The initial search employed the terms “data breach” OR “data leakage” OR “personal data breach” OR “information security incident.” The resulting records were subsequently restricted by publication year, subject area, language, document type, and access status, followed by title-and-abstract and full-text screening to identify studies specifically addressing data breaches in government-provided digital public services.

The search was limited to English-language journal articles published between 2015 and 2025, with no geographic restrictions, to capture the global discourse on data breaches in digital public services. Search results were exported in CSV format and screened following PRISMA

guidelines, including duplicate removal, title and abstract screening, and full-text eligibility assessment based on predefined criteria (Moher et al., 2009; Page et al., 2022), ensuring a relevant, transparent, and replicable bibliometric dataset.

To ensure transparency and reproducibility, the Scopus search was executed on a single date, 15 August 2025, to provide a fixed and citable snapshot of the database. Exported records were screened in a stepwise manner: duplicate records were removed automatically in the reference manager and verified manually; titles and abstracts were then screened against the inclusion criteria; and the remaining records underwent full-text eligibility assessment. Screening was conducted by the first author, while the second author cross-checked the screening decisions. Disagreements were resolved through discussion. To further assess the consistency of the inclusion decisions and reduce potential selection bias, a subsample of records was re-screened.

To complement the bibliometric analysis, this study employs scientometric science mapping to identify the intellectual structure and conceptual relationships in the literature on data breaches in digital public services by examining thematic clusters of interconnected concepts (Ogutu et al., 2023; Zupic & Čater, 2015). The analysis was conducted using VOSviewer (Visualization of Similarities viewer, v1.6.20) through author keyword co-occurrence analysis, which maps conceptual proximity based on the co-occurrence of keywords within the same documents (McAllister et al., 2022; van Eck & Waltman, 2010). Author keywords were selected as the primary unit of analysis because they directly represent the core conceptual focus of each publication and are considered more reflective of authors' theoretical intentions than index keywords (Aria & Cuccurullo, 2017; Liu et al., 2023).

The co-occurrence network was constructed based on the frequency with which two or more keywords appear together within a single document, using the association strength normalization method, as recommended in the development of VOSviewer's mapping algorithms to produce a more accurate representation of conceptual distances (McAllister et al., 2022; van Eck & Waltman, 2010). To enhance the clarity and interpretability of the analysis, a minimum occurrence threshold was applied, such that only keywords with a certain level of frequency were included in the network mapping. Specifically, a minimum co-occurrence threshold of five was applied, so that only author keywords appearing in at least five documents were retained for network construction; this value balances network readability against the risk of discarding substantively relevant but less frequent terms (McAllister et al., 2022; van Eck & Waltman, 2010).

To reduce noise and focus on substantively significant concepts, the analysis applied a minimum occurrence threshold (Donthu et al., 2021; Klarin, 2024). Two indicators were used: occurrence, measuring a keyword's prominence across documents, and total link strength (TLS), indicating its conceptual interconnectedness and relative centrality within the network (Shao & Shi, 2023; van Eck & Waltman, 2014). Keyword clustering was performed automatically using the VOSviewer algorithm based on relationship density and visualized through color-coded clusters to support thematic interpretation.

Through this approach, scientometric analysis enables the identification of dominant thematic clusters and the evaluation of the degree of fragmentation and integration within the literature, particularly in assessing whether data breaches are treated primarily as technical security issues, ethical and privacy concerns, or governance challenges in digital public services. This approach aligns with contemporary scientometric practices that emphasize network analysis and knowledge visualization as key instruments for understanding the intellectual structure and developmental dynamics of a research field in a systematic, transparent, and replicable manner (Aria & Cuccurullo, 2017; Ogutu et al., 2023; Zupic & Čater, 2015).

RESULTS AND DISCUSSION

Results

The initial screening stage was conducted by applying temporal, disciplinary, and publication-type criteria to limit the scope of the study to literature relevant to digital public services and public sector governance. The filters applied included publication year, the Social Sciences subject area, English-language publications, and journal-article document types. These restrictions were intended to ensure that the analyzed literature had strong conceptual relevance to public administration and digital government studies and was not dominated by research that

was purely technical or focused on information systems engineering (Janssen & Estevez, 2013; Ogutu et al., 2023; Saydi et al., 2025; Zupic & Čater, 2015). Subsequently, the remaining documents were evaluated through title and abstract screening to assess the alignment of their research focus with data breach issues in the context of government-provided digital public services.

Articles that discussed data breaches in general without a clear connection to the public sector, or that treated the issue exclusively as a technical problem without implications for governance and public administration, were excluded from the analysis. Articles that met the inclusion criteria then underwent full-text assessment to ensure substantive alignment with the study's objectives and conceptual framework. This stepwise selection process is consistent with systematic review practices that emphasize the importance of consistent criteria and documented exclusion decisions to minimize selection bias (Kitchenham & Charters, 2007; Page et al., 2022). Through these data collection and selection stages, this study established a body of literature with strong empirical and theoretical relevance for further analysis. This systematic data collection process provides the foundation for mapping research trends, intellectual structures, and research gaps through bibliometric and scientometric analyses of studies on data breaches in digital public services.

