

Governing Africa's Digital Infrastructure and Artificial Intelligence for Regional Anti-Corruption and Public Service Delivery

Thomas Angesha*, Catherine Kalondu Mutua, Rosemary Chiedza Mukucha, Naim Shehu

Pan-African University, Institute of Governance, Humanities and Social Sciences (PAUGHSS)

*Corresponding Author

DOI: <https://doi.org/10.47772/IJRISS.2026.100801045>

Received: 07 September 2026; Accepted: 12 September 2026; Published: 23 September 2026

ABSTRACT

Africa's digital transformation is advancing faster than the governance frameworks required to make digital infrastructure and artificial intelligence (AI) accountable, inclusive and effective. This study examines how digital infrastructure and AI interact with anti-corruption efforts and public service delivery across eight African states: Kenya, Ghana, Nigeria, Rwanda, South Africa, Ethiopia, Mauritius, and Egypt. Using an integrative documentary review, the study synthesises findings across digital public infrastructure, AI anti-corruption tools, institutional capacity, and regional governance. A structured comparative coding framework evaluates governance readiness across the target African states using explicit legal, institutional, and technical criteria. The findings reveal a persistent sequencing failure; public administrations deploy AI systems amid uneven connectivity, infrastructure deficits, fragmented administrative systems, skills shortages, and incomplete regulatory frameworks. Digital public infrastructure strengthens traceability and service efficiency when it is supported by data protection laws, institutional oversight and equitable access. The study advances an integrated regional governance framework structured around four reinforcing pillars: enforceable continental standards, interoperable digital public infrastructure, coordinated institutional mandates, and outcome-based monitoring. The study points out that Africa's strategic priority should not be AI deployment in isolation but the deliberate construction of the legal, infrastructural and institutional conditions that make AI governable. Regional coordination through the African Union and Regional Economic Communities remains vital for cross-border data governance, cybersecurity, digital sovereignty and public-sector algorithmic accountability. The study concludes that Africa's digital transformation will deliver sustainable public value only when technological ambition is sequenced with institutional capacity, legal legitimacy and inclusive governance.

Keywords: Digital Infrastructure, Artificial Intelligence, Anti-Corruption, Public Service.

INTRODUCTION

Digital transformation is a core element of modern public governance, altering the efficiency of institutions, transparency and the delivery of public value. This shift means moving from the old manual bureaucratic models to intelligence-driven government (i-Gov) which relies more on automated flows of information and machine learning models in administrative processes and decision-making¹. Artificial Intelligence (AI) has therefore emerged as a strategic tool in the modernisation of public administration². AI enables machines to imitate human cognitive functions like learning, reasoning, and solving problems. In Africa, this transition is underpinned by the African Union's Agenda 2063 and the Digital Transformation Strategy for Africa (2020-2030) that consider digital public infrastructure (DPI) and emerging technologies as drivers of inclusive socio-economic development. Artificial intelligence is believed to have great potential in contributing to the socio-economic transformation of Africa but its impact depends on infrastructure, skills, institutional capacity and governance^{1,2}.

A wide gap separates continental policy ambition from national implementation capacities³. Sub-Saharan Africa is the least prepared region in the world for AI governance with an average score of 32.70 out of 100, ranking lowest globally despite growing adoption in revenue collection, procurement monitoring, and healthcare

logistics^{2,4}. This disparity stems from a sequencing failure as governments deploy advance artificial intelligence systems without the proper foundational infrastructure, such as reliable electricity and broadband connectivity, and basic digitisation^{3,5}. More than 900 million Africans lack internet while the continent accounts for less than 1% of the global data centre capacity. This heightens risks which potentially exclude millions from the Fourth Industrial Revolution (4IR)⁶.

Corruption drains Africa an estimated \$128 billion annually in misused and lost public resources, degrading infrastructure investment and public service delivery. Automated public procurement systems and AI risk models offer mechanisms to detect fraud and trace funds. Unregulated technological deployment creates severe risks of digital colonialism, where foreign entities extract local data to train proprietary algorithms, entrenching dependency⁵. To overcome these risks, requires a digital constitutional order grounded in Ubuntu-based ethics, establishing data as a collective resource, protecting privacy, and enforcing algorithmic accountability with clear citizen redress mechanisms⁷.

