
AI Policy Recommendations for Southern Africa Informed by Region-Specific Risks and Domestic Governance Precedents ¹

Karabo Motsileng
University of Cape Town

Génevieve Chikwanha
University of Cape Town

With
Apart Research

Abstract

AI governance frameworks and risk taxonomies have been developed predominantly for Global North settings, yet AI adoption across Southern Africa is accelerating. Emerging scholarship has begun mapping AI risks in the African context, but the relationship between those academic risk categories and documented cases of AI-related harm in the region has received limited attention, and the connection between region-specific risks and actionable domestic policy precedents remains underdeveloped. This paper triangulates six academic risk-mapping sources with eleven empirical sources, including case law, regulatory investigations, and legislative instruments across six African jurisdictions, to identify where academic risk categories hold, where they require mechanistic specification, and where they miss documented harms entirely. We find a systematic divergence: the academic literature covers surveillance, disinformation, and general algorithmic bias, while the empirical evidence documents sectoral algorithmic discrimination, legal ambiguity as a structural risk enabler, and fiscal base erosion from technology outsourcing. We then analyse AI policy objectives across four Southern African countries and the African Union, identifying gaps between stated policy goals and the empirically documented risks. Using fiscal base erosion as a focused case, we demonstrate that South African legal and regulatory precedents already contain interpretive tools that can inform mechanism-level AI policy recommendations. For each recommendation, we state the institutional antecedents required for it to apply beyond South Africa.

¹ Research conducted at the [The Global South AI Safety Hackathon](#), June 2026

1. Introduction

AI adoption across Southern Africa is advancing ahead of the governance frameworks needed to manage its risks. Over 40 per cent of surveyed institutions across nine African countries, have begun experimenting with or implementing generative AI (Kuyoro et al., 2025), building on AI systems already deployed across healthcare, financial services, and public administration (Baloyi, 2025; Ngcukaitobi et al., 2025). Yet AI governance frameworks have been produced predominantly in and for Global North institutional settings (Okolo & Raji, 2026); and countries in African are at varying stages of AI policy development, with some having published national strategies and others still in early drafting phases (Diallo et al., 2025), and effective AI governance requires both regionally tailored and internationally coordinated regulatory responses.

This matters practically because the risks attending AI adoption in Southern Africa and the policy precedents available to address them have not yet been examined together. Work documenting AI adoption, governance concerns, and specific harm cases in African and South African settings is emerging (Baloyi, 2025; Diallo et al., 2025; Ngcukaitobi et al., 2025), but the synthesis of that work into a mapping of region-specific risks, and the connection of those risks to actionable policy precedents, remains underdeveloped. Southern African countries need not begin from first principles, however. Existing national policies in related domains, such as the Protection of Personal Information Act (POPIA) for data governance, have already addressed analogous technology governance challenges, and their implementation records offer empirical lessons for AI-specific policy design (Baloyi, 2025; Mtuze & Morige, 2024).

Our project addresses this by combining two Africa Track ideas proposed by the hackathon organisers: mapping region-specific AI risks for Southern Africa, and examining precedents in local policy using South Africa as a case study. We treat South Africa as a case study rather than a proxy for the region; where recommendations draw on South African precedents, we state the antecedents required for them to apply elsewhere in Southern Africa.

Our main contributions are:

1. An extended mapping of AI safety risks that are specific to or particularly salient in the Southern African context, grounded in academic and grey literature, policy documents, and documented cases.
2. An analysis of how existing South African policy and legislation have addressed analogous governance challenges, and an assessment of the lessons those precedents offer for AI-specific policy design.
3. A set of antecedent-aware policy recommendations that connect the identified risks to concrete precedents, stating the antecedents (preconditions) required for each recommendation to apply beyond the South African case.