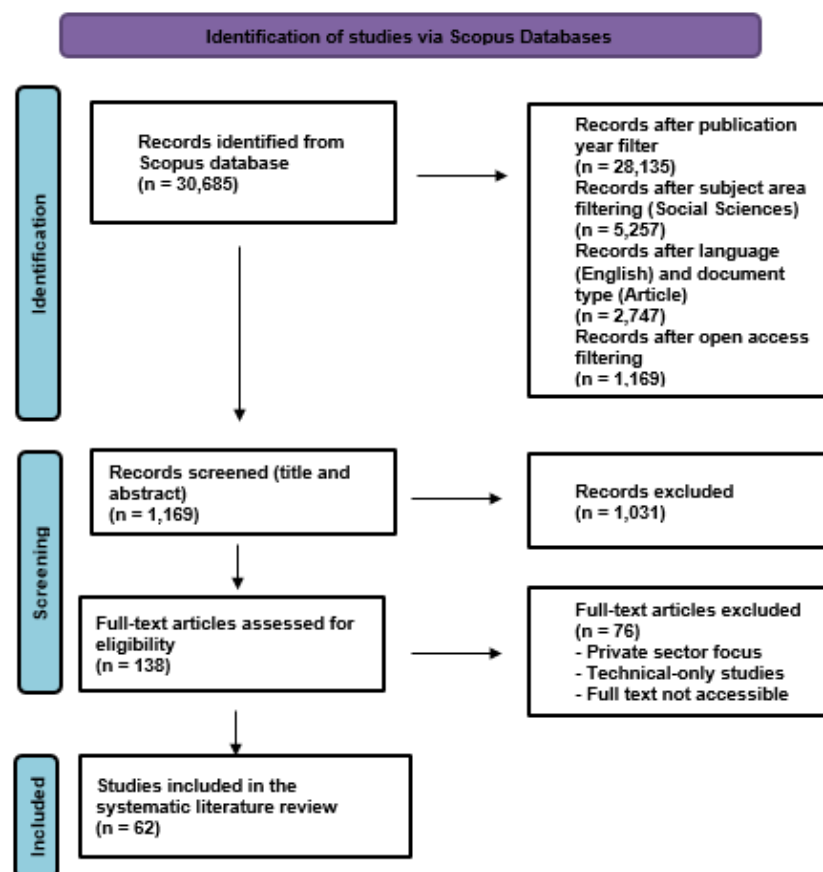


Figure 1. PRISMA 2020 flow diagram of the study selection process.

Source : Scopus database, authors' analysis.

The literature selection process followed the PRISMA 2020 guidelines to ensure transparency and reproducibility. The initial search of the Scopus database using the query string “data breach” OR “data leakage” OR “personal data breach” OR “information security incident” yielded 30,685 documents. After the publication period was limited to 2015–2025, the number of records decreased to 28,135. Subsequent filtering by subject area restricted the dataset to the Social Sciences, resulting in 5,257 documents. Further restrictions to English-language publications and journal articles reduced the dataset to 2,747 records. To enhance accessibility

and traceability, the analysis was restricted to open-access publications, yielding 1,169 articles.

Title and abstract screening excluded 1,031 articles that did not explicitly address data breaches in the context of the public sector or government-provided digital services. A total of 138 articles underwent full-text eligibility assessment. Of these, 76 articles were excluded because they primarily focused on private-sector contexts, presented purely technical discussions without relevance to public administration, or lacked accessible full texts. Consequently, 62 articles met all inclusion criteria and were retained for the final analysis. Figure 1 presents the complete PRISMA flow diagram illustrating the selection process.

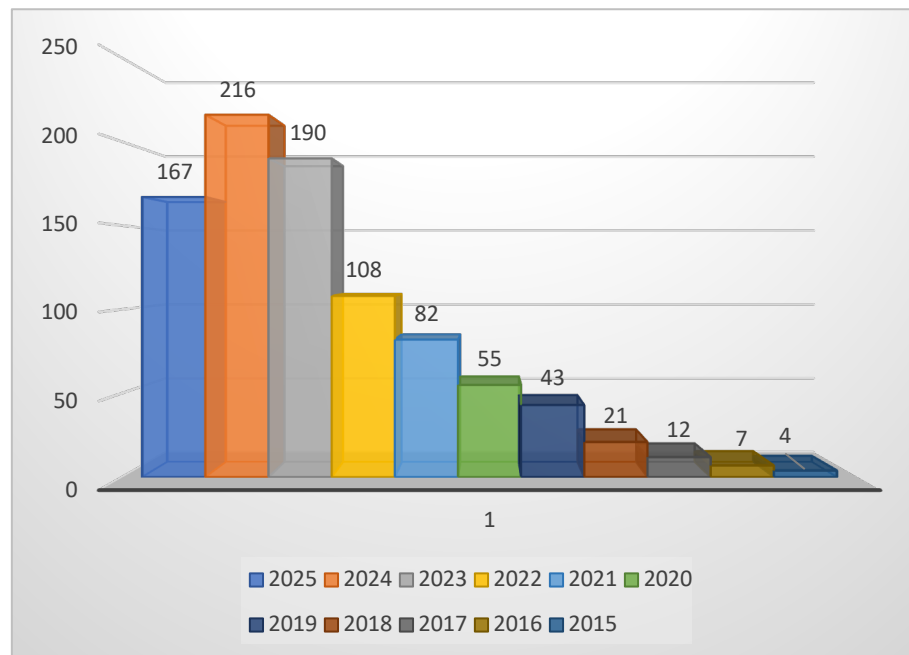


Figure 2. Growth of academic publications on data breaches in digital public services (2015–2025)

Source: Scopus database, authors' analysis.

Figure 2 illustrates the annual distribution of academic publications related to data breaches in digital public services between 2015 and 2025. The annual publication count increased overall from 4 publications in 2015 to 167 in 2025, although the trend was not consistently upward. Publication output remained relatively limited during the early years, with 7 publications in 2016, 12 in 2017, and 21 in 2018, before increasing to 43 in 2019 and 55 in 2020. Publication output continued to rise, reaching 82 in 2021, 108 in 2022, and 190 in 2023. The highest annual publication output was recorded in 2024, with 216 publications, followed by a decline to 167 in 2025. These findings indicate a substantial expansion of scholarly interest in data breaches in digital public services, particularly between 2021 and 2024, despite the decline observed in the final year of the study period.

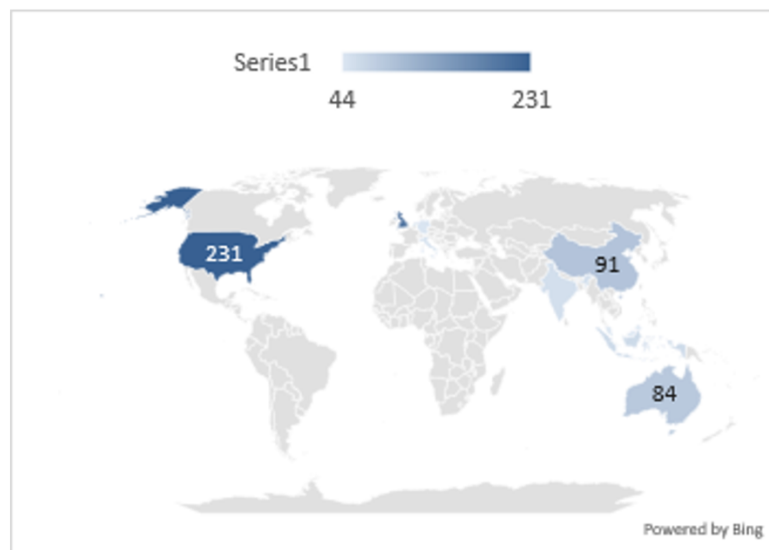


Figure 3. Country-wise distribution of Scopus-indexed publications on data breaches in government digital public services
Source: Scopus database, authors' analysis.