Digital identification and mobile financial platforms in Ghana, Kenya and Nigeria have shown promise for strengthening fiscal integrity, including the identification of “ghost workers”, while also revealing risks of digital exclusion without inclusive design^{2,8}. While the number of national AI strategies is increasing, there is still a lack of research on the use of AI in everyday life by administrative staff and the contribution of Africa’s youth, who constitute around 60% of the population^{2,9}. The existing literature treats digital transformation, anti-corruption, and public service delivery as separate topics and pays little attention to the interaction of these topics within the framework of regional integration.

This study therefore explores the role of digital infrastructure and artificial intelligence in improving national and regional anti-corruption efforts while bolstering public service delivery across Africa. It assesses the digital infrastructure and regional services; AI and public sector efficiencies; institutional challenges to adoption; and policy measures for regional cooperation, providing evidence-based guidance for the implementation of the AU Continental AI Strategy during its 2025-2030 time frame and contributing to the vision of “The Africa We Want”.

LITERATURE REVIEW

An integrative documentary review approach is used to synthesise empirical evidence, policy literature and contemporary theory on the governance of Africa’s digital infrastructure and AI for anti-corruption and public service delivery. It contrasts existing and preferred paradigms of global governance with realities of governance in Africa. It explores the relationship between advanced governance concepts and successful anti-corruption and sustainable public service.

Comparative Global AI Governance and the Aspirational African Model

There is a “trilemma” in global AI governance that balances innovation, human rights and security across multiple regulatory ideologies¹⁰. A good example of the rights-based precautionary model is the AI Act of the European Union, which uses a mandated three-tier classification of risks, with mandatory audits and human oversight of high-risk systems¹¹. The United States prioritises market innovation through sector-specific policies to accelerate industry integration, although it occasionally creates legal ambiguity. China employs a state-centric management model focused on national security, while Singapore embeds ethics-by-design into technical protocols to secure public trust. The models reveal a core regulatory trade-off between strict risk prevention and rapid technological adoption^{4,10}.

Regulatory structures determine auditability, administrative accountability, and rule of law outcomes. Empirical evidence across 121 developing nations confirms that e-governance reduces petty corruption by limiting administrative discretion and raising bribe-detection costs. In transition economies, automated service portals decrease direct bribery opportunities by replacing face-to-face interactions. However, unmonitored digital platforms open new vectors for cybercrime, financial fraud, and administrative manipulation¹². Institutional

capacity, regulatory design, and enforcement rigour determine whether digital tools strengthen or undermine public integrity⁵.

A dominant argument among scholars is that the continent needs to develop its own digital and AI governance models that are in harmony with African technological needs, as opposed to transplanting governance models from the Global North. Scholars propose a digital constitutional order grounded on Ubuntu-based ethics, which redefines data as a communal resource and algorithmic accountability as a shared public responsibility^{5,7}. Plantinga et al. (2024), in their survey on laws and legislation, asserted that the existing legal capacities in model management across eight African countries offer foundational leverage for responsible AI model oversight, human supervision, and sector-specific regulation. Effective governance requires polycentric oversight involving judiciaries, civil society groups, and the African Union and regional economic organisations to prevent single-point institutional capture scenarios typical of centralised bureaucracies^{5,13}. Without enforceable legal frameworks, anti-corruption gains remain theoretical.

Digital Public Infrastructure (DPI) in Africa and the Sequencing Paradox

The governance of AI in Africa is crucially dependent on the reliability and security of Digital Public Infrastructure (DPI) such as digital ID, payment systems and data interchange layers⁸. Comparative research across eleven African countries indicates four DPI architectures: identification-led, authentication-led, multiple and payment-led systems, where the interactions between identity and payment layers affect both efficiency and vulnerability to fraud¹⁴. The operation of DPI is an exercise of public authority that must be legally bounded, proportionate, transparent and open to challenge as it integrates identity, payments and data flows across institutions; the more DPI layers are interwoven with tax and welfare administration, the more consequential their legal design becomes for detecting fraud and protecting citizens¹⁵.

