DIGITAL SOVEREIGNTY INSTITUTE
Research Paper | April 2026

Data Protection in the Age of Artificial Intelligence:

An Evaluation of the Adequacy of the Protection of Personal Information Act (POPIA) in South Africa

Submitted by: Bokang Ralenkoane
Edited by: Bekezela Jamela
Reviewed by: Hloriso Mohale
Prepared for: Digital Sovereignty Institute
Date of Submission: April 2026

Executive Summary

This paper examines the adequacy of the Protection of Personal Information Act, 4 of 2013 (POPIA), in addressing the regulatory challenges posed by artificial intelligence (AI) systems within contemporary data-driven environments. POPIA establishes a legally binding framework grounded in the lawful processing of personal information, incorporating core conditions such as accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, and data subject participation. However, the increasing deployment of AI technologies introduces novel forms of data processing that extend beyond the original legislative assumptions underpinning the Act.

The study finds that AI systems materially alter the nature of personal information processing through large-scale data aggregation, automated decision-making, inferential analytics, and secondary data utilisation. These processes increasingly involve the derivation of inferred or predicted personal attributes, which are not directly supplied by data subjects and are not always explicitly contemplated within traditional consent-based frameworks under POPIA.

The analysis identifies structural tensions between POPIA and AI-enabled processing environments, particularly in relation to the conditions of processing limitation (Section 13 to 14), purpose specification, and further processing compatibility (Section 15). Additional challenges arise in relation to transparency obligations, the practical enforceability of data subject rights under Sections 23 to 25, and the allocation of accountability in complex, multi-actor AI value chains.

The findings indicate that while POPIA remains applicable and legally operative within South Africa's data protection regime, its current provisions are not fully adapted to regulate algorithmic inference, automated profiling, and continuously adaptive machine learning systems. Limitations emerge in the regulation of derived data, the explainability of automated decision-making, and effective control over downstream data reuse.

Accordingly, the study concludes that POPIA requires complementary regulatory enhancement to remain effective in AI-driven contexts. This includes the development of AI-specific governance instruments addressing algorithmic transparency, risk-based processing frameworks, strengthened accountability mechanisms across data processing chains, and clearer regulatory treatment of inferred and synthetic personal information. Consideration should also be given to reinforcing data sovereignty protections in relation to cross-border AI systems and data flows.

Overall, the paper concludes that the evolution of AI systems necessitates a shift from predominantly consent-based regulatory models toward more adaptive, risk-sensitive, and technologically responsive governance frameworks that preserve the underlying objectives of POPIA while addressing emerging systemic risks in automated data processing environments.

Abstract

The rapid adoption of artificial intelligence (AI) systems is reshaping traditional approaches to data governance and privacy regulation. South Africa's Protection of Personal Information Act (POPIA) provides a foundational legal framework for protecting personal data through principles of consent, purpose limitation, accountability, and transparency. However, AI systems introduce new data practices such as large-scale data aggregation, automated inference, and continuous data reuse, which challenge the assumptions embedded in traditional regulatory frameworks. This paper adopts a qualitative policy analysis approach to assess the adequacy of POPIA in the context of AI systems. The findings suggest that while POPIA remains relevant, it is structurally limited in addressing AI-driven data ecosystems, particularly in relation to inferred data, transparency, and accountability. The study concludes that complementary AI-specific governance frameworks are required to address emerging regulatory gaps.

Contents

1. Introduction

Traditional data governance frameworks, including the Protection of Personal Information Act 4 of 2013 (POPIA), establish legally enforceable conditions for the lawful processing of personal information, grounded in principles of accountability, purpose specification, processing limitation, and security safeguards (Republic of South Africa, 2013; Information Regulator South Africa, 2026). However, artificial intelligence systems fundamentally disrupt this model. AI systems rely on large-scale datasets obtained through aggregation, reuse, and sometimes automated scraping of publicly available information (Heinonline, 2026). Unlike traditional systems, AI does not only process data but also generates new forms of information through inference and prediction (Krenn et al., 2023).

As highlighted by Wachter, S. and Mittelstadt, B. (2019), AI systems can produce inferred personal attributes that were never directly provided by individuals. This creates a structural tension between traditional data protection frameworks and modern AI systems (Stamp and Samwel Dick Mwapwele, 2024).

