IJITEB
Vol. 8
No. 1
2025

International Journal of Information Technology and Business

http://ejournal.uksw.edu/ijiteb



Privacy Protection and Trust in the Digital Era: A Systematic Review of Data Breach Impacts on SDG Progress

Toni Wijanarko Adi Putra[1*], Danang[2]
[1-2]Universitas Sains dan Teknologi Komputer, Indonesia

Abstract: Objective – In the digital transformation era, the integrity of personal data has become essential for maintaining trust and ensuring the sustainability of digital services. This paper aims to systematically review how data privacy violations affect public trust and progress toward Sustainable Development Goals (SDGs), especially SDG 9 (infrastructure and innovation) and SDG 16 (strong institutions and justice).
Methodology – This study adopts the Systematic Literature Review (SLR) approach based on Kitchenham's framework. Relevant articles from 2021–2025 were retrieved from Scopus, IEEE, Springer, and ScienceDirect using a predefined search string aligned with PICOC. A total of 19,504 records were screened, and 36 high-quality studies were selected after applying inclusion/exclusion criteria and quality assessment tools (e.g., CASP, AMSTAR).
Findings – The review reveals that sectors such as education, healthcare, and smart cities are increasingly adopting data protection technologies including encryption, federated learning, differential privacy, and blockchain. However, many still face regulatory, infrastructural, and human literacy gaps. Breaches in personal data significantly reduce public trust, impair the exercise of digital rights, and pose ethical and operational risks for achieving SDGs.
Limitations – The study is limited by the timeframe (2021–2025) and focuses primarily on peer-reviewed literature. Practical insights from developing countries may be underrepresented due to database indexing limitations.
Contribution – This review contributes a cross-sectoral synthesis of technological and regulatory practices for data protection, identifies key challenges, and outlines a strategic roadmap for policymakers and technologists to integrate ethical data governance for sustainable digital futures.

Keywords: Data Privacy, Digital Trust, Sustainable Development Goals (SDGs), Systematic Literature Review, Cybersecurity Governance

1. Introduction

In the era of increasingly rapid digital transformation, personal data has become a strategic asset that is widely utilized in various sectors of life [1]. In the world of education, data such as student academic achievement and teacher evaluations are not only assessment tools, but also the foundation for improving the quality of education and building a collaborative culture through co-creation involving all stakeholders [2]. A similar role is also seen in the health sector, where personal information is a major pillar in the process of diagnosis, treatment, and medical research [4]. The government has also adopted a similar approach in developing smart cities that integrate cross-sector data to improve public services holistically [5].
Not to be left behind, the industrial sector is utilizing data through Internet of Things (IoT) technology, by processing various data formats to automatically control systems and improve operational efficiency [3]. However, along with the widespread use of personal data, serious concerns have arisen regarding security and privacy [6]. The rise in data breaches and non-transparent information collection practices reveal the weakness of the existing protection system, both in terms of regulation, technology, and individual awareness [7].
Personal data protection is a human right recognized by the constitution and international law [8]. Therefore, systematic efforts are needed through policies such as the General Data Protection Regulation (GDPR) and the Privacy by Design approach so that digital systems are designed from the start with ethical and security principles. In this context, research on data protection is becoming increasingly important, because data is no longer just a passive archive, but has become the main basis for public policy and technological innovation [9].
The fact that individuals consciously or unconsciously continue to share data through educational applications, digital health services, online government systems, and IoT devices, shows the high dependence on the digital ecosystem [3]. When the protection

* Corresponding authors

e-mail addresses : toni.wijanarko@stekom.ac.id

system is inadequate, the risk of misuse increases. Various cases of data leaks at the global level show that this vulnerability is not only technical, but also reflects weak regulations and low public literacy—especially in developing countries like Indonesia before the enactment of Law No. 27 of 2022 [10].

The urgency of this research is further strengthened when linked to the Sustainable Development Goals (SDGs), especially SDG 16 which emphasizes the importance of accountable institutions and SDG 9 which encourages safe and inclusive digital infrastructure. Without reliable data protection, public trust in technology will decline, and fair and sustainable digital transformation will be difficult to achieve [11].

Thus, this research has significance not only in strengthening the legal and technical aspects of personal data protection, but also in shaping the digital literacy culture of society. This is an important first step in building an ethical, safe, and equitable digital ecosystem for all parties.

2. Methods

This study uses the Systematic Literature Review (SLR) approach as guided by Kitchenham [12], to ensure that the process of collecting and analyzing literature is carried out systematically, structured, and accountable. The selection of this method is based on the need to obtain a deep and comprehensive understanding of the topic being studied.