Figure 3 presents the country-level distribution of publications based on authors' institutional affiliations. The United States recorded the highest number of publications, followed by China, India, and Australia. European countries also contributed a substantial number of publications, while representation from Africa, Latin America, and Southeast Asia remained limited. The distribution illustrates an uneven geographic pattern in the production of Scopus-indexed research on data breaches in digital public services, with publication activity concentrated in a relatively small number of countries.

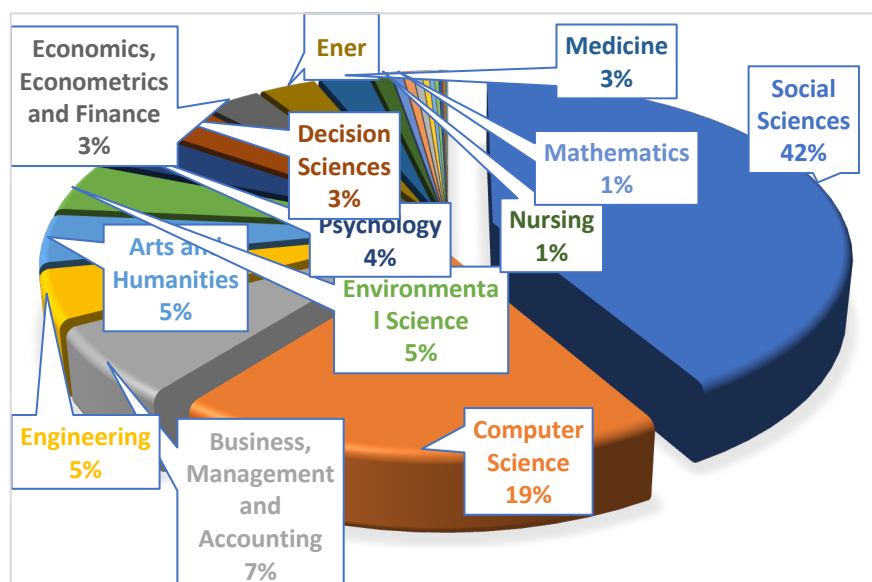


Figure 4. Distribution of Scopus-indexed publications by subject area of data breaches in government digital public services.
Source: Scopus database, authors' analysis

Figure 4 displays the distribution of publications by subject area. Social Sciences accounted for the largest share (42%), followed by Computer Science (19%). Other contributing fields included Business, Management and Accounting (7%), Engineering (5%), Arts and

Humanities (5%), and Environmental Science (5%). Additional subject areas, including Psychology, Decision Sciences, Economics, Medicine, Energy, Mathematics, and Nursing, each accounted for smaller proportions. The results indicate that research on data breaches in digital public services spans multiple disciplinary domains.

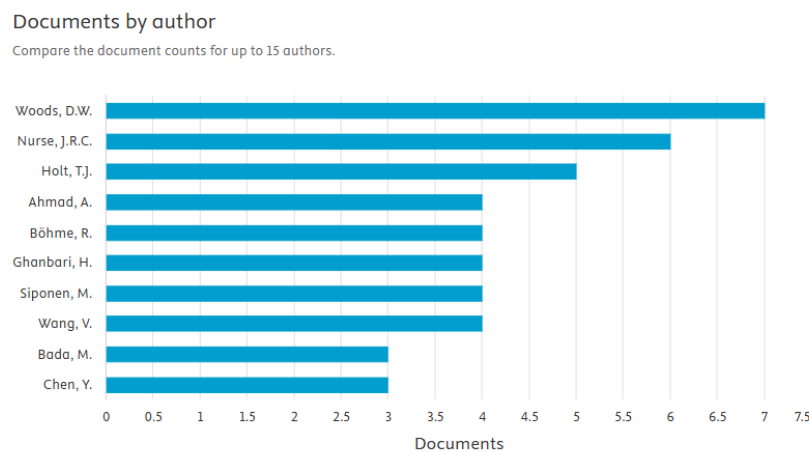


Figure 5. Documents by author in the literature on data breaches in digital public services.
Source: Scopus database, authors' analysis

Figure 5 presents the distribution of publications by author. The results show that research output in this field is distributed across multiple authors, with no single author dominating the literature. Several authors contributed multiple publications, while the majority authored one or two articles. This distribution reflects a dispersed authorship pattern within the dataset.

Building on the descriptive results presented above, this section interprets the identified patterns and clusters through a governance and public administration lens to explain their theoretical and practical implications. Author keyword co-occurrence analysis was conducted to identify the thematic structure and dominant research focuses in the literature on data security and protection in digital services. The analysis was performed on the broader corpus of 1,169 open-access Scopus-indexed documents retrieved before full-text screening, rather than on the 62 articles retained for the final qualitative synthesis. The results were visualized using VOSviewer (version 1.6.20). Two main indicators were employed: total occurrences, which measure the frequency of a keyword across the documents analyzed, and total link strength (TLS), which represents the cumulative strength of a keyword's links with other keywords in the thematic network.