Empirical evidence shows a “sequencing paradox or failure”: African states tend to introduce high-level AI applications before broadband, energy reliability and digital reforms are in place, and with low e-government development indices^{5,16}. The Ghana Card is being progressively incorporated into the tax administration in Ghana. This exemplifies the World Bank’s “stacked approach” to DPI, whereby the governance of organised infrastructure produces tangible improvements in administrative efficiency and revenue mobilisation¹⁷. The same systems are also institutional mirrors: Ghana’s digital welfare infrastructure increased health insurance uptake by 14-15 percentage points at the same time as systematically excluding Fulani pastoralists, illustrating how ungoverned DPI exacerbates marginalisation and a transparency deficit in favour of urban elites⁸. Digital public administration in South Africa promotes ethical behaviour and reduces the chance of corruption¹⁸. Remote communities are consistently excluded from the advantages of e-government. Kenya’s drive to centralise services via the eCitizen portal and Huduma centres has reduced delivery timescales from years to weeks. However, consumers with different levels of online literacy are benefiting unevenly¹⁵. Single-registry DPI, streamlined and closed, has opened the space for ghost workers, duplicate claims and identity fraud only where data protection, proportionality and independent oversight are embedded in its governance. Thus, regulated, phased and inclusive DPI is the prerequisite that turns digital infrastructure into an anti-corruption and service delivery asset instead of a new vector of exclusion¹⁷.

Governed AI for Local Anti-Corruption

In the domain of digital infrastructure and AI, they serve as “algorithmic guardians” to reduce systematic corruption when guided by noble values of openness and accountability¹³. The possibility is explained by Eisenhardt’s (1989) Principal-Agent Theory, in which AI lowers the information asymmetry between the public (principals) and the government officials (agents) by offering real-time, auditable logs of the state of actions¹⁹.

But in the absence of strong governance, artificial intelligence may erode accountability through opaque decision pathways, biased outcomes, automation bias and insufficient routes for citizen redress. The institutional capacity of developing states, their procurement maturity and independent oversight differ, increasing the risks¹⁴. A practical risk-based regulatory framework that differentiates between low, medium and high-risk government AI applications and establishes minimum requirements for deployment including named accountability,

oversight by humans, impact assessment, audit trails and redress mechanisms. This framework protects against the indefensible automation of service delivery²⁰. Africa is experiencing such operational challenges. Nigeria has faced various problems such as lack of infrastructure, technological knowledge and lack of institutional capacity to implement systems such as the Treasury Single Account and Integrated Payroll and Personnel Information System²¹. E-governance in Edo State improved service delivery, reduced bureaucratic delays and petty corruption with a relatively small effect on public service²⁰. In Nigerian cities, weak governance and regulatory agencies are hampering the wider adoption of technology. The findings support the argument that constraints to fight corruption in the public sector are more related to weak public reforms and legislative support to promote the adoption of digital and phased implementation rather than mere reliance on external technology deployment^{19,21}. Responsible AI governance requires an institutional architecture for lawful and just service delivery: a model designed based on normative legitimacy, regulatory architecture, institutional capability, operational lifestyle governance and sustainable development alignment¹¹.

Intelligence-Driven Governance Toward Public Service Excellence (i-Gov)

The delivery of sustainable services relies on moving from passive e-government to active intelligence-driven governance (i-Gov), but it requires seven capacity domains: governance and regulation, infrastructure, data, skills, financing and stakeholder engagement, without which AI-enabled services cannot run^{8,19}. The developed world offers both the promise and the prerequisites, such as OECD experience, that strong leadership, comprehensive strategies, and robust legal structures are crucial for proactive citizen-centred digital services, as exemplified by South Korea's "control room" coordination, the United States, and Sweden¹⁹. Estonia and South Korea have also innovated in e-government, resulting in faster processing and higher public satisfaction. The sharing of data in real time and open government have also improved trust and reduced corruption⁴. More than 1,700 government AI use cases in the United States reveal that "assistive" technologies dramatically cut reaction times and workloads, but only when deployment is accompanied by risk-tiered safeguards^{1,18}.

African success stories match similar characteristics where governing competence is present. The Africa-US e-governance partnerships have shown that leadership, stakeholder involvement and capacity building are essential success elements, while the digital divide and insufficient infrastructure remain persistent limitations¹⁵. For example, in South Africa e-government at the municipal level is perceived to encourage ethical behaviour and minimise the risks of corruption, yet poor rural areas are excluded due to a lack of ICT infrastructure and basic online literacy skills¹⁸. Digital inequalities, lack of people with information and communication technologies' skills and resistance to change will impede digital governance in South Africa^{18,21}.