The SLR stages begin with the planning phase, where researchers first examine the urgency of conducting a literature review. At this stage, research questions are formulated clearly, accompanied by the preparation of work procedures that will serve as guidelines for implementing the study.

Next, the research enters the implementation phase, which includes the process of searching, selecting, and analyzing relevant scientific articles. Of the many publications found, only sources that meet the criteria for quality and topic relevance are selected. Each article is then reviewed in depth to identify important information, find patterns, and compile a synthesis that answers the research questions.

Finally, the results of the entire process are summarized in the reporting phase, with the aim of presenting findings in a concise and easy-to-understand manner. This report is expected to be not only useful for academics, but also to be a valuable reference for policy makers and the wider community, so that the research results can provide real contributions to the development of science and practice in the field.

3. Research Question

Research questions are a key element in any systematic review, as they form the basis for formulating the focus of the review and the direction of the analysis. In this study, the process of formulating research questions follows the approach of Kitchenham [12], which emphasizes the importance of a strong methodological structure to produce a comprehensive and meaningful literature review.

One of the methods used to formulate research questions is the PICOC framework—namely Population, Intervention, Comparison, Outcome, and Context. This framework helps to clearly identify the scope of the study. In the context of this study, Population refers to digital systems that manage personal data (such as educational platforms, digital health services, and industrial IoT). Intervention includes data protection policies and technologies such as GDPR, the Privacy by Design principle, and encryption. Comparison compares systems that have not adopted maximum data protection. The outcomes include increased data security, public trust, legal compliance, and contributions to achieving the SDGs. Meanwhile, the Context is the era of digital transformation with massive online data exchange in various sectors.

Based on the PICOC analysis, three main research questions were formulated. First (RQ1), how do digital sectors such as education, health, and government implement the principle of personal data protection amidst digital transformation. Second (RQ2), what technologies and ethical approaches are most widely used to maintain data privacy, and how effective is their implementation at the global and national levels. Third (RQ3), what impact does a personal data breach have on public trust, individual digital rights, and the achievement of the Sustainable Development Goals (SDGs).

4. Search Strategy

To answer the research questions in depth, the literature search process was carried out systematically and comprehensively, with the aim of identifying relevant, reliable, and up-to-date scientific publications. The search focused on highly reputable journals indexed in databases such as Scopus, IEEE Xplore, SpringerLink, and ScienceDirect, to ensure the validity and quality of the sources used.

The initial stage began with the formulation of a search string based on the PICOC elements (Population, Intervention, Comparison, Outcome, Context), which reflect the core of the research study. The keywords used include terms such as "data protection", "privacy", "personal data", "digital transformation", to "Privacy by Design". To ensure completeness of coverage, Boolean operators such as AND, OR, and NOT were used carefully so that the search results were right on target.

One example of a search string used is: ("personal data" OR "data privacy" OR "data protection") AND ("digital transformation" OR "smart city" OR "IoT") AND ("regulation" OR "governance" OR "privacy law" OR "GDPR"). The search string was designed to cover a wide range of data protection topic combinations in the context of digital transformation and regulatory governance.

Inclusion and exclusion criteria were then set to filter the most relevant articles. Only publications within the last five years (2021–2025) and in English were

considered. Articles that did not directly address the context of personal data protection, or were merely opinions without empirical support, were excluded from the selection process.

More than just a technical process, this literature search was also conducted with a reflective and critical approach. Each publication was reviewed not only from a technical and legal perspective, but also from a social and ethical perspective. With this approach, the search process became an integral part of a contextual and nuanced scientific exploration, enriching the understanding of the dynamics of personal data protection in various sectors.

5. Study Selection Criteria

After the initial search process yields a large number of publications, the screening and selection phase of studies is a crucial step to ensure that only the most relevant and high-quality literature is analyzed. This process is carried out carefully by combining an objective approach and a contextual understanding of the issue of personal data protection in the digital era.

To that end, strict selection criteria were applied. Only articles that explicitly discuss personal data protection, digital privacy, or data regulation in the context of digital transformation, smart cities, IoT, and modern information systems were included in the review. This focus is important to capture the actual dynamics that are developing amidst the flow of global digitalization.

The selected literature comes from highly reputable journals such as Scopus, IEEE, Springer, Elsevier, and ACM, and was published in the last five years (2021–2025) and in English. We prioritize studies that present in-depth and relevant empirical findings, systematic reviews, or conceptual frameworks.