2. Related Work

The most directly related work to this paper is Segun et al. (2025), which maps AI risks across the African continent using the International AI Safety Report's tripartite framework of malicious use, malfunction, and systemic risks, and goes further to propose a five-pillar action plan for an African research and policy agenda on AI safety. That agenda foregrounds a human rights-based approach to AI governance, calls for

an African AI Safety Institute, and advocates for continent-wide public AI literacy, inclusive benchmarking for African languages, and an annual AU-level AI Safety and Security Forum. Segun et al. is therefore not only a risk taxonomy but a programmatic statement about what African AI safety research and policy should prioritise. Other recent work complements this baseline from different angles. Hübschle & Shearing (2026) develop a "harmscapes" framework grounded in critical criminology and nodal governance theory, with case studies on predictive policing in Cape Town and digital identity exclusion in Kenya. Ireri et al. (2026) focus specifically on severe and catastrophic AI risks, proposing evaluation methodologies calibrated to African infrastructure constraints such as unreliable electricity, low connectivity, and weak state capacity. Akpudo et al. (2024) survey AI concerns for Sub-Saharan Africa's vulnerable groups and identify data governance, safety, privacy, and skills gaps as key themes.

Collectively, these papers establish a broad categorical vocabulary for AI risks in Africa. What they do not do, and what our paper addresses, is test whether those categories are adequate when examined against documented cases of AI-related harm in the region. Segun et al. (2025) acknowledge, for instance, the risk of biased credit-scoring and content moderation failures, but the specific mechanisms through which algorithmic systems produce racially discriminatory outcomes in South African healthcare administration, or through which digital lending apps in Nigeria use harvested device data for coercive debt recovery, do not appear in any existing taxonomy. Our paper triangulates the academic risk-mapping literature with empirical evidence from case law, regulatory actions, and investigation reports across six jurisdictions to identify where the categories hold, where they require mechanistic specification, and where they miss documented harms entirely. We then extend the analysis into the AI policy and precedent domains, examining how the region's preceding governance instruments and judicial decisions can inform mechanism-level recommendations that complement the broader agenda Segun et al. (2025) propose.

3. Methods

We adopt a qualitative document analysis approach, which Bowen (2009) describes as a systematic procedure for reviewing and evaluating documents in order to elicit meaning, gain understanding, and develop empirical knowledge. Document analysis is well suited to this study because it enables the examination of diverse source types, including academic literature, case law, regulatory reports, and legislative instruments, within a single analytical framework. It is efficient, non-reactive, and permits broad coverage across jurisdictions and time periods.

Our risks corpus comprises two layers. The first consists of six academic papers that map AI risks in Africa or the Global South, selected through a purposive search of Google Scholar, Scopus, and arXiv using targeted search strings combining exact-phrase risk terminology with geographic qualifiers. The second layer consists of eleven empirical sources: case law, regulatory investigation reports, legislative texts, industry data, and institutional publications from South Africa, Nigeria, Ghana, Uganda, Kenya, and Tanzania, identified through searches of legal databases (SAFLII, Kenya Law Reports), civil society repositories (CIPESA, Access Now, ISER Uganda), and institutional websites (SARS, FCCPC). Sources were screened against inclusion criteria requiring substantive engagement with AI-related risks in an African or Global South context, publication from 2019 onwards, and availability in English.

Next, we analysed national AI policies and AI policy drafts from South Africa, Zimbabwe, Zambia, Lesotho, and the African Union. These documents were identified through Google keyword searches and

retrieved from official government or institutional websites. Where multiple versions existed, the most recent publicly available policy or policy draft was chosen. The only exception was South Africa, where the 2026 AI policy draft had been withdrawn. Thus, the 2024 draft was used instead. Policies not available in English and policies originating outside the Global South were excluded.

The final stage of our analysis involved identifying South African legal and regulatory precedents relevant to the risks identified in the preceding section. These sources were identified primarily through keyword searches of the SAFLII along with official institutional websites. The corpus includes case law, legislation, regulations, government reports, institutional publications, and guidance documents from bodies such as the Competition Commission and other relevant government departments. Sources were screened for relevance to the AI risk under consideration and their applicability within the South African legal and regulatory context. No publication date restrictions were applied to precedents.

Our analysis combines content analysis and thematic analysis, consistent with Bowen's (2009) description of the document analysis procedure as an iterative process that organises information into categories related to the central research questions while simultaneously recognising emergent patterns. We draw on the six-phase thematic analysis framework described by Braun & Clarke (2006) and elaborated by Ahmed et al. (2025): familiarisation with the data, generating initial codes, searching for themes, reviewing themes, defining and naming themes, and producing the report.