2. Problem Statement

Despite the existence of POPIA as South Africa's primary data protection legislation, there is increasing concern that its principles are not fully aligned with the operational realities of AI systems. The core problem addressed in this study is the structural mismatch between traditional data protection assumptions based on consent, purpose limitation, and transparency and AI systems that operate through large-scale data reuse, inference, and automated decision-making.

3. Research Objectives

This study aims to:

- Assess the limitations of POPIA in regulating AI-driven data systems
- Analyse how AI transforms traditional data governance principles
- Identify gaps in accountability, transparency, and consent mechanisms
- Evaluate policy implications for South Africa's data governance framework

4. Methodology

This study adopts a qualitative, desktop-based research design grounded in literature review and doctrinal analysis. The research relies exclusively on secondary data sources and does not involve primary data collection such as interviews or surveys.

The study is structured around three analytical approaches:

Firstly, doctrinal legal analysis is used to examine the provisions of the Protection of Personal Information Act (POPIA), focusing on its core principles, including consent, purpose limitation, accountability, and transparency.

Secondly, conceptual analysis is applied to understand how artificial intelligence (AI) systems process, reuse, and infer data, particularly in relation to machine learning models and automated decision-making systems.

Thirdly, comparative literature analysis is used to synthesise findings from international scholarship and regulatory frameworks, including discussions around the General Data Protection Regulation (GDPR), as well as academic work in AI governance and data protection.

The study draws on peer-reviewed academic literature, policy documents, legal texts, and institutional reports to identify gaps between traditional data protection frameworks and emerging AI-driven data practices.

This methodology is appropriate for exploring regulatory and conceptual gaps in fast-evolving technological domains where empirical field data is limited and where normative legal interpretation is required.

5. Literature Review

5.1. Traditional Data Governance Models

Traditional data protection frameworks such as the Protection of Personal Information Act (POPIA) are based on principles of consent, purpose limitation, accountability, transparency, and data minimisation (Information Regulator South Africa, 2026). These principles assume a linear data lifecycle in which data is collected for a specific purpose and processed within defined boundaries. Within this model, individuals are expected to maintain meaningful control over their personal information through informed consent and clearly defined processing purposes.

However, this governance approach is increasingly challenged by data-intensive digital ecosystems where data is continuously collected, reused, and repurposed beyond its original intent.

5.2. AI and Transformation of Data Use

Artificial intelligence (AI) systems fundamentally transform traditional data governance models by enabling large-scale data ingestion, continuous reuse, and predictive inference. Floridi argues that AI-driven environments shift data governance from static, rule-based regulatory structures to

dynamic and adaptive systems characterised by continuous learning, probabilistic reasoning, and feedback loops (Floridi et al., 2018). In this context, data is no longer processed in a fixed lifecycle but becomes part of an evolving informational ecosystem where meaning is continuously reconstructed through algorithmic processes.

In addition, Wachter and Mittelstadt highlight that AI systems are capable of generating inferred personal data attributes derived not directly from individuals but through computational analysis of behavioural, contextual, and relational datasets (Wachter and Mittelstadt, 2019). These inferred attributes introduce a new class of "shadow profiles" that are not explicitly provided by data subjects but may still have significant effects on decision-making and profiling outcomes. As a result, traditional data protection frameworks struggle to clearly define ownership, consent, and accountability over such derived data.

This shift creates regulatory tension for frameworks such as POPIA, which are primarily designed around principles of direct data collection, explicit consent, and purpose limitation, rather than autonomous inference and predictive analytics embedded within AI systems.

6. Findings / Analysis

6.1. Consent and Processing Limitations

POPIA assumes meaningful consent as a core mechanism for lawful processing of personal information. This requires that data subjects are informed about the purpose of data collection and actively agree to how their data will be used, thereby ensuring a degree of individual control.

However, in AI-driven environments, the effectiveness of consent is limited. Many systems rely on indirectly collected, aggregated, or inferred data rather than data explicitly provided by individuals. In addition, data is often reused across multiple contexts and purposes, which makes it difficult for users to fully understand or meaningfully consent to all forms of processing.