Figure 6. Network visualization of author keyword co-occurrence for data breaches in government digital public services, generated using VOSviewer
Source: Scopus database, authors' analysis

Table 2
Analysis of Author Keyword Clustering Using VOSviewer

(	Main Thematic Focus	Dominant Keywords	Total Occurrence	Total Link Strength	Exemplary Studies (Scopus)
Purple	Cybersecurity & Data Security	cybersecurity; cybercrime; information security; data security; security	235	447	Malatji et al. (2021); Ismagilova et al. (2022); Shaikh & Siponen (2023); Tripathi & Behl (2020); Oroni & Fu (2025)
Blue	Privacy, Ethics & Data Protection	privacy; ethics; data protection; personal data; GDPR	194	457	Malatras et al. (2017); Floridi et al. (2018); Tikkinen-Piri et al. (2018); Goggin et al. (2019); Wong (2017); Attidhira & Permana (2022)
Green	Social Media & Digital Platform	social media; facebook; surveillance; platform governance	79	162	Kietzmann et al. (2011); Bucher (2018); Gillespie (2019)
Yellow	Artificial Intelligence & Data Analytics	artificial intelligence; machine learning; deep learning; large language models	101	196	Shokri et al. (2017); LeCun et al. (2015); Bender et al. (2021)
Orange	Cyber Threats & Technical Protection	malware; ransomware; phishing; cryptography	37	78	Farwell & Rohozinski, (2011); Verkijika (2018); Jones et al. (2019); Katz & Lindell (2025)
Tosca	Risk Management, Governance & Trust	risk management; cyber insurance; trust; governance	59	144	Katz & Lindell (2025); Pavlou (2003); van Loon & Toshkov (2015); Saydi et al. (2025); ISO/IEC 27005

Figure 6 and Table 2 summarize the results of the author keyword co-occurrence analysis of Scopus-indexed publications, identifying six main thematic clusters in the cybersecurity and data protection literature. The cybersecurity and data security cluster (purple) recorded the highest total number of keyword occurrences (235), whereas the privacy, ethics, and data protection cluster (blue) had the highest total link strength (457). Figure 6 illustrates the prominent positions of both clusters within the research landscape. Based on the applied occurrence threshold, six keyword clusters were identified. Figure 6 visualizes the keyword network, while Table 2 summarizes the clusters, dominant keywords, total occurrences, and total link strength values. The identified clusters cover cybersecurity and data security; privacy, ethics, and data protection; social media and digital platforms; artificial intelligence and data analytics;

cyber threats and technical protection; and risk management, governance, and trust. The cybersecurity and data security cluster recorded the highest keyword occurrence, while the privacy, ethics, and data protection cluster demonstrated the highest total link strength. The remaining clusters exhibited lower occurrence and connectivity values.

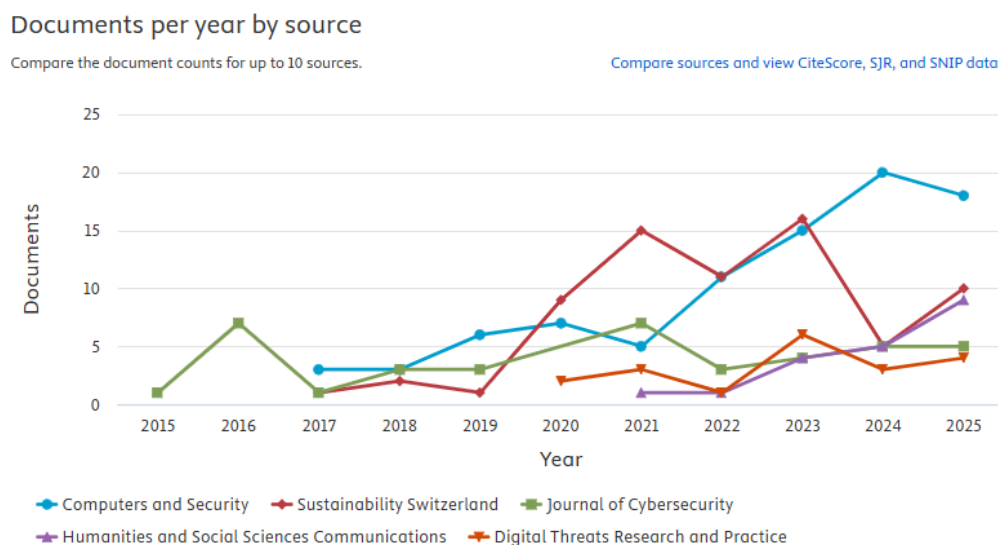


Figure 7. top 5 most productive journals
Source: Scopus database, authors' analysis.

Figure 7 presents the most productive journal sources publishing research on data breaches and digital public services. Computers & Security emerged as the most prolific journal, followed by Journal of Cybersecurity, Sustainability, Humanities and Social Sciences Communications, and Digital Threats: Research and Practice. Publication trends varied across journals, with some showing steady growth and others exhibiting fluctuations over the observation period. Taken together, these results provide a descriptive overview of publication trends, geographic distribution, disciplinary composition, authorship patterns, journal sources, and thematic structures in the literature on data breaches in digital public services. The findings map the empirical structure of the literature without engaging in theoretical interpretation, which is addressed in the subsequent Discussion section.

Discussion

This discussion interprets the results of the bibliometric and scientometric analyses to explain how the literature on data breaches in digital public services has evolved, how its dominant perspectives are structured, and where key theoretical gaps remain. Rather than treating the findings as isolated descriptive patterns, this section situates them within broader debates in digital government, public administration, and data governance. The scientometric results demonstrate the prominence of cybersecurity- and data security-oriented themes in the literature, as reflected in the high occurrence and connectivity of keywords related to technical protection, cybercrime, and information security. This pattern indicates that data breaches are frequently conceptualized as technical system failures that can be addressed through technological safeguards, such as encryption, malware detection, and network security. It should be emphasized, however, that author keyword co-occurrence analysis reveals patterns of thematic interconnectedness rather than causal relationships. The interpretations that follow are therefore framed as associations supported by the mapping, not as evidence that any one theme causes another.