Conversely, publications that are only opinions, do not focus on the issue of personal data protection, are duplicates, or are not fully available are excluded from the review. This selective approach is taken to maintain the accuracy, integrity, and depth of analysis in compiling the literature review.

The selection process is carried out in stages—starting with an initial evaluation through the title and abstract, then continuing with a thorough review of the contents of the article (full-text review). The assessment is carried out by two researchers independently to ensure objectivity, and any differences of opinion are resolved through open discussion.

With this rigorous and transparent approach, we not only ensure the validity of the results but also demonstrate a commitment to scientific quality. The results are expected to provide a sharp, reflective, and meaningful understanding of the challenges and opportunities in personal data protection amidst the ever-growing digital transformation.

6. Quality Assessment

After the relevant studies have been successfully selected, the next stage is to systematically and in-depth assess the quality of the publications. This step is important to ensure that only truly credible and methodologically sound literature is used as the basis for the analysis. The assessment is carried out not only based on the reputation of the journal or indexing, but also by examining the structure of the study, the appropriateness of the methodological approach, and the clarity in presenting the results and discussion.

To guide this process, quality assessment instruments such as the Critical Appraisal Skills Programme (CASP) and AMSTAR are used as references, with adjustments to the context of the study of personal data protection. This approach provides a systematic framework for assessing the scientific value of an article fairly and comprehensively.

Each publication is assessed based on five main criteria. First, clarity of research objectives, namely the extent to which the article formulates explicit objectives that are relevant to the issue of personal data protection. Second, the appropriateness of the methodology, which assesses whether the approach used is able to answer the research questions appropriately and in a structured manner. Third, the credibility of the data source, which emphasizes the importance of using valid and verifiable references or data.

The fourth criterion is the strength of the analysis and argumentation, namely the extent to which the research results are critically reviewed and logically connected to previous findings. Finally, openness to limitations is also assessed, which reflects the reflective quality of the author in recognizing the limitations of his study and suggesting directions for further research. Through this assessment process, the literature review does not only become a collection of references, but develops into a solid and responsible foundation for understanding the issue of personal data protection scientifically and contextually.

Each article that passed the initial selection was then assessed using a simple quality scale, namely a score of 1 for low, 2 for medium, and 3 for high. The assessment was carried out by two researchers independently to maintain objectivity. If there were differences in scores, an open discussion was held until a mutual agreement was reached.

This assessment process was designed not only to be methodologically rigorous, but also to remain fair and respectful of the context of the research being analyzed. The goal was to ensure that only relevant, reliable literature that has meaningful scientific contributions was used in this study. This approach helps build a strong foundation for analysis of personal data protection issues in the digital era.