In the same way, the moderate adoption of AI and digitalisation, as undermined by weak online literacy levels, inadequate energy infrastructure and limited regulatory structures in Nigeria, reflects the smart governance agenda that calls for an integrated model linking governance reform, technology deployment and capacity building⁸. The lesson is the same in both hemispheres. I-Gov delivers anti-corruption and service delivery benefits only in the event of controlled and streamlined governance preceding technological ambition¹¹. The Youth Dividend and STEM Gaps in the Fourth Industrial Revolution (4IR) Africa's youth population is a strategic resource for the AI-enabled public sector, but a lack of STEM education, digital infrastructure and AI-related skills structurally limits preparedness for the digital economy⁶.

The digital divide is a major challenge in Nigeria, and the low level of digital competence and energy infrastructure are some of the main barriers to the adoption of smart governance. The barriers to the implementation of e-government at the local level in South Africa are lack of digital competence and ICT staff²². e-Government engagement is hampered by limited ICT infrastructure and digital skills in rural areas. The cost of data and digital illiteracy also pose a challenge to the implementation of e-governance in Nigeria²⁰. Good governance must therefore speak to digital inclusiveness and to the investment in technical literacy and skills development of the next generation of public administrators. If such efforts are not made, the adoption of AI is likely to increase socio-economic disparities, not decrease them^{18,22}.

Literature gaps

While national AI initiatives are proliferating in African countries, there are numerous gaps in the available literature. The first is micro-practice blindness; most of the studies focus on macro policy or technical applications and pay little attention to the day-to-day administrative workflows and institutional culture of African public sector enterprises. Thus, there is no empirical evidence concerning the effectiveness of e-governance in the different contexts of the states². “Another challenge is the absence of data on youth-led innovation. “Young people are strategic assets in the digital era, but there are no real publicly managed initiatives for youth-led innovation in Africa. Moreover, the extent of capture by informal institutions has not been addressed in the literature, nor has the critical testing of literature on the systematic resistance or capture of formal digital governance frameworks by informal norms, patronage networks and bureaucratic inertia¹⁴. Lastly, there is very little research on the conflict of laws when algorithms are created in one jurisdiction but the data is processed in another. This creates accountability gaps for the transnational operation of AI in a world of conflicting global regulatory philosophies.

METHODOLOGY

Study Design

This study uses an integrative documentary review design based on secondary sources, combining thematic synthesis with a structured comparative scoring exercise²³. The design addresses research questions spanning institutional, technological, and normative domains that single empirical studies do not address. Integrative reviews accommodate heterogeneous evidence, combining empirical and theoretical literature to evaluate how Africa’s digital infrastructure and artificial intelligence (AI) governance affect anti-corruption outcomes and public service performance. The analytical framework synthesises empirical evidence on digital public infrastructure, policy analyses of continental frameworks, and economic evaluations of digital investments. This triangulation moves the analyses beyond descriptive accounts, evaluating the institutional conditions under which digital technologies create public value²⁴.

Documentary Population and Sampling

The study population comprises policy documents and secondary literature across the 55 African Union member states. The study area is the African Continental policy terrain comprising the fifty-five member states of the African Union, with analytical depth concentrated on the states that have enacted national AI or digital strategies: Kenya, Ghana, Nigeria, Rwanda, South Africa, Ethiopia, Mauritius, and Egypt. Regional instruments like the AU Continental AI Strategy, Agenda 2063, and the AFCFTA Digital Trade Protocol provide continental context while global comparators including the European Union, the United States, China, and Singapore, enter the review solely as referential benchmarks for contrasting regulatory philosophies, not as units of primary analysis²⁵. The study population comprises the eligible corpus of documents: peer-reviewed empirical studies reporting cross-sectional surveys, longitudinal cohorts, and qualitative case studies; national policy instruments and legislative texts; institutional reports from multilateral organisations; and economic evaluations of digital government investments. The sampling involved purposive selection of policy instruments and systematic database searching in Scopus, Web of Science, ProQuest, SSRN, African Journals Online (AJOL) and Google Scholar, supplemented by grey literature from the African Union, World Bank, United Nations (UN), UNDP, International Telecommunication Union (ITU), Afrobarometer and Transparency International. The search string was Boolean and covered four concept blocks: infrastructure, artificial intelligence and algorithmic governance, anti-corruption and accountability, and public service delivery, and combined with inclusion criteria that required documents to address at least two of the four constructs in an African or comparative governance context and report empirical or policy analytic substance within the publication window. Opinion editorials and purely technical papers without governance implications were excluded, as were studies outside of the scope²⁴.