In Part 1 (risk identification), coding proceeded inductively, allowing risk concepts to emerge from the data. We then constructed a concept matrix following (Webster & Watson, 2002), mapping each source against the inductively derived risk concepts to identify patterns of convergence, divergence, and absence between the academic and empirical layers. In Part 2 (policy objectives), coding proceeded deductively using predefined categories drawn from the governance instruments reviewed. In Part 3 (precedents and recommendations), we combined both approaches: risk categories from Part 1 guided the selection of relevant precedents, and the analysis of their governance implications proceeded inductively.

The study is a document analysis conducted within a two-day hackathon timeframe. The corpus is purposive rather than exhaustive, and the analysis captures what is documented rather than what may exist undocumented.

4. Findings and Analyses

4.1 Risk Identification

Table 1 presents the concept matrix mapping seventeen sources against eight risk concepts derived inductively from the corpus. The matrix organises sources into two layers: academic literature that identifies or taxonomises AI risks, and empirical evidence that documents concrete risk manifestations. A checkmark indicates substantive engagement with the risk concept, not merely a passing mention.

Concepts (Risks)	Surveillance & Predictive Policing	Disinformation & Electoral Manipulation	Algorithmic Bias	Algorithmic Discrimination in Sectoral Deployment	Digital Identity & Automated Exclusion	AI Supply Chain Labour Exploitation	Labour Displacement & Automation	AI-Enabled Gender-Based Violence	Environmental Costs (Carbon, E-waste)	Data Governance & Regulatory Gaps	Legal Ambiguity as Structural Risk Enabler	Fiscal Base Erosion from Tech Outsourcing	Infrastructure Fragility & Cascading Failure	Digital/Data Colonialism & Compute Dependency	Cybercrime & AI-Enabled Fraud	Reliability, Hallucination & Safety
Sources																
LAYER 1: ACADEMIC LITERATURE																
Segun et al. (2025)	✓	✓	✓				✓	✓	✓					✓	✓	✓
Hübschle & Shearing (2026)	✓				✓					✓				✓		
Ileri et al. (2026)		✓											✓			
Allaham et al. (2025)	✓	✓	✓				✓		✓						✓	
Akpudo et al. (2024)	✓		✓				✓			✓			✓			✓
Yang et al. (2026)						✓								✓		
LAYER 2: EMPIRICAL EVIDENCE																
Ngcukaitobi et al. (2025)				✓												
P.P.M. v Minister of Home Affairs (2024)					✓						✓					
ISER et al. v NIRA (2025)					✓											
Gorni v Vodafone Ghana (2026)					✓						✓					
Uzoigwe & Edward (2026)				✓							✓					
WASPA v FCCPC (2026)											✓					
Malekela & Thaldar (2024)											✓					
Kenya Data Protection Act (2019)										✓						
Daily Investor (2025)												✓				
Banga et al. (2025)												✓				
Monkam (2024)												✓				

The matrix reveals a systematic divergence between the risk domains covered by the academic literature and those documented in the empirical evidence from the region.

One risk domain shows productive convergence across both layers. **Digital identity and automated exclusion** is addressed academically by Hübschle & Shearing (2026) through the Kenyan Huduma Namba case study, and is documented empirically in three distinct jurisdictions. In South Africa, the High Court found that the Home Affairs National Identification System had blocked 1.8 million identity numbers through an automated mechanism that could not separate the act of flagging an identity from the act of blocking it, thereby stripping affected persons of access to banking, healthcare, education, and social grants without prior notice or hearing (*P.P.M. et al. v Minister of Home Affairs et al.*, 2024). In Uganda, the High Court declined to recognise the exclusionary effects of the Ndaga Muntu system despite evidence that up to one third of the adult population lacks a National ID required for access to social protection and healthcare (*ISER et al. v Attorney General & NIRA*, 2025). In Ghana, the Supreme Court ruled that the unauthorised linking of a citizen's Ghana Card to a mobile phone number constituted a privacy violation, holding that the aggregation of individually non-sensitive identifiers triggers a duty of confidentiality under the Data Protection Act 2012 (*Gorni v Vodafone Ghana Ltd & et al.*, 2026). These cases confirm the academic category but reveal a mechanism it does not name: automated systems that architecturally fuse distinct administrative steps (suspicion, investigation, determination) into a single automated action, making proportionate response structurally impossible.

Three risk domains are documented empirically but are either absent from or underspecified in the academic literature.

First, **algorithmic discrimination in sectoral deployment**: the Section 59 Investigation into South African medical schemes found statistically significant racial disparities in the outcomes of algorithmic fraud, waste, and abuse detection systems, with Black healthcare providers disproportionately flagged and financially penalised (Ngcukaitobi et al., 2025). The Uzoigwe & Edward (2026) analysis of AI errors in Nigerian banking documents how credit-scoring algorithms trained on unrepresentative data routinely reject low-income applicants, while the Nigeria Data Protection Act's Section 37 right to contest automated decisions lacks operational enforcement mechanisms. These are not instances of "algorithmic bias" in the abstract; they are sector-specific deployments producing measurable discriminatory outcomes within existing legal and institutional structures.

Second, **legal ambiguity as a structural risk enabler**: this cross-cutting finding appears in five empirical sources spanning healthcare, identity systems, banking, lending, lending regulation, and data protection, but in no academic source. In South Africa, the Home Affairs National Identification System was permitted to block 1.8 million identity numbers without prior notice or hearing because the underlying legislative and regulatory framework imposed no requirement that the act of flagging an identity be separated from the act of blocking it (*P.P.M. et al. v Minister of Home Affairs et al.*, 2024); the Tanzanian High Court struck down provisions of the Personal Data Protection Act for undefined terms such as "unlawful means" (*Tito Magoti v Attorney General*, 2024); South Africa's POPIA contains a parallel ambiguity in its "disproportionate effort" threshold for processing special personal information (Malekela & Thaldar, 2024); and Nigeria's NDPA creates statutory rights whose enforcement architecture does not yet exist (Uzoigwe & Edward, 2026); and jurisdictional ambiguity between Nigeria's telecommunications and consumer protection

regulators allowed an industry association to suspend enforcement of digital lending regulations through procedural challenge before their substantive provisions could be tested (*WASPA v FCCPC*, 2026). The finding here is not the absence of legal frameworks, which the academic literature already identifies, but the specific ambiguities within frameworks that do exist, which interact with automated systems to produce harm that neither the legal instrument nor the AI risk taxonomy anticipates.

Third, **fiscal base erosion** from technology outsourcing: SARS regulatory actions in 2024 documented that foreign e-commerce platforms Shein and Temu secured an estimated R7.3 billion in South African sales while exploiting customs concessions designed for low-value imports (LSF, 2025), and Banga et al. (2025) estimate that the WTO moratorium on customs duties on electronic transmissions cost South Africa over \$161 million between 2017 and 2020. No source in the academic risk-mapping literature addresses the fiscal consequences of technology platform dependence, despite its direct relevance to the structural economics of AI adoption: subscription-based access to foreign AI systems is economically equivalent to hiring an offshore workforce whose labour generates no domestic tax revenue, payroll contribution, or consumption multiplier.

The overall pattern is that the academic literature and the empirical evidence occupy largely separate columns of the concept matrix. The literature provides strong coverage of surveillance, disinformation, general algorithmic bias, labour displacement, and environmental costs. The empirical evidence documents sectoral algorithmic discrimination, legal ambiguity, and fiscal erosion. The implication for governance is that interventions designed at the level of the academic categories will not reach the specific mechanisms through which harm is currently being produced in the region.

4.2 AI Policy Objectives in Southern Africa

While each country has its own policy objectives, some commonalities emerged. In order to understand these commonalities, we examined the AI policies and policy drafts of four Southern African countries and the African Union (African Union, 2024). The countries examined include South Africa (Department of Communications and Digital Technologies, 2024), Zambia (Ministry of Technology and Science, 2024), Lesotho (Ministry of Information, Communications, Science, Technology and Innovation, 2025), and Zimbabwe (Ministry of ICT, Postal, and Courier Services, 2026). Botswana, Mozambique, Angola, Eswatini, Malawi, and Namibia were excluded from this examination.