Table 3

Theoretical Gaps in Studies on Data Breaches in Digital Public Services

Theoretical Aspect	Dominant Focus in Existing Literature	Theoretical Limitations / Gaps	Theoretical Implications	Position of This Study
Cybersecurity	Data breaches are understood primarily as technical issues (cybersecurity, data security, cybercrime).	Technical approaches fail to explain institutional accountability and government organizational responsibility.	Cybersecurity theory needs to be expanded to include governance and public administration perspectives.	Shifts the focus from technical security to the governance of data breaches in digital public services.
Privacy & Data Protection	Privacy and data protection are discussed within general or global regulatory frameworks.	Limited discussion of citizens' privacy as users of digital public services, particularly in developing countries.	Privacy theory needs to be integrated with citizens' rights and public service provision.	Contextualizes privacy theory within the Indonesian digital public service and data governance context.
Public Administration Ethics	Data ethics is discussed in a normative and abstract manner.	Ethics is rarely linked to digital bureaucratic practices and the real consequences of data breaches.	Ethical theory needs to be enriched with the context of data-driven administrative decision-making.	Positions data breaches as an issue of public administration ethics rather than merely technical failure.
Digital Governance	Digital governance is discussed in general terms and separately from data breach issues.	There is no theoretical framework linking government digital transformation with data breach risks.	Digital governance theory needs to incorporate risk and system failure dimensions.	Integrates digital governance and data breaches into a single analytical framework.
Public Trust	Public trust is treated mainly as an outcome variable.	It is rarely analyzed as a direct consequence of data breaches in public services.	A theoretical approach is needed to link data breaches with legitimacy and trust in government.	Analyzes data breaches as a key factor in the erosion of public trust.
Indonesian Context	Global literature dominates the discourse.	Limited studies grounded in Indonesia's institutional regulatory context.	Theory needs to be tested and adapted to developing country contexts.	Provides contextual contributions by examining the relevance of global data breach research to Indonesia's institutional, regulatory, and digital governance context.

Source : Scopus database, authors' analysis

The theoretical gap table above summarizes the main conceptual gaps in the literature on data breaches, particularly in the context of digital public services. In the area of cybersecurity, existing studies tend to frame data breaches primarily as technical problems, emphasizing system vulnerabilities, data protection mechanisms, and cybercrime. Although this approach dominates information security and information systems research, it remains limited in explaining public institutional accountability and the responsibility of government organizations as the primary custodians of citizens' data (Bannister & Connolly, 2015; Donthu et al., 2021; Klarin, 2024). As a result, data breaches are often understood merely as technological failures rather than as governance failures. Therefore, there is a clear need to extend cybersecurity perspectives into governance and public administration frameworks, as this study seeks to do.

In the area of privacy and data protection, existing studies generally operate within global regulatory frameworks and universal normative principles, such as the right to privacy and the protection of personal data. Although these frameworks are important, the literature remains relatively limited in its treatment of citizens' privacy as users of digital public services, particularly in developing countries with diverse levels of institutional capacity and governance arrangements (Masinde et al., 2025). Table 3 highlights the need to integrate privacy theory with concepts of citizens' rights and public service provision. This study addresses that need by contextualizing privacy theory through the examination of data breaches in Indonesia's digital public services.

Furthermore, in the area of public administration ethics, discourse on data ethics tends to remain abstract and normative, focusing on general principles such as fairness, transparency, and responsibility without sufficiently linking them to everyday digital bureaucratic practices. This limitation hinders a deeper understanding of the ethical consequences of data breaches for administrative decision-making and the delivery of digital public services (Floridi et al., 2018; Putra et al., 2025; van den Hoven, 2017). This study addresses this gap by positioning data breaches as an issue of public administration ethics rather than merely as technical failures or cybersecurity incidents. Within the digital governance dimension, the e-government and digital governance literature often discusses government digital transformation in general terms, emphasizing innovation, interoperability, and service performance, while separating these discussions from the risks of data breaches and information security incidents (Janssen & Estevez, 2013; Saydi et al., 2025).

The absence of a theoretical framework that explicitly links government digital transformation with system failures and data risks constitutes a key gap identified in Table 3. This study seeks to integrate digital governance and data breaches into a single, coherent analytical framework by viewing data breaches as outcomes of interactions among technology, organizational practices, and institutional arrangements. In the literature, public trust is generally treated as an outcome variable, with limited in-depth analysis of data breaches as a direct contributor to the erosion of trust and government legitimacy. Yet a growing body of research indicates that government failures to protect citizens' personal data can significantly affect perceptions of institutional legitimacy and public trust in the state (Grimmelikhuijsen et al., 2013; Tai, 2026). Table 3 underscores the need for a theoretical approach that directly links data breaches to public trust and institutional legitimacy, which constitutes a central analytical focus of this study.

Finally, Table 3 highlights the Indonesian context as a significant gap in the global literature, which remains dominated by studies from developed countries. The limited number of studies grounded in the institutional, regulatory, and governance contexts of developing countries constrains the generalizability of existing data breach theories (Janssen & Estevez, 2013; Saydi et al., 2025). By situating the findings within the Indonesian digital public service context, this study provides a contextual contribution and highlights the relevance and limitations of existing data breach theories in a developing-country setting.

Although technical cybersecurity approaches are essential, the concentration of research within technical cybersecurity clusters suggests limited engagement with the institutional and organizational dimensions of data breaches in public sector contexts. In digital public services, where governments are responsible for safeguarding citizens' personal data, technical explanations alone are insufficient to capture the complexity of data breach incidents. The persistence of data breaches despite technological advances suggests that vulnerabilities are

embedded not only in systems but also in governance arrangements, organizational practices, and institutional accountability structures.

The strong connectivity of the privacy, ethics, and data protection cluster indicates that normative concerns about personal data protection have gained prominence in the literature. Much of this work is framed within global regulatory regimes and universal privacy principles, emphasizing compliance, rights-based approaches, and legal safeguards. However, the findings suggest that these discussions often remain detached from the operational realities of digital public services. Citizens are frequently treated as abstract data subjects rather than as users who depend on government services and have limited choice regarding the provision of their personal data. As a result, privacy is discussed more as a regulatory obligation than as a lived governance challenge embedded in public service delivery. This gap limits the ability of existing theories to explain why formal data protection frameworks have not consistently prevented breaches in public sector systems, particularly in developing-country contexts.

The results also show that themes related to digital governance, risk management, and trust appear in secondary, less integrated clusters. Although governance concepts are present, they are not structurally central to the literature. This fragmentation reflects a broader disconnect between digital government studies, which often emphasize innovation, service performance, and platform development, and data breach research, which focuses on security incidents without embedding them in governance frameworks. This separation limits theoretical development by preventing a holistic understanding of data breaches as outcomes of interactions among technology, organizational capacity, and institutional arrangements. In public administration, digital transformation initiatives that prioritize rapid service expansion without parallel investments in governance capacity can inadvertently increase exposure to data breaches. The fragmented structure of the literature thus mirrors the institutional fragmentation often observed in digital government practice.