Data Analysis Approach

Data analysis follows a two-track approach, combining thematic analysis with comparative quantitative scoring. Qualitative findings were coded line-by-line into a structured matrix to identify recurring institutional patterns, policy gaps, and operational barriers across jurisdictions. Retrieved records were screened by title, abstract, and data reduction based on the study objectives, in which extracted findings were coded into a structured matrix, organised thematically for data comparison, as patterns and contradictions across sources were systematically examined for drawing conclusions and verification²⁴.

To evaluate country readiness, the study applies a composite Governance Readiness Score (GRS_i) across the eight target states:

$$GRS_i = 0.40L_i + 0.35I_i + 0.25T_i$$

Governance readiness is operationally defined as the legal, institutional, and technical capacity of a state to deploy public sector AI safely, ethnically, and effectively, and indicators are defined as follows: Legal Readiness (L_i , weight = 0.40) to evaluate binding data protection legislation, national frameworks, statutory privacy rights and algorithmic transparency mandates scored on a continuous scale from 0.00 to 1.00; Institutional Capacity (I_i , weight = 0.35) to measure independent data protection authorities, judicial review capabilities, and anti-corruption agency oversight mechanisms scored on a continuous scale from 0.00 to 1.00, Technical Infrastructure to assess national broadband penetration rates, power grid stability, data centre hosting capacity, and digital ID system interoperability scored on a continuous scale from 0.00 to 1.00. Legal and institutional dimensions receive higher weights because public sector AI requires statutory authorisation, privacy safeguards, and enforceable oversight mechanisms to prevent administrative abuse.

Screening Reliability and Ethical Considerations

Since the documentary corpus functions as the study's analytical sample, screening reliability was validated using Cohen's kappa coefficient (k) $k = \frac{Po - Pe}{1 - Pe}$ between two independent reviewers who evaluated a random 20% sample of retrieved records²⁶. Where Po is the observed proportion of literature and Pe is the expected proportion of the literature by chance. A k of 0.80 or more was considered an acceptable agreement, which for this particular study yielded a stronger inter-rater agreement score of $k = 0.84$, exceeding the standard 0.80 threshold for documentary consistency²⁶. Disagreements during the screening were resolved through joint re-examination of the full source test against the inclusion criteria.

Since the study relies exclusively on publicly accessible secondary data, it required no human-subject ethical approval. Academic integrity standards apply throughout: all sources are fully cited, data extraction reflects original context, and potential publication biases within grey literature are explicitly addressed in the analytical findings.

Documentary Analysis

This section synthesises findings across the corpus using comparative analysis and structured display matrices. The extraction framework organises empirical evidence, legal text, and institutional reports directly against the four research questions. This process links national policy to public sector anti-corruption outcomes and service delivery performance.

State of Digital Infrastructure in Africa

Only eight of 55 AU member states (14.8%) maintain national AI strategies backed by statutory data protection acts. Among these, Mauritius, Rwanda and Egypt demonstrate the most advanced policy and regulatory frameworks. However, even strategy-bearing states rank near the bottom of the Global AI Index metrics on talent, compute infrastructure and policy dimensions. Fragmented administrative capacity and limited regulatory convergence across regional economic communities hinder broader continental adoption²⁷. Regulatory progress

advances primarily where national digital strategies integrate directly with public sector modernisation agendas, as observed in Ghana²⁸

Applying the Governance Readiness Score (GRS_i) matrix to the qualitative corpus converts heterogeneous legal, institutional and technical indicators into standardised comparative metrics across the eight target states. The resulting values reflect actual operational capacity rather than formal policy intent, showing clear stratification across the continent²⁹. High scores correlate directly with centralised AI strategies, independent data protection authorities, and established digital public infrastructure, while lower scores signal structural bottlenecks in statutory enforcement and technical compute power.

For illustration, using $GRS_i = 0.40L_i + 0.35I_i + 0.25T_i$, the score is calculated as follows: as coded for Legal readiness ($L_i = 0.90$), Institutional readiness ($I_i = 0.85$) and Technical readiness ($T_i = 0.80$), giving $GRS_i = 0.86$ out of a full score of 1. The score is a review instrument, not an external ranking. Its emphasis on law and institutions reflects the need for accountable delegation, privacy protection and reviewable decisions in public-sector AI³⁰. Legal and institutional dimensions receive greater weight because AI systems used in public administration requires lawful data use, accountable delegation, independent review and enforceable safeguards.