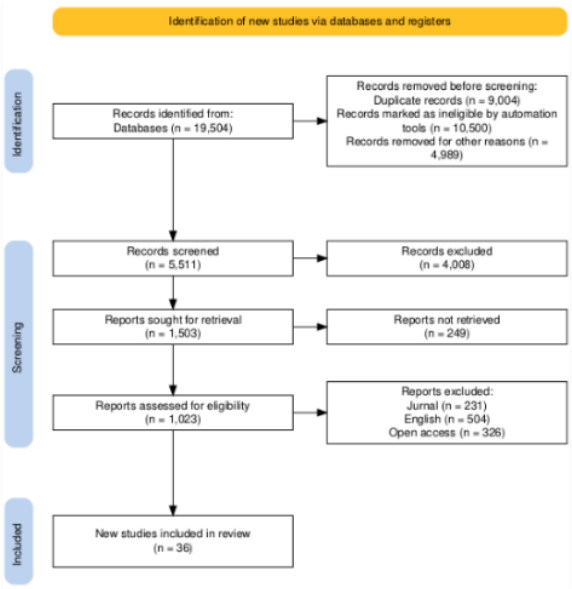


Figure 1. Selection process diagram based on the PRISMA flow diagram

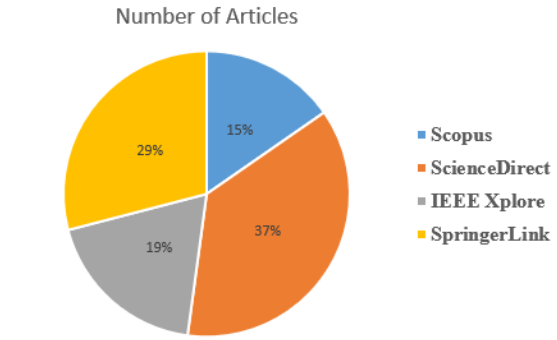


Figure 2. Distribution of articles retrieved per source

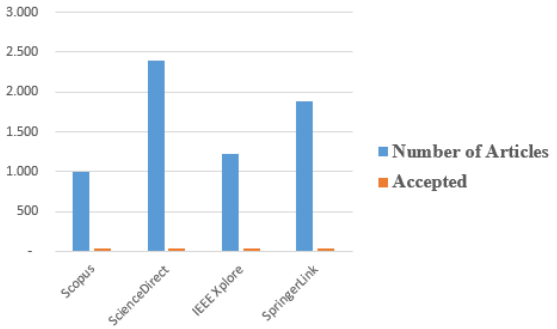


Figure 3. Accepted articles based on sources

Each article that passed the initial selection was then assessed using a simple quality scale, namely a score of 1 for low, 2 for medium, and 3 for high. The assessment was carried out by two researchers independently to maintain objectivity. If there were differences in scores, an open discussion was held until a mutual agreement was reached.

This assessment process was designed not only to be methodologically rigorous, but also to remain fair and respectful of the context of the research being analyzed. The aim was to ensure that only relevant, reliable literature with meaningful scientific contributions was used in this review. This approach helped build a strong foundation for analysis of the issue of personal data protection in the digital era.

Of the total 19,504 articles searched, only 36 studies met all quality criteria. Most of them came from highly reputable journals, namely 24 from Q1 journals, 7 from Q2, 2 from Q3, and 3 from Q4. Full details of the list of articles can be found in Table 3, while the distribution of years is presented visually in Figure 4.

Table 3. Publication categories

No	Kategori Publikasi	Qty
1	Q1	24
2	Q2	7
3	Q3	2
4	Q4	3

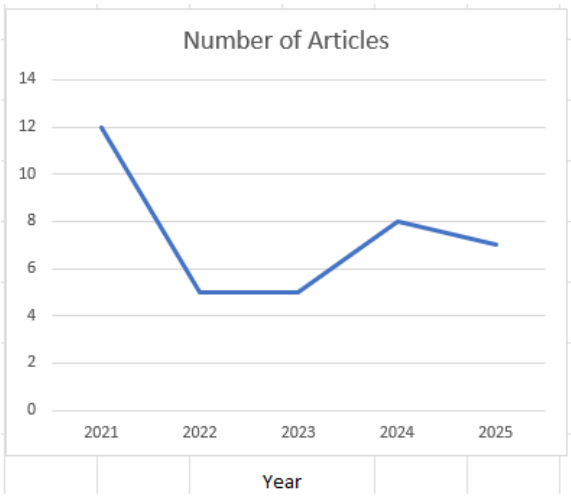


Figure 4. Final articles per year (After study selection and quality assessment).

7. Data Extraction

After the articles have gone through the selection and quality assessment process, the next stage is data extraction, which is an important foundation in constructing research analysis and synthesis. This process aims to extract key information from each selected study and organize it in a structured format for easy comparative and thematic review.

The extraction was carried out carefully and with great care, such as assembling pieces of information into a complete picture of the dynamics of personal data protection—both in terms of practices, challenges, and policies that apply in various sectors and countries.

Each article was analyzed using a systematically compiled data extraction form, covering a number of key components relevant to the focus of the study. These components include:

1. Study Identity: recording the title, author, year, journal, and institutional affiliation.
2. Research Objectives: the main focus of the study, whether related to policy, technology, user awareness, or a multidisciplinary approach.

3. Study Context and Area: location and sector of the study, such as education, health, government, or industry.
4. Research Methodology: type of approach (qualitative, quantitative, mixed), data collection techniques, and analysis methods.
5. Main Findings: summary of the study results, including successes, challenges, and recommendations related to data protection.
6. Legal and Regulatory Aspects: references to policies such as GDPR, the Indonesian PDP Law, or the Privacy by Design principle.
7. Contribution to SDGs: the relevance of the study results to sustainable development goals, especially in terms of equity, institutional governance, and sustainable technology.
8. Study Limitations: authors' acknowledgement of the limitations of the study and their impact on the interpretation of the results.

By using this extraction framework, the analysis process not only becomes more systematic, but also more reflective and meaningful, enabling a comprehensive understanding of personal data protection issues in the digital era.

8. Result And Discussion

After a systematic data extraction process, a number of important findings were obtained that describe the state of personal data protection in the digital era from various sectors, regions, and methodological approaches. These findings not only provide factual information, but also open up space for reflection on the real dynamics and challenges in the field.