The discussion of public administration ethics in the literature remains largely normative and abstract, emphasizing general principles such as transparency, responsibility, and fairness. The findings suggest that ethical considerations are rarely connected to routine administrative practices or to the concrete consequences of data breaches for citizens. By contrast, the results of this study support the interpretation of data breaches as ethical governance failures in which the inability to safeguard personal data reflects shortcomings in institutional responsibility, oversight, and decision-making. In digital public services, ethical failure is not limited to the intentional misuse of data but also includes negligence, insufficient safeguards, and weak accountability mechanisms. This perspective extends data ethics beyond abstract norms to the realities of digital bureaucratic operations.

Although public trust appears in the literature as an outcome variable, the results indicate that it is rarely analyzed as a direct consequence of data breaches in public services. This omission is significant because breaches in government-operated systems may have distinct implications for institutional legitimacy compared with similar incidents in the private sector. In public sector contexts, repeated data breaches can undermine citizens' confidence in the state's capacity to manage digital transformation responsibly. The erosion of trust affects not only perceptions of data protection but also citizens' willingness to engage with digital public services more broadly. The limited integration of trust into data breach theory therefore represents a critical gap in understanding the societal consequences of governance failures in digital government.

The geographic distribution of publications highlights a strong concentration of research in developed countries, with limited representation from developing-country contexts. This imbalance constrains the generalizability of existing theories, which are often grounded in institutional environments with relatively mature governance frameworks and digital infrastructure. In countries such as Indonesia, where digital public service expansion may outpace governance capacity, data breaches can reveal structural vulnerabilities related to coordination, regulatory enforcement, and organizational readiness. The findings of this study suggest that theories developed in advanced digital states require contextual adaptation to remain analytically useful in developing-country settings. Incorporating such contexts is therefore essential to advancing a more inclusive and empirically grounded understanding of data breaches in digital

public services.

Taken together, the discussion demonstrates that the literature on data breaches in digital public services remains conceptually fragmented. Technical cybersecurity, privacy regulation, digital governance, ethics, and public trust are often treated as separate analytical domains rather than as interdependent components of a single governance problem. This study contributes to the literature by reframing data breaches as sociotechnical governance failures embedded within digital public administration. By integrating technological vulnerabilities with organizational capacity, regulatory arrangements, ethical responsibility, and societal trust, the discussion advances a more coherent theoretical perspective for explaining why data breaches persist despite technological and regulatory progress.

CONCLUSION

direct response to the research objective, this study identifies three principal patterns in the literature on data breaches in digital public services. First, scholarly output increased substantially after 2018 but remains geographically concentrated in a limited number of countries. Second, the mapped literature is organized into six thematic clusters dominated by cybersecurity and data security, while privacy and data protection demonstrate particularly strong thematic connectivity. Third, governance, risk management, organizational accountability, and public trust remain comparatively less integrated into the technical core of the literature. These findings support the conceptualization of data breaches in digital public services as sociotechnical governance failures involving interactions among technological vulnerabilities, organizational capacity, regulatory arrangements, ethical responsibility, and societal trust. This conceptual synthesis extends data security discussions into digital government and public administration without claiming causal relationships or country-specific empirical validation.

Practically, the findings indicate that responses to public sector data breaches should extend beyond technical safeguards to encompass clearer institutional responsibility, stronger accountability, interagency coordination, and effective data protection governance. These implications are particularly relevant to the Indonesian context, especially in relation to the Personal Data Protection Law and the Electronic-Based Government System (*Sistem Pemerintahan Berbasis Elektronik*, SPBE) policy framework, although this study does not empirically evaluate their effectiveness. The study is limited by its reliance on Scopus-indexed publications, its restriction to English-language and open-access publications, and the distinction between the 1,169-document mapping corpus and the 62-article qualitative synthesis corpus. Future research should empirically examine the proposed sociotechnical governance framework through institutional case studies, comparative research across developed and developing contexts, and studies incorporating the perspectives of public organizations and citizens who use digital public services.

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to Dr. Suswanta, M.Si., for his valuable academic guidance, constructive feedback, and insightful suggestions throughout the development of this study. His guidance contributed to refining the conceptual framework, strengthening the analytical discussion, and improving the overall academic quality of the manuscript.

AUTHOR CONTRIBUTION STATEMENT

Indah Purwaningsih and Dian Eka Rahmawati contributed to the development of this study. Their respective contributions to conceptualization, research methodology, data collection, bibliometric and scientometric analysis, interpretation of findings, manuscript preparation, and substantive revision should be specified according to their actual roles. Both authors should confirm their respective contributions and approve the final manuscript before publication.