This challenges the principle of purpose limitation under POPIA, as data is frequently repurposed for analytics and predictive modelling beyond its original intent. As a result, consent becomes less practical as a control mechanism in complex AI systems, highlighting limitations in traditional data protection approaches.

6.2. Purpose Limitation Breakdown

POPIA requires that personal information be collected for a specific, explicitly defined, and lawful purpose, and that further processing must be compatible with the original purpose (Republic of South Africa, 2013). However, academic literature highlights that AI systems depend on continuous data reuse across multiple contexts, which creates structural tension with traditional purpose limitation principles (Wachter and Mittelstadt, 2019).

This creates tension with POPIA's principle of purpose limitation, which requires that personal information be collected for a clearly defined and specific purpose and not further processed in a way that is incompatible with that purpose. In AI environments, however, the value of data often comes from its reuse and combination with other datasets, making strict purpose boundaries difficult to maintain.

As a result, data is frequently processed beyond its original intended scope, weakening the practical application of purpose limitation in AI-driven systems.

6.3. Transparency and Explainability Challenges

AI systems often operate as complex and opaque models, particularly in the case of machine learning and deep learning algorithms. This reduces the level of transparency available to both users and regulators regarding how decisions are made and how personal data is processed.

POPIA requires openness in personal information processing, including that data subjects be made aware of the collection and use of their personal information (Republic of South Africa, 2013). However, the Information Regulator has emphasised that transparency obligations must be interpreted considering emerging technologies, including automated decision-making systems (Information Regulator South Africa, 2026). Academic literature further notes that AI systems often lack explainability due to model complexity (Wachter and Mittelstadt, 2019).

This limits the practical implementation of transparency and makes it challenging for data subjects to fully understand or verify how their information contributes to outcomes.

6.4. Accountability Fragmentation

POPIA places responsibility on organisations to ensure that personal information is processed lawfully, securely, and in accordance with its principles. This establishes a clear accountability requirement for data controllers.

However, AI systems often involve multiple stakeholders, including data providers, model developers, third-party platforms, and automated decision systems. This distributed structure makes it difficult to assign clear responsibility for specific processing activities or outcomes.

In addition, continuous learning systems may change their behaviour over time without direct human intervention, further complicating accountability. This creates challenges for enforcement under traditional regulatory frameworks such as POPIA, which are designed around clearly identifiable data controllers and static processing activities.

6.5. Data Subject Rights Limitations

Although POPIA grants data subjects rights to access, correct, and delete their personal information, the practical enforcement of these rights becomes more complex in AI-driven systems. Once data is used to train machine learning models, it is no longer stored in a directly retrievable form but embedded within model parameters and statistical relationships.

This makes it difficult to identify, extract, or remove specific individual data points from trained models. As a result, the right to erasure and correction may be limited in practice, particularly where data has already been used in model training or inference processes.

6.6. Technical Safeguards and Limitations

Technical safeguards such as encryption, anonymisation, and access control remain important components of data protection frameworks. These measures are effective in reducing unauthorised access and protecting data at rest or in transit.

However, in AI systems, these safeguards are often insufficient on their own. Advanced machine learning models can sometimes re-identify individuals from anonymised datasets or infer sensitive attributes through pattern recognition and correlation of multiple data sources. This reduces the effectiveness of traditional technical protections and highlights the need for more advanced privacy-preserving techniques in AI environments.

6.7. Data Sovereignty Concerns

The increasing use of South African-generated data in global AI systems raises important concerns regarding data sovereignty. Data is often processed, stored, or analysed by international organisations, with limited visibility over how it is used or monetised.

This creates a situation where local data contributes to global AI value creation, while control over processing and derived insights may lie outside national jurisdiction. As a result, concerns arise regarding regulatory oversight, economic value extraction, and the ability of South Africa to govern AI-generated outputs involving its citizens' data.