RQ1: Digital transformation encourages sectors such as education, health, and government to adopt data protection policies and technologies. However, the level of readiness and success varies greatly, depending on infrastructure, regulations, and user digital literacy [13]. In the education sector, student data is now a strategic element in learning management. Although principles such as data minimization and consent-based access are starting to be applied, the understanding of teachers, parents, and students is still limited, resulting in privacy vulnerabilities [15].

Technologies such as encryption and access control have been used to keep data secure, but the challenges are not just technical. Lack of digital literacy is a major barrier to understanding complex privacy policies. On the other hand, educational approaches such as training and awareness raising are considered crucial to support the success of data protection systems in educational settings.

In the healthcare sector, patient personal data is categorized as highly sensitive data because it concerns medical conditions, disease history, and even genetic information. Regulations such as GDPR [16][17][18][19] and HIPAA have set strict limitations on the processing of this data [9]. Although developed countries have developed a well-established legal system and security infrastructure, developing countries still face major challenges—from the absence of clear privacy policies, budget constraints, to low awareness of medical personnel regarding the importance of data protection [8].

The digitalization of public services also has a major impact on data management in the government sector and smart cities [29]. Technologies such as IoT and big data do improve the efficiency and quality of services, but they also present significant privacy risks. Therefore, the government needs to promote a strong policy framework, such as the principle of privacy by design, and build a transparent, accountable, and inclusive information system.

The findings also show that interoperability and coordination between institutions remain critical challenges [20]. The misalignment of technology and legal standards hampers the effectiveness of data protection, especially in the context of smart cities and digital health services. An adaptive national cybersecurity system, independent oversight institutions, and synergy between stakeholders are needed to maintain public trust.

Although regulations such as GDPR have been implemented in many countries, the gap between policy, implementation, and privacy culture is still evident. Many people do not understand how their data is used, do not read privacy policies thoroughly, and do not have full control over data use consent [9][7][17]. This shows that data protection is not enough with regulation alone, but also requires a holistic approach that includes education, transparency, and public participation [26].

After going through a thorough data extraction process, we managed to identify several important findings that reflect the state of personal data protection in the digital era from various perspectives, geographical contexts, and research approaches. These findings not only provide a factual picture, but also open up space for reflection on the dynamics, challenges, and opportunities that are developing.

RQ2: What are the most widely used technologies and ethical approaches to safeguard personal data security and privacy, and how effective are they at the global and national levels?

This systematic review identified that two main approaches dominate efforts to protect personal data, namely through digital security technologies and regulatory-based ethical frameworks [28][19][25][26][20][14]. These two approaches complement each other in creating a safe, transparent and accountable system.

From a technological perspective, various innovations have been implemented to maintain data integrity, confidentiality, and authentication. The most common methods include:

1. End-to-end encryption and homomorphic encryption, which maintain the confidentiality of digital communications, including in cloud and IoT systems [5] [16] [25] [29] [30] [31] [32].
2. Blockchain, which is used to ensure the immutability and transparency of medical, educational, and smart city data through

cryptographic-based logging [16] [21] [24] [29] [33].
3. Multi-Factor Authentication (MFA) and biometric verification, such as fingerprints, which increase the security of user identities [14].
4. Federated Learning (FL) and Differential Privacy (DP), which allow data processing without the need to move the data from its original source, particularly relevant in the education and healthcare sectors [16] [18] [21].

However, the effectiveness of technology is highly dependent on human resource support and regulatory alignment [15]. Advanced encryption technology, for example, will not be effective if users do not understand the importance of safeguarding credentials. Even in healthcare institutions, poor use of electronic medical record systems or staff non-compliance with security policies can lead to data leaks.

To address the complexity of these challenges, ethical and legal frameworks are key pillars. The Privacy by Design (PbD) principle has been widely adopted globally, emphasizing that privacy protection should be built in early in the system development process [9]. Policies such as the GDPR in Europe have become international standards, setting out important principles such as legality, data minimization, and individual rights over their personal data [33].

However, in many countries, including at the national level, the implementation of policies such as GDPR still faces various obstacles. Low digital literacy, limited technological infrastructure, and weak law enforcement are significant obstacles [15]. In some areas, people do not understand the risks of data sharing, and the IoT devices used are often unable to run complex security algorithms. Regulatory inconsistencies also make it difficult to interoperate data across systems and countries.

This means that personal data protection cannot be left solely to technology. A holistic approach is needed that combines digital innovation with public literacy, ethical awareness, and regulatory enforcement [18]. In the context of smart cities, for example, massive data collection must be accompanied by clear policies, transparency of data use, and citizen involvement in the decision-making process.