REFERENCES

- Abdulkareem, A. K., Abdulkareem, Z. J., Ishola, A. A., & Akindele, I. T. (2022). Does e-government impact e-participation? The influence of trust in e-government. *International Review of Public Administration*, 27(2), 91–110. <https://doi.org/10.1080/12294659.2022.2071540>
- Amin, M. M., Sutrisman, A., Stiawan, D., Alzahrani, M. Y., & Budiarto, R. (2020). Interoperability framework for integrated e-health services. *Bulletin of Electrical Engineering and Informatics*, 9(1), 354–361. <https://doi.org/10.11591/eei.v9i1.1825>
- Anggara, S. M., Hariyanto, A., Arman, A. A., & Kurniawan, N. B. (2024). The Development of Digital Service Transformation Framework for the Public Sector. *IEEE Access*, 12, 146160–146189. <https://doi.org/10.1109/ACCESS.2024.3406571>
- Apostolos, K. (2021). Electronic health records and personal data protection: The legal and sociological approach. *Archives of Hellenic Medicine*, 38(3), 394–400.
- Aria, M., & Cuccurullo, C. (2017). bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of Informetrics*, 11(4), 959–975. <https://doi.org/10.1016/j.joi.2017.08.007>
- Attidhira, S. W., & Permana, Y. S. (2022). Review of Personal Data Protection Legal Regulations in Indonesia. *Awang Long Law Review*, 5(1), 280–294.
- Bannister, F., & Connolly, R. (2015). The great theory hunt: Does e-government really have a problem? *Government Information Quarterly*, 32(1), 112–121. <https://doi.org/10.1016/j.giq.2014.10.003>
- Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). On the Dangers of Stochastic Parrots. *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, 610–623. <https://doi.org/10.1145/3442188.3445922>
- Bucher, T. (2018). *If...Then*. Oxford University Press New York. <https://doi.org/10.1093/oso/9780190493028.001.0001>
- Digay, D., Bochkova, S., Nurbek, D., Khanov, T., Kolganov, S., & Mussekenova, A. (2025). Finding A Balance Between Personal Data Protection And Public Safety In The Age Of Digitalization: International Approaches And Their Adaptation. *Relacoes Internacionais No Mundo Atual*, 4(50), 124–142. <https://doi.org/10.21902/Revrima.v4i50.7787>
- Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. *Journal of Business Research*, 133, 285–296. <https://doi.org/10.1016/j.jbusres.2021.04.070>
- Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival*, 53(1), 23–40. <https://doi.org/10.1080/00396338.2011.555586>
- Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Lütge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. *Minds and Machines*, 28(4), 689–707. <https://doi.org/10.1007/s11023-018-9482-5>
- Fouracres, A. J. (2023). *Handling a data breach out of your control BT - Ethical Case Studies for Coach Development and Practice: A Coach's Companion* (pp. 150–153). Taylor and Francis. <https://doi.org/10.4324/b23351-38>
- Garbaccio, G. L., & Kischelewski, F. L. N. (2024). Governance and best practices at LGPD trough compliance, risk management and accountability. *Revista Brasileira de Estudos Politicos*, 128, 155–195. <https://doi.org/10.9732/2024.V128.894>
- Gillespie, T. (2019). *Custodians of the Internet*. Yale University Press. <https://doi.org/10.12987/9780300235029>
- Goggin, G., Vromen, A., Weatherall, K., Martin, F., & Sunman, L. (2019). Data and digital rights: Recent australian developments. *Internet Policy Review*, 8(1). <https://doi.org/10.14763/2019.1.1390>
- Grimmelikhuijsen, S., Porumbescu, G., Hong, B., & Im, T. (2013). The Effect of Transparency on Trust in Government: A Cross-National Comparative Experiment. *Public Administration Review*, 73(4), 575–586. <https://doi.org/10.1111/puar.12047>
- Heryawan, L., Mori, Y., Yamamoto, G., Kume, N., Lazuardi, L., Fuad, A., & Kuroda, T. (2025). Fast Healthcare Interoperability Resources (FHIR)-Based Interoperability Design in Indonesia: Content Analysis of Developer Hub's Social Networking Service. *JMIR Formative Research*, 9.

- <https://doi.org/10.2196/51270>
- Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2022). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. *Information Systems Frontiers*, 24(2), 393–414. <https://doi.org/10.1007/s10796-020-10044-1>
- Janssen, M., & Estevez, E. (2013). Lean government and platform-based governance—Doing more with less. *Government Information Quarterly*, 30, S1–S8. <https://doi.org/10.1016/j.giq.2012.11.003>
- Jenson, D. (2008). Enterprise data management: Governing for data security. *DB2 Magazine*, 13(1).
- Jones, H. S., Towse, J. N., Race, N., & Harrison, T. (2019). Email fraud: The search for psychological predictors of susceptibility. *PLOS ONE*, 14(1), e0209684. <https://doi.org/10.1371/journal.pone.0209684>
- Katz, J., & Lindell, Y. (2025). *Introduction to Modern Cryptography*. Chapman and Hall/CRC. <https://doi.org/10.1201/9781003398134>
- Kayyali, M. (2025). *Digital transformation in public sector management: An overview BT - Enhancing Public Sector Accountability and Services Through Digital Innovation* (pp. 289–324). IGI Global. <https://doi.org/10.4018/979-8-3693-9251-5.ch009>
- Kietzmann, J. H., Hermkens, K., McCarthy, I. P., & Silvestre, B. S. (2011). Social media? Get serious! Understanding the functional building blocks of social media. *Business Horizons*, 54(3), 241–251. <https://doi.org/10.1016/j.bushor.2011.01.005>
- Kitchenham, B., & Charters, S. (2007). *Guidelines for performing Systematic Literature Reviews in Software Engineering* (Number 2).
- Klarin, A. (2024). How to conduct a bibliometric content analysis: Guidelines and contributions of content co-occurrence or co-word literature reviews. *International Journal of Consumer Studies*, 48(2), e13031.
- Kumar, S., & Singh, V. (2021). *Information hiding techniques for cryptography and steganography BT - Advances in Intelligent Systems and Computing* (Vol. 1257, pp. 511–527). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-981-15-7907-3_39
- Lallie, H. S., Thompson, A., Titis, E., & Stephens, P. (2025). Analysing cyber attacks and cyber security vulnerabilities in the university sector. *Computers*, 14(2), 49.
- LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, 521(7553), 436–444. <https://doi.org/10.1038/nature14539>
- Liu, B., Zhou, C. J., Ma, H. W., & Gong, B. (2023). Mapping the youth soccer: A bibliometrix analysis using R-tool. In *Digital Health* (Vol. 9). <https://doi.org/10.1177/20552076231183550>
- Lodge, M., & Wegrich, K. (2014). *The Problem-Solving Capacity of the Modern State: Governance Challenges and Administrative Capacities*. Oxford University Press.
- Malatji, M., Marnewick, A. L., & von Solms, S. (2021). Cybersecurity policy and the legislative context of the water and wastewater sector in South Africa. *Sustainability (Switzerland)*, 13(1), 1–33. <https://doi.org/10.3390/su13010291>
- Malatras, A., Sánchez, I., Beslay, L., Coisel, I., Vakalis, I., D'Acquisto, G., Sanchez, M. G., Grall, M., Hansen, M., & Zorkadis, V. (2017). Pan-European personal data breaches: Mapping of current practices and recommendations to facilitate cooperation among Data Protection Authorities. *Computer Law and Security Review*, 33(4), 458–469. <https://doi.org/10.1016/j.clsr.2017.03.013>
- Masinde, J., Mugambi, F., & Muthee, D. W. (2025). Big data and personal information privacy in developing countries: Insights from Kenya. *Frontiers in Big Data*, 8, 1532362. <https://doi.org/10.3389/fdata.2025.1532362>
- Mazzucato, M., & Kattel, R. (2026). *Market-Shaping States: A new theory of public sector capacities and capabilities*.
- McAllister, J. T., Lennertz, L., & Atencio Mojica, Z. (2022). Mapping a discipline: a guide to using VOSviewer for bibliometric and visual analysis. *Science & Technology Libraries*, 41(3), 319–348.
- Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *Open Medicine*, 3, e123-30.