7. Discussion

The findings indicate a structural misalignment between POPIA and AI systems. While POPIA is designed around principles of control, consent, and purpose limitation, AI systems operate through scale, reuse, and inference (Mbonye et al., 2024). This creates three core tensions:

- Control vs Automation: Individuals lose meaningful control over how their data is used due to automated processing, third-party integration, and algorithmic decision-making (Christodoulou and Limniotis, 2024)
- Purpose vs Reuse: Data is continuously repurposed beyond its original intent, particularly in machine learning model training and predictive analytics (Davis et al., 2023)
- Transparency vs Complexity: AI systems limit interpretability and explainability due to the complexity of machine learning and deep learning models (Barnes and Hutson, 2024)

These tensions are not unique to South Africa but are also observed in stronger regulatory frameworks such as the General Data Protection Regulation (GDPR), indicating a systemic global challenge.

8. Policy Implications

The analysis suggests several key policy directions:

- The Information Regulator of South Africa recognises the need for evolving governance approaches to address emerging risks associated with digital technologies and automated processing systems (Information Regulator South Africa, 2026). International policy developments similarly advocate for risk-based and adaptive regulatory frameworks for artificial intelligence governance (OECD, 2019; European Commission, 2025).
- Shift from strict consent-based models to risk-based governance approaches aligned with international policy thinking on AI ethics and accountability (OECD, 2019; UNESCO, 2021).
- Strengthening transparency and explainability requirements for AI systems, particularly in high-impact decision-making contexts (Goodman and Flaxman, 2017).
- Clarification of accountability across AI value chains, ensuring clear responsibility for data controllers, processors, and model developers (Floridi et al., 2018).
- Enhanced protections for data sovereignty and cross-border data usage, particularly in relation to global data flows and jurisdictional control (UNCTAD, 2021).

9. Conclusion and Findings

9.1. Overview of the Study

This study examined the alignment between traditional data protection frameworks, specifically the Protection of Personal Information Act (POPIA), and the evolving realities of artificial intelligence (AI)-driven data ecosystems. The primary focus was to assess whether existing governance principles remain effective in regulating modern data practices characterised by large-scale data processing, continuous reuse, and algorithmic inference.

The analysis was structured around key dimensions of data governance, including consent, purpose limitation, transparency, accountability, technical safeguards, data subject rights, and data sovereignty. Across these dimensions, the study identified significant structural tensions between regulatory assumptions embedded in POPIA and the operational logic of AI systems.

9.2. Summary of Key Findings

The findings indicate a fundamental misalignment between POPIA and AI-enabled data environments. POPIA is grounded in traditional data governance principles such as informed consent, defined processing purposes, and direct control over personal information. In contrast, AI systems operate through continuous data ingestion, adaptive learning, and predictive inference, which extend beyond static regulatory boundaries.

Three core tensions were consistently identified throughout the analysis:

I. Control versus Automation:

While POPIA assumes meaningful user control over personal information, AI systems reduce this control through automated processing, third-party data integration, and large-scale system design.

II. Purpose versus Reuse:

POPIA requires that data be collected for specific and defined purposes. However, AI systems depend on the reuse and repurposing of datasets across multiple applications, making strict purpose limitation difficult to maintain in practice.

III. Transparency versus Complexity:

POPIA emphasises transparency in data processing. However, AI systems, particularly machine learning models, are often complex and opaque, limiting interpretability and reducing the ability of individuals to understand how decisions are made.

In addition, the study found that data subject rights, technical safeguards, and accountability mechanisms become increasingly difficult to enforce in AI environments due to embedded model learning, re-identification risks, and distributed governance structures.

9.3. Contribution of the Study

This study contributes to the growing body of literature on AI governance and data protection law by highlighting the structural limitations of applying traditional regulatory frameworks to modern AI systems. It demonstrates that the challenge is not merely compliance-based but systemic in nature, arising from the fundamental differences between linear data processing models and adaptive, inference-driven AI architectures.

Furthermore, the study reinforces the argument that regulatory frameworks such as POPIA, while foundational and necessary, may require augmentation to effectively address emerging risks associated with algorithmic decision-making, predictive analytics, and large-scale data reuse.