Finally, the study emphasizes that ethical and transparent data governance is an important foundation for successful digital transformation. In various studies, the role of government, user involvement, and the development of fair security standards are key to creating a trustworthy digital ecosystem. Thus, technology and ethics must go hand in hand in maintaining people's privacy rights in the digital era.

RQ3: What impact do personal data breaches have on public trust, individual digital rights, and the achievement of sustainable development goals (SDGs)?

Personal data breaches not only harm the individuals directly affected, but also erode public trust in digital systems and service providers [17][15][8][34][5][32][9][28][22][26][13]. This is most visible in the healthcare sector, where leaks of medical information have caused people to fear and hesitate to share their data even for essential public services. In this situation, a sense of digital security becomes a key requirement to encourage active citizen participation in the digital ecosystem [15][22][26].

Another equally serious impact is on individual digital rights, such as the right to privacy, control over personal data, and the right to be forgotten [17][9][19]. Studies show that even in systems that use encryption or differential privacy, personal information can still be identified by combining data from various sources [16][17]. Regulations such as GDPR exist to protect these rights, but their implementation still faces challenges in a complex and cross-border digital environment.

Furthermore, data breaches can have implications for personal and social security, including the risk of fraud, discrimination, or algorithmic bias in artificial intelligence (AI) systems [15][34][4][26][14]. In an increasingly digital context, small errors in data management can have serious consequences for individuals and vulnerable groups.

Data breaches also have major implications for achieving the Sustainable Development Goals (SDGs). For SDG 9 (Industry, Innovation and Infrastructure), failure to safeguard digital infrastructure can hinder the progress of smart cities and technology-based services due to loss of user trust [4][5].

For SDG 16 (Strong and Transparent Institutions), data breaches reflect weak governance and oversight, increasing the risk of manipulation and misuse of information [15][17][22][5] [33][28][19][25][7][14].

Meanwhile, in SDG 17 (Global Partnership), the success of collaboration across institutions and countries depends heavily on trust in data management [17][16]. Frameworks such as the Data Privacy Framework (DPF) and Data Transfer Agreement (DTA) are needed to maintain privacy in cross-border data exchanges [28][19][3][2][20].

Thus, data protection is not just a technical or legal issue, but also an issue of ethics, sustainability, and social justice. The application of the Privacy by Design principle, regular audits, public data literacy, and ethical AI governance are key elements to building an inclusive, safe, and responsible digital ecosystem. These efforts will strengthen public trust and ensure that technology plays a role in supporting, rather than threatening, the future of sustainable development.

9. Conclusion

Amidst the rapid flow of digital transformation that has changed almost all aspects of human life, personal data protection has emerged as a crucial issue that can no longer be ignored. Personal data is not just technical information, but a representation of an individual's identity, rights, and freedoms. Therefore, protecting data means protecting human dignity in the digital era.

Through this systematic review, we found that although many efforts have been made to strengthen data security regulations and technologies, fundamental challenges still remain. The imbalance

between technological progress and ethical awareness, the inequality of policy implementation between countries, and the low digital literacy of the community are real obstacles in creating a safe and fair digital ecosystem.

The studies analyzed also underline that data protection not only impacts individuals, but is also closely related to achieving global goals such as social justice, public trust, and the sustainability of digital systems. In other words, building strong personal data protection is part of building an inclusive and civilized future.

Therefore, cross-sector synergy is needed: the active role of the government in regulation and law enforcement, the commitment of the industrial world in implementing the Privacy by Design principle, the contribution of academics in research and education, and public awareness in understanding and demanding their privacy rights.

This study is not an end in itself, but an invitation to continue developing a more holistic and humane approach to understanding and fighting for the protection of personal data. Because ultimately, the digital future we build today will reflect the values we hold together: trust, responsibility, and humanity.

10. References

[1] C. Calculli, A. M. D'Uggento, A. Labarile, and N. Ribecco, "Evaluating people's awareness about climate changes and environmental issues: A case study," J Clean Prod, vol. 324, Nov. 2021, doi: 10.1016/j.jclepro.2021.129244.

[2] M. Zingmark and S. Iwarsson, "Case study on challenges in research with public partners: A personal data incident during recruitment for a survey study on ageing and housing," BMC Res Notes, vol. 18, no. 1, p. 173, Apr. 2025, doi: 10.1186/s13104-025-07246-8.

[3] C. Song, L. Chen, X. Wu, and Y. Li, "A Secure Data Sharing Model Utilizing Attribute-Based Signcryption in Blockchain Technology," Sensors, vol. 25, no. 1, Jan. 2025, doi: 10.3390/s25010160.