- <https://doi.org/10.1016/j.jclinepi.2009.06.005>
- Moutamir, H., & El Qour, T. (2025). Digital Transformation Of Public Services Systematic Review Of Key Success Factors. *Journal of Theoretical and Applied Information Technology*, 103(15), 5895–5912.
- Ogut, H., El Archi, Y., & Dávid, L. D. (2023). Current trends in sustainable organization management: A bibliometric analysis. *Oeconomia Copernicana*, 14(1), 11–45.
- Oroni, C. Z., & Fu, F. (2025). Evaluating the influence of cybersecurity policies and cybersecurity behavior on institutional security performance in remote learning: the moderating role of technological readiness. *Sustainable Futures*, 10. <https://doi.org/10.1016/j.sfr.2025.101554>
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., & Brennan, S. E. (2022). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *Revista Panamericana de Salud Publica*, 46, e112.
- Pavlou. (2003). Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. *International Journal of Electronic Commerce*, 7(3), 101–134. <https://doi.org/10.1080/10864415.2003.11044275>
- Putra, A. A., Pambudi, R., & Sulistiani, H. (2025). The ethical principles and regulatory frameworks that shape the global landscape of artificial intelligence (AI), situating the analysis within the context of leading international efforts to study and govern AI ethics. *Proceeding of International Conference on Islamic Education (ICIED)*, 10(1), 53–59.
- Rahman, F. (2025). Safeguarding Personal Data In The Public Sector: Unveiling The Impact Of The New Personal Data Protection Act In Indonesia. *UUM Journal of Legal Studies*, 16(1), 1–18. <https://doi.org/10.32890/uumjls2025.16.1.1>
- Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, tyw001. <https://doi.org/10.1093/cybsec/tyw001>
- Saydi, F., Mousakhani, M., Tootian Esfahani, S., & Tayaran, S. (2025). Designing and validating the lean governance model in government governance. *Public Management Researches*, 18(69), 351–385.
- Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, 124, 102974. <https://doi.org/10.1016/j.cose.2022.102974>
- Shao, Y., & Shi, X. (2023). Bibliometric analysis and visualization of research progress in the diabetic nephropathy field from 2001 to 2021. *Oxidative Medicine and Cellular Longevity*, 2023(1), 4555609.
- Shokri, R., Stronati, M., Song, C., & Shmatikov, V. (2017). Membership Inference Attacks Against Machine Learning Models. *2017 IEEE Symposium on Security and Privacy (SP)*, 3–18. <https://doi.org/10.1109/SP.2017.41>
- Sleem, A. (2022). A Comprehensive Study of Cybersecurity Threats and Countermeasures: Strategies for Mitigating Risks in the Digital Age. *Journal of Cybersecurity and Information Management*, 10(2), 35–46. <https://doi.org/10.54216/JCIM.100204>
- Sonia Dewi, P. P., Lubis, M., & Abdurrahman, L. (2024). *Aligning Healthcare Strategies Through Digital Information and Technology: Challenges and Solution BT - 2024 12th International Conference on Cyber and IT Service Management (CITSM)*. <https://doi.org/10.1109/CITSM64103.2024.10775893>
- Syifa, S. N., Abdillah, M. T., & Fadil, S. J. (2025). The Legal Responsibility of the General Elections Commission in the 2024 Election Data Leak: Integration of Personal Data Protection Laws and the Principle of Sadd al-Dharī'at. *Justicia Islamica*, 22(1), 185–210. <https://doi.org/10.21154/justicia.v22i1.10390>
- Tai, Y. C. (2026). Introducing the trust in government (TrustGov) dataset: A new resource for cross-national time-series trust research. *Research & Politics*, 13(1), 20531680261432468.
- Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law and Security Review*, 34(1), 134–153. <https://doi.org/10.1016/j.clsr.2017.05.015>
- Tripathi, A., & Behl, T. (2020). Protecting The Health Data Of Consumers: Need For An Iron-Clad

- Law In India. *International Journal on Consumer Law and Practice*, 8, 105–117.
- van den Hoven, J. (2017). *Ethics for the Digital Age: Where Are the Moral Specs? BT - Ethics and Law of Intellectual Property* (pp. 65–76). https://doi.org/10.1007/978-3-319-55735-9_6
- van Eck, N. J., & Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics*, 84(2), 523–538. <https://doi.org/10.1007/s11192-009-0146-3>
- van Eck, N. J., & Waltman, L. (2014). *Visualizing Bibliometric Networks BT - Measuring Scholarly Impact: Methods and Practice* (Y. Ding, R. Rousseau, & D. Wolfram, Eds.; pp. 285–320). Springer International Publishing. https://doi.org/10.1007/978-3-319-10377-8_13
- van Loon, A., & Toshkov, D. (2015). Adopting open source software in public administration: The importance of boundary spanners and political commitment. *Government Information Quarterly*, 32(2), 207–215. <https://doi.org/10.1016/j.giq.2015.01.004>
- Vatamanu, A. F., & Tofan, M. (2025). Integrating artificial intelligence into public administration: Challenges and vulnerabilities. *Administrative Sciences*, 15(4), 149.
- Verkijika, S. F. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers & Security*, 77, 860–870. <https://doi.org/10.1016/j.cose.2018.03.008>
- Wirtz, B., & Müller, W. (2018). An integrated artificial intelligence framework for public management. *Public Management Review*, 21, 1–25. <https://doi.org/10.1080/14719037.2018.1549268>
- Wong, Y. Q. (2017). Data privacy law in Singapore: The Personal Data Protection Act 2012. *International Data Privacy Law*, 7(4), 287–302. <https://doi.org/10.1093/idpl/ix016>
- Zakiuddin, N. F., & Anggara, S. M. (2024). Developing Digital Service Transformation Maturity Model in Public Sector. *IEEE Access*, 12, 174491–174506. <https://doi.org/10.1109/ACCESS.2024.3468341>
- Zupic, I., & Čater, T. (2015). Bibliometric methods in management and organization. *Organizational Research Methods*, 18, 429–472. <https://doi.org/10.1177/1094428114562629>