9.4. Implications of the Study

The findings have several important implications for policy and governance:

Firstly, there is a need to develop AI-specific regulatory mechanisms that explicitly address inference, profiling, and automated decision-making processes. Secondly, governance approaches may need to shift from strict consent-based models toward risk-based and accountability-driven frameworks that better reflect the realities of AI systems. Thirdly, greater emphasis should be placed on transparency and explainability requirements, particularly where AI systems are used in decision-making contexts that affect individuals or communities. Fourthly, accountability structures must be clarified across complex AI value chains involving multiple actors, including data providers, model developers, and platform operators. Finally, issues of data sovereignty require stronger regulatory attention, particularly in relation to cross-border data flows and the use of locally generated data in global AI systems.

9.5. Limitations of the Study

This study is primarily conceptual and based on secondary literature, which limits its ability to provide empirical validation of the identified challenges. In addition, the rapidly evolving nature of AI technologies means that regulatory interpretations and technological capabilities may change over time, potentially affecting the long-term relevance of certain findings.

Future research could incorporate empirical case studies or industry-specific analyses, particularly within sectors such as supply chain management, finance, or healthcare, where AI-driven data processing is highly prevalent.

9.6. Conclusion

In conclusion, POPIA remains a critical foundation for data protection in South Africa; however, its underlying assumptions are increasingly challenged by the rise of artificial intelligence systems. The central issue is not the absence of regulation, but rather a structural incompatibility between traditional data governance principles and the operational realities of AI-driven ecosystems.

Addressing this gap will require both the refinement of existing legal frameworks and the development of complementary AI governance approaches that account for inference, scale, and automated decision-making.

10. References

Barnes, E. and Hutson, J. (2024) 'Navigating the complexities of AI: The critical role of interpretability and explainability in ensuring transparency and trust', Digital Commons@Lindenwood University. Available at: https://digitalcommons.lindenwood.edu/faculty-research-papers/643/ (Accessed: 29 April 2026).

Christodoulou, P. and Limniotis, K. (2024) 'Data protection issues in automated decision-making systems based on machine learning: research challenges', Network, 4(1), pp. 91-113. doi:https://doi.org/10.3390/network4010005

Davis, J.C., Jajal, P., Jiang, W., Schorlemmer, T.R., Synovic, N. and Thiruvathukal, G.K. (2023) 'Reusing deep learning models: challenges and directions in software engineering'. doi:https://doi.org/10.1109/jva60410.2023.00015

European Commission (2025) AI Act. Available at: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (Accessed: 29 April 2026).

Floridi, L. et al. (2018) 'AI4People: An ethical framework for a good AI society: opportunities, risks, principles, and recommendations', Minds and Machines, 28(4), pp. 689-707. doi:https://doi.org/10.1007/s11023-018-9482-5

Information Regulator South Africa (2026) About the Information Regulator. Available at: https://inforegulator.org.za/about/ (Accessed: 29 April 2026).

Krenn, M. et al. (2023) 'Forecasting the future of artificial intelligence with machine learning-based link prediction in an exponentially growing knowledge network', Nature Machine Intelligence. doi:https://doi.org/10.1038/s42256-023-00735-0

OECD (2019) The OECD Artificial Intelligence (AI) Principles. Available at: https://oecd.ai/en/ai-principles (Accessed: 29 April 2026).

OECD (2025) Privacy principles. Available at: https://www.oecd.org/en/topics/privacy-principles.html (Accessed: 29 April 2026).

Republic of South Africa (2013) Protection of Personal Information Act 4 of 2013. Government Gazette. Available at: https://www.gov.za/documents/protection-personal-information-act (Accessed: 29 April 2026).

Stamp, J. and Mwapwele, S.D. (2024) 'Examining data governance to determine how democratic data management can be achieved in organizations', Communications in Computer and Information Science, pp. 421-436. doi:https://doi.org/10.1007/978-3-031-64881-6_25

UNCTAD (2021) Digital Economy Report 2021. Available at: https://unctad.org/system/files/official-document/der2021_en.pdf (Accessed: 29 April 2026).

UNESCO (n.d.) Ethics of Artificial Intelligence. Available at: https://www.unesco.org/en/artificial-intelligence/recommendation-ethics (Accessed: 29 April 2026).

Wachter, S. and Mittelstadt, B. (2019) 'A right to reasonable inferences: re-thinking data protection law in the age of big data and AI', Columbia Business Law Review, 2019(2), pp. 494-620. doi:https://doi.org/10.7916/cblr.v2019i2.3424