From the policies that we examined (African Union, 2024; Department of Communications and Digital Technologies, 2024; Ministry of Technology and Science, 2024; Ministry of Information, Communications, Science, Technology and Innovation, 2025; Ministry of ICT, Postal, and Courier Services, 2026), we found that Southern African countries aim to become regional or continental leaders in AI and foster better collaboration across national, regional, and international borders. To ensure that they have the capacity and capability to achieve this, they aim to upskill the population, with particular focus on introducing AI education to primary, secondary, and tertiary levels. The newly skilled population should then be able to find employment with the new jobs the government hopes to create, which in turn will improve economic resilience and development. AI will be adopted across some or all of the following sectors: healthcare, agriculture, education, mining, climate change, and public services in accordance with continental (the AU) and international ethical and regulatory standards. Specifically, there is an emphasis on deploying AI

systems ethically, including but not limited to addressing issues of transparency, bias, privacy violations, and human rights violations.

Mapping these policy objectives against the risks that we identified in Section 4.1 shows where the policies' objectives align with risks and where gaps remain. The policy goals of addressing transparency, bias, privacy violations, and human rights violations directly respond to the risks of algorithmic discrimination and automated exclusion. For example, the policies' emphasis on ethical deployment aligns with the need to prevent the algorithmic bias risk.

However, the remaining risks discussed in Section 4.1 expose a gap in current policy objectives. First, while policies aim to adopt AI to improve economic resilience and sectoral inclusion, they do not address the specific risk of predatory algorithmic lending. Second, the policies commit to international regulatory standards but overlook the structural risk of legal ambiguity. The empirical evidence shows that harms often stem from undefined terms and missing enforcement mechanisms within existing domestic laws (Magoti v Attorney General, 2024; Malekela and Thaldar, 2024). High-level policy commitments to transparency and ethics may not be sufficient to resolve these specific legal ambiguities.

Finally, while the policies focus heavily on job creation and economic development, they do not address the risk of fiscal base erosion from technology outsourcing. The policies encourage AI adoption but do not address the economic consequences of relying on foreign AI systems, which operate similarly to an offshore workforce and generate no domestic tax revenue (Banga, Beyleveld and Munu, 2025). As a result, the current policies may overlook a structural risk that directly undermines their own economic development goals. Bridging this gap between high-level objectives and empirical risks is necessary for effective governance, which we address in Section 4.3.

4.3 Precedents and Recommendations

This section narrows the analysis to a single risk domain, fiscal base erosion arising from technology outsourcing, to show how domestic legal precedents and regulatory instruments can be used to translate empirically observed risks into concrete policy. The purpose is not to suggest that this is the most significant risk, but rather to use it as a focused case study for showing how Southern African legal systems already contain interpretive tools that can be extended to emerging AI governance challenges. This approach is particularly important for risks that remain under-theorised or insufficiently recognised in dominant academic taxonomies, yet are already materialising within regional institutional contexts.

Recommendation 1: AI policy should ensure that AI outsourcing decisions consider the economic benefit to South Africa.

One of the key risks identified in Section 4.1 is the structural reduction of South Africa's domestic fiscal base through AI outsourcing. As computing infrastructure, cloud services, AI models, and associated profits move overseas, domestic value creation and taxable economic activity decline, which in turn weakens the state's ability to fund public investment and long-term economic development (Ajuzieogu, 2025; Carmody, 2020, as cited in Ajuzieogu, 2025). South African law already recognises the importance of protecting domestic economic value from cross-border extraction. In *Dölberg Asset Finance Ltd v Dölberg South Africa (Pty) Ltd* (2021), the Court confirmed that cross-border transfers may legitimately be assessed according to whether sufficient value remains within South Africa. Thus, by analogy, this principle supports

evaluating AI outsourcing on commercial grounds and also on its contribution to domestic capability and economic development.

Recommendation 2: AI policy should draw from existing tax mechanisms to explicitly monitor and mitigate fiscal base erosion.

This approach is reinforced by South Africa's tax mechanisms. Transfer pricing rules, thin-capitalisation provisions, earnings stripping rules, and the Global Minimum Tax all serve to prevent multinational companies from negatively impacting South Africa's tax base through cross-border financial arrangements (*ABC (Pty) Ltd v Commissioner for the South African Revenue Service*, 2021; Goosen & Greeff, 2025; Global Minimum Tax Act 46 of 2024). These measures show that South Africa has an established policy objective of preventing domestic value from being moved abroad without an accompanying contribution to the local economy.

Recommendation 3: AI policy should prioritise domestic capability development (wherever feasible).

The same objective is present in South Africa's digital and economic development policies. The National Policy on Data and Cloud (2024) identifies data and digital infrastructure as strategic national assets and prioritises domestic capability building and the participation of South African SMMEs in government digital projects (Department of Communications and Digital Technologies, 2024). Similarly, the Preferential Procurement Policy Framework Act 5 of 2000 requires public procurement to advance developmental objectives alongside value for money. Competition law reinforces this approach by recognising that dominant digital platforms can undermine domestic innovation and market participation, thus justifying regulatory intervention to support local businesses and promote economic development (Magau, 2024; *GovChat Proprietary Limited v Facebook Inc.*, 2021). Thus, retaining domestic value and strengthening local technological capability are already established policy objectives.

5. Discussion and Limitations

The findings of this paper carry a broader implication for how AI governance is designed in the Southern African context. The concept matrix in Section 4.1 reveals that the risk domains most thoroughly addressed in the academic literature, such as surveillance, disinformation, and algorithmic bias in the abstract, occupy largely different columns from the risk domains documented in the empirical evidence, such as sectoral algorithmic discrimination, legal ambiguity as a structural risk enabler, and fiscal base erosion. The policy objective analysis in Section 4.2 confirms that current Southern African AI policies orient their commitments toward the former set of categories. Governance interventions calibrated at the level of those academic categories, for instance, commitments to "address bias" or "close governance gaps," will not reach the specific mechanisms through which harm is currently being produced in the region: automated systems that architecturally fuse distinct administrative steps into a single action (Section 4.1, digital identity), undefined statutory terms that permit discriminatory outcomes to persist within nominally compliant systems (Section 4.1, legal ambiguity), or customs concession structures that foreign platforms exploit to extract domestic value (Section 4.1, fiscal erosion). What the precedent analysis in Section 4.3 demonstrates is that the region's own courts and regulators are already generating the interpretive tools needed for this more granular, mechanism-level governance. The task for AI policy is to draw on those precedents

deliberately rather than defaulting to governance frameworks whose risk categories do not match the harms the region is experiencing.

Limitations

This analysis has several limitations. First, due to time constraints and language barriers, we could not evaluate the AI policies of all Southern African countries. For example, Angola's policy is in Portuguese, and several other national strategies remain unpublished or otherwise inaccessible or not easily accessible. Second, our analysis relies exclusively on South African precedents. This was due to our existing expertise in South Africa's regulatory landscape as well as the limited scope of the project. As a consequence, the legal precedents discussed may not map perfectly onto other nations.

Future Work

Future work should expand on this work by evaluating all existing policies and policy drafts from across the continent. Additionally, they can build on our work to provide jurisdiction-specific precedent analyses and recommendations that align with the current legal contexts of individual African countries.

LLM Usage Statement

We used Gemini and Claude to help source papers to read. However, all papers were read by us, and all analyses and written work were developed by us, independent of any AI tool with the exception of Grammarly, which was used for automatic spelling and grammar checking.

References

- ABC (Pty) Ltd v Commissioner for the South African Revenue Service*, Case No. IT 14305 (Tax Court of South Africa, held at Johannesburg 2021).
- African Union. (2024). *Continental Artificial Intelligence Strategy*. Available: <https://au.int/en/documents/20240809/continental-artificial-intelligence-strategy>.
- Ahmed, S. K., Mohammed, R. A., Nashwan, A. J., Ibrahim, R. H., Abdalla, A. Q., M. Ameen, B. M., & Khedhir, R. M. (2025). Using thematic analysis in qualitative research. *Journal of Medicine, Surgery, and Public Health*, 6, 100198. <https://doi.org/10.1016/j.glmedi.2025.100198>
- Ajuzieogu, U. C. (2025). *From aspiration to implementation: The African Union AI Continental Strategy and the development-governance paradox*. African Institute for Artificial Intelligence Policy.
- Akpudo, U. E., Effoduh, J. O., Kong, J. D., & Gao, Y. (2024). Unveiling AI Concerns for Sub-Saharan Africa and its Vulnerable Groups. *International Conference on Intelligent and Innovative Computing Applications*, 2024, 45–55. <https://doi.org/10.59200/ICONIC.2024.007>

- Baloyi, M. W. (2025). A Systematic Analysis of Ethical and Governance Concerns Relating to Artificial Intelligence Adoption in the South African Public Sector. *SSRN Electronic Journal*.
<https://doi.org/10.2139/ssrn.5065151>
- Banga, K., Beyleveld, A., & Munu, M. L. (2025). Trading away tax sovereignty? How trade rules shape taxation of the. *Journal of International Economic Law*, 28(1), 43–62.
<https://doi.org/10.1093/jiel/jgaf004>
- Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*, 9(2), 27–40. <https://doi.org/10.3316/QRJ0902027>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp063oa>
- Competition Act 89 of 1998*, Republic of South Africa.
- Daily Investor. (2025). Bad news for Shein and Temu in South Africa. *Daily Investor*.
<https://dailyinvestor.com/retail/98283/bad-news-for-shein-and-temu-in-south-africa/>
- Data Protection Act, 2019, No. 24 of 2019 (2019). <https://new.kenyalaw.org/akn/ke/act/2019/24>
- Department of Communications and Digital Technologies. (2024). *South Africa National Artificial Intelligence Policy Framework*. Government Gazette No. 50741. Republic of South Africa. Available: <https://www.dcdt.gov.za/sa-national-ai-policy-framework/file/338-sa-national-ai-policy-framework.html>.
- Diallo, K., Smith, J., Okolo, C. T., Nyamwaya, D., Kgomo, J., & Ngamita, R. (2025). Case studies of AI policy development in Africa. *Data & Policy*, 7, e15. <https://doi.org/10.1017/dap.2024.71>
- Dölberg Asset Finance Ltd v Dölberg South Africa (Pty) Ltd*, Case No. 2020/25831 (High Court of South Africa, Gauteng Division, Pretoria 2021).
- Global Minimum Tax Act 46 of 2024*, Republic of South Africa.
- Goosen, L., & Greeff, C. (2025). *Thin capitalisation safe harbour rules: A proposed conceptual legislative design*. Potchefstroom Electronic Law Journal (PER / PELJ), 28, 1-36.
<https://doi.org/10.17159/1727-3781/2025/v28i0a17049>.
- Gorni v Vodafone Ghana Ltd & Others, Civil Appeal No. J4/40/2025 (Supreme Court of Ghana February 25, 2026). <https://thebftonline.com/2026/04/14/when-privacy-becomes-risk-based-the-supreme-courts-decision-in-gorni-v-vodafone/>
- GovChat Proprietary Limited and Another v Facebook Inc. and Others*, Case No. IR165Nov20 (Competition Tribunal of South Africa 2021).

- Hübschle, A., & Shearing, C. (2026). Artificial intelligence harmscapes: Rethinking digital governance in the age of cognitive tools. *Contemporary Justice Review*, 1–18. <https://doi.org/10.1080/10282580.2026.2647199>
- Initiative for Social and Economic Rights (ISER) and Others v Attorney General and National Identification and Registration Authority (NIRA), HCT-00-CV-MC-0066-2022 (High Court of Uganda at Kampala June 10, 2025). <https://digitalrightsalliance.africa/ugandas-digital-id-barrier-worsens-as-court-delivers-blow-to-access/>
- Ileri, G., Abungu, C., Cheptumo, J., Dounia, S., Gitau, M., Kasaon, S., Michie, M., Okolo, C. T., & Shock, J. (2026). *Assessing the Case for Africa-Centric AI Safety Evaluations* (Version 2). arXiv. <https://doi.org/10.48550/ARXIV.2602.13757>
- Kuyoro, M., Bagus, U., Benshrir, A., & Bobat, Z. (2025). *Leading, not lagging: Africa's gen AI opportunity* (QuantumBlack, AI by McKinsey) [Industry Report]. McKinsey & Company. <https://www.mckinsey.com/capabilities/quantumblack/our-insights/leading-not-lagging-africas-gen-ai-opportunity#/>
- LSF. (2025). *Offshore E-commerce Disruption in South Africa*. LSF. <https://www.lsf-sa.co.za/reports/offshore-e-commerce-disruption-in-south-africa>
- Magau, P. (2024). *An overview of the extent of the powers of South African competition authorities in the regulation of price discrimination under the Competition Act 89 of 1998 in the context of digital transformation*. Potchefstroom Electronic Law Journal (PER / PELJ), 27, 1-21. <https://doi.org/10.17159/1727-3781/2024/v27i0a17154>.
- Malekela, M., & Thaldar, D. (2024). Data protection law: Lessons from Tanzania for South Africa? *South African Journal of Bioethics and Law*, 17(2), e2301.
- Ministry of ICT, Postal and Courier Services. (2026). *Zimbabwe National Artificial Intelligence (AI) Strategy*. Republic of Zimbabwe. Available: https://veritaszim.net/sites/veritas_d/files/Zimbabwe%20National%20Artificial%20Intelligence%20Strategy.pdf.
- Ministry of Information, Communications, Science, Technology and Innovation. (2025). *Draft Artificial Intelligence Policy Implementation Plan*. Kingdom of Lesotho. Available: https://www.gov.ls/download/draft-artificial-intelligence-policy_1-0/.

- Ministry of Technology and Science. (2025). *National Artificial Intelligence Strategy 2024-2026*. Republic of Zambia. Available: <https://www.mots.gov.zm/wp-content/uploads/2025/02/Zambia-Ai-Strategy-Book-option-2.pdf>.
- Monkam, N. (2024, November 12). African Strategies to Combat Illicit Financial Flows. *Carnegie Endowment for International Peace*. <https://carnegieendowment.org/research/2024/11/illicit-financial-flows-africa-tax>
- Ngcukaitobi, T., Hassim, A., & Williams, K. (2025). *FINAL REPORT OF THE SECTION 59 INVESTIGATION PANEL*.
- P.P.M. and Others v Minister of Home Affairs and Others, ZAGPPHC [2024] ZAGPPHC 2; 2024 (3) SA 469 (GP); 2024 (5) BCLR 703 (GP) (High Court of South Africa, Gauteng Division, Pretoria 2024). <https://www.saflii.org/za/cases/ZAGPPHC/2024/2.html>
- Preferential Procurement Policy Framework Act 5 of 2000*, Republic of South Africa.
- Segun, S. T., Adams, R., Florido, A., Timcke, S., Shock, J., Junck, L., Adeleke, F., Grossman, N., Alayande, A., Kponyo, J. J., Smith, M., Fosu, D. M., Tetteh, P. D., Arthur, J., Kasaon, S., Ayodele, O., Badolo, L., Plantinga, P., Gastrow, M., ... Bissyande, T. (2025). *Toward an African Agenda for AI Safety* (White Paper arXiv:2508.13179). arXiv. <https://doi.org/10.48550/arXiv.2508.13179>
- Sizwe Snail Ka Mtuze & Masego Morige. (2024). TOWARDS DRAFTING ARTIFICIAL INTELLIGENCE (AI) LEGISLATION IN SOUTH AFRICA. *Obiter*, 45(1). <https://doi.org/10.17159/obiter.v45i1.18399>
- Tito Magoti v Attorney General, TZHC [2024] TZHC 1939 (High Court of Tanzania (Dar es Salaam) 2024). <https://tanzlii.org/akn/tz/judgment/tzhc/2024/1939/eng@2024-05-08>
- Uzoigwe, S., & Edward, A. (2026, March). *AI-Driven Errors in Nigerian Banking: Legal Accountability and Data Subject Rights Under the Nigeria Data Protection Act, 2023*. Alliance Law Firm. <https://alliancelawfirm.ng/ai-driven-errors-in-nigerian-banking-legal-accountability-and-data-subject-rights-under-the-nigeria-data-protection-act-2023/>
- Webster, J., & Watson, R. T. (2002). ANALYZING THE PAST TO PREPARE FOR THE FUTURE: WRITING A LITERATURE REVIEW. *MIS Quarterly*, xiii–xxiii.

Wireless Application Service Providers Association of Nigeria (WASPA) v Federal Competition and Consumer Protection Commission (FCCPC), Suit No. FHC/L/CS/720/2026 (Federal High Court, Lagos April 15, 2026). <https://www.lawyard.org/news/federal-high-court-halts-fccpc-digital-lending-regulations/>