[4] L. Xia, D. T. Semirumi, and R. Rezaei, "A thorough examination of smart city applications: Exploring challenges and solutions throughout the life cycle with emphasis on safeguarding citizen privacy," Sustain Cities Soc, vol. 98, Nov. 2023, doi: 10.1016/j.scs.2023.104771.

[5] J. Cha, S. K. Singh, T. W. Kim, and J. H. Park, "Blockchain-empowered cloud architecture based on secret sharing for smart city," Journal of Information Security and Applications, vol. 57, Mar. 2021, doi: 10.1016/j.jisa.2020.102686.

[6] J. Yu, H. Xue, B. Liu, Y. Wang, S. Zhu, and M. Ding, "Gan-based differential private image privacy protection framework for the internet of multimedia things," Sensors (Switzerland), vol. 21, no. 1, pp. 1–21, Jan. 2021, doi: 10.3390/s21010058.

[7] N. Farag, A. Noë, D. Patrinos, and M. H. Zawati, "Mapping the Apps: Ethical and Legal Issues with Crowdsourced Smartphone Data using mHealth Applications," Asian Bioeth Rev, vol. 16, no. 3, pp. 437–470, Jul. 2024, doi: 10.1007/s41649-024-00296-3.

[8] M. Yang, T. Guo, T. Zhu, I. Tjuawinata, J. Zhao, and K. Y. Lam, "Local differential privacy and its applications: A comprehensive survey," Apr. 01, 2024, Elsevier B.V. doi: 10.1016/j.csi.2023.103827.

[9] A. Aljeraisy, M. Barati, O. Rana, and C. Perera, "Privacy Laws and Privacy by Design Schemes for the Internet of Things: A Developer's Perspective," Jun. 30, 2021, Association for Computing Machinery. doi: 10.1145/3450965.

[10] V. Yunanda, I. G. A. Wiranata, Y. Agustin, R. Rohaini, and A. Zazili, "The Urgency of Establishing LPPDP as an Effort to Strengthen Personal Data Protection: A Comparison between Indonesia, Hong Kong and Singapore," Jurnal Ilmiah Hukum dan Hak Asasi Manusia, vol. 4, no. 1, pp. 11–25, Jul. 2024, doi: 10.35912/jihham.v4i1.2962.

[11] Y. Wanasiri, S. Tinggi, and M. Ppm, "Analysis of NIK Data Breaches and Their Implications for Achieving the SDGs in Indonesia: A Case Study and Policy Recommendations," Records Management System Journal (RMSJ), vol. 03, no. 02, pp. 11–19, 2025.

[12] B. Kitchenham and P. Brereton, "A systematic review of systematic review process research in software engineering," 2013, Elsevier B.V. doi: 10.1016/j.infsof.2013.07.010.

[13] I. van Ooijen, C. M. Segijn, and S. J. Opree, "Privacy Cynicism and its Role in Privacy Decision-Making," Communic Res, vol. 51, no. 2, pp. 146–177, Mar. 2024, doi: 10.1177/00936502211060984.

[14] R. R. Krishna, A. Priyadarshini, A. V. Jha, B. Appasani, A. Srinivasulu, and N. Bizon, "State-of-the-art review on IoT threats and attacks: Taxonomy, challenges and solutions," Aug. 02, 2021, MDPI. doi: 10.3390/su13169463.

[15] J. Pool, S. Akhlaghpour, F. Fatehi, and A. Burton-Jones, "A systematic analysis of failures in protecting personal health data: A scoping review," Feb. 01, 2024, Elsevier Ltd. doi: 10.1016/j.ijinfomgt.2023.102719.

[16] R. Al-Huthaifi, T. Li, W. Huang, J. Gu, and C. Li, "Federated learning in smart cities: Privacy and security survey," Inf Sci (N Y), vol. 632, pp. 833–857, Jun. 2023, doi: 10.1016/j.ins.2023.03.033.

[17] N. Truong, K. Sun, S. Wang, F. Guitton, and Y. K. Guo, "Privacy preservation in federated learning: An insightful survey from the GDPR perspective," Comput Secur, vol. 110, Nov. 2021, doi: 10.1016/j.cose.2021.102402.

[18] R. Gao et al., "Legal regulation of AI-assisted academic writing: challenges, frameworks, and pathways," 2025, Frontiers Media SA. doi: 10.3389/frai.2025.1546064.