The coding matrix converts qualitative policy evidence and institutional evaluations into comparable readiness scores across the target states. Table 1 details the final indices, national strategy adoption years, and primary data protection legislation.

Country	AI Strategy Year	Data Protection Law	L_i	I_i	T_i	Composite Score (GRS_i)
Mauritius	2018	2017	0.9	0.85	0.8	0.86
Egypt	2021	2020	0.85	0.8	0.75	0.81
Rwanda	2023	2021	0.85	0.8	0.7	0.8
South Africa	2024	2013	0.8	0.75	0.75	0.77
Ghana	2023	2012	0.75	0.75	0.7	0.74
Kenya	2025	2019	0.75	0.7	0.65	0.71
Nigeria	2024	2023	0.7	0.65	0.6	0.66
Ethiopia	2020	2019	0.6	0.55	0.55	0.57
Mean	—	—	0.77	0.73	0.69	0.74

Legal (L_i), Institutional (I_i), Technical (T_i). **Sources:** Researcher's computation using previous literature

Note. Scores represent researcher calculations based on comparative documentary coding across national policy texts, statutory enactments, and institutional reports.

The GRS distribution across the target states demonstrates clear structural stratification. Mauritius ($GRS_i = 0.86$), Egypt ($GRS_i = 0.81$), and Rwanda ($GRS_i = 0.80$) lead the index, achieving high scores across legal authority and institutional coordination³¹. Strategic prioritisation in these state pairs formalises policy adoption with independent supervisory agencies. Middle-tier states, including South Africa ($GRS_i = 0.77$), Ghana ($GRS_i = 0.74$), and Kenya ($GRS_i = 0.71$), display statutory protections but face institutional fragmentation or technical limitations. Lower scores in Nigeria ($GRS_i = 0.66$) and Ethiopia ($GRS_i = 0.57$) highlight persistent gaps between strategic ambition, operational funding, and technical deployment capacity³².

Legal readiness (L_i , mean = 0.77) consistently outpaces technical infrastructure (T_i mean = 0.69) across all evaluated jurisdictions. States establish comprehensive statutory frameworks, such as data protection acts, faster than they deploy scalable compute capabilities or enterprise broadband networks. However, institutional capacity (I_i , mean = 0.73) creates a secondary bottleneck. Data protection authorities in several states lack financial

independence, specialised staff, and enforcement powers. Without robust enforcement, formal legal protections fail to prevent administrative bias or unauthorised access in public sector deployment³³.

Empirical Benchmark Analysis: E-Government Development Index (EGDI)

The UN e-government Development Index (EGDI) benchmarks public sector digital transformation by calculating the arithmetic mean across three normalised core dimensions: $EGDI_i = \frac{OSI_i + TII_i + HCI_i}{3}$, where OSI_i represents the Online Service Index for evaluating the scope, quality, and accessibility of national public service portals. TII_i represents the Telecommunication Infrastructure Index, measuring broadband penetration, mobile cellular subscriptions and international internet bandwidth, and HCI_i measures the Human Capital Index, assessing adult literacy rates and overall educational enrolment metrics essential for digital participation³⁴.

Evaluating the documentary benchmark value of 0.405 highlights severe structural constraints across African public sector digitisation. Comparing the regional baseline against the global average of 0.610 reveals a relative performance of 33.6%: $(\frac{0.610-0.405}{0.610} \times 100 \approx 33.6\%)$. While 39 of the 55 AU member states maintain statutory data protection legislation, only eight states (14.8%) combine national AI or digital strategies with operational data protection laws. Deficient rural power grids, high data costs, and low digital literacy escalate administrative exclusion¹⁰. These rural population exclusions from e-government appear consistently in empirical studies of South African municipal service delivery, as well as public procurement systems in Ghana and Nigeria. Absent foundational connectivity, automated anti-corruption oversight systems cannot capture the administrative transactions they are designed to police¹⁶.

Table 2 shows the e-government infrastructure indicators and performance benchmarks.

Benchmark Dimension	Africa	Global Benchmark