[19] C. Tschider, M. C. Compagnucci, and T. Minssen, "The new EU-US data protection framework's implications for healthcare," J Law

Biosci, vol. 11, no. 2, Jul. 2024, doi: 10.1093/jlb/lsae022.
[20] T. Kreutzer et al., "Ethical implications related to processing of personal data and artificial intelligence in humanitarian crises: a scoping review," BMC Med Ethics, vol. 26, no. 1, Dec. 2025, doi: 10.1186/s12910-025-01189-2.
[21] A. Choudhury et al., "Advancing Privacy-Preserving Health Care Analytics and Implementation of the Personal Health Train: Federated Deep Learning Study," JMIR AI, vol. 4, 2025, doi: 10.2196/60847.
[22] H. Zhang et al., "The impact of information technology applications on the quality of life of disabled older adults in nursing homes in China: a qualitative study," Front Public Health, vol. 13, 2025, doi: 10.3389/fpubh.2025.1560306.
[23] A. Almalawi, A. I. Khan, F. Alsolami, Y. B. Abushark, and A. S. Alfakeeh, "Managing Security of Healthcare Data for a Modern Healthcare System," Sensors, vol. 23, no. 7, Apr. 2023, doi: 10.3390/s23073612.
[24] A. A. Khan, A. A. Laghari, A. A. Shaikh, M. A. Dootio, V. V. Estrela, and R. T. Lopes, "A blockchain security module for brain-computer interface (BCI) with Multimedia Life Cycle Framework (MLCF)," Neuroscience Informatics, vol. 2, no. 1, p. 100030, Mar. 2022, doi: 10.1016/j.neuri.2021.100030.
[25] Z. Zuo, M. Watson, D. Budgen, R. Hall, C. Kennelly, and N. Al Moubayed, "Data anonymization for pervasive health care: Systematic literature mapping study," Oct. 01, 2021, JMIR Publications Inc. doi: 10.2196/29871.
[26] N. Martinez-Martin, H. T. Greely, and M. K. Cho, "Ethical development of digital phenotyping tools for mental health applications: Delphi study," JMIR Mhealth Uhealth, vol. 9, no. 7, Jul. 2021, doi: 10.2196/27343.
[27] K. Semyonov-Tal, "Keeping medical information safe and confidential: a qualitative study on perceptions of Israeli physicians," Isr J Health Policy Res, vol. 13, no. 1, p. 54, Dec. 2024, doi: 10.1186/s13584-024-00641-9.
[28] L. Swales, A. Gooden, and D. Thaldar, "The anatomy of a data transfer agreement for health research," 2024, Frontiers Media SA. doi: 10.3389/fphar.2024.1332700.
[29] E. Kapassa, M. Themistocleous, K. Christodoulou, and E. Iosif, "Blockchain application in internet of vehicles: Challenges, contributions and current limitations," Dec. 01, 2021, MDPI. doi: 10.3390/fi13120313.
[30] D. Ahamad, S. Alam Hameed, and M. Akhtar, "A multi-objective privacy preservation model for cloud security using hybrid Jaya-based shark smell optimization," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 6, pp. 2343–2358, Jun. 2022, doi: 10.1016/j.jksuci.2020.10.015.
[31] M. Poongodi et al., "5G based Blockchain network for authentic and ethical keyword search engine," IET Communications, vol. 16, no. 5, pp. 442–448, Mar. 2022, doi: 10.1049/cmu2.12251.
[32] M. K. Hasan et al., "Lightweight Cryptographic Algorithms for Guessing Attack Protection in Complex Internet of Things Applications," Complexity, vol. 2021, 2021, doi: 10.1155/2021/5540296.
[33] A. A. Khan, A. A. Laghari, A. A. Shaikh, M. A. Dootio, V. V. Estrela, and R. T. Lopes, "A blockchain security module for brain-computer interface (BCI) with Multimedia Life Cycle Framework (MLCF)," Neuroscience Informatics, vol. 2, no. 1, p. 100030, Mar. 2022, doi: 10.1016/j.neuri.2021.100030.
[34] Y. Wen, B. Liu, M. Ding, R. Xie, and L. Song, "IdentityDP: Differential private identification protection for face images," Neurocomputing, vol. 501, pp. 197–211, Aug. 2022, doi: 10.1016/j.neucom.2022.06.039.
[35] F. Öhman, J. Hassenstab, D. Berron, M. Schöll, and K. V. Papp, "Current advances in digital cognitive assessment for preclinical Alzheimer's disease," 2021, John Wiley and Sons Inc. doi: 10.1002/dad2.12217.
[36] M. R. Naeem et al., "Harnessing AI and analytics to enhance cybersecurity and privacy for collective intelligence systems," PeerJ Comput Sci, vol. 10, 2024, doi: 10.7717/peerj-cs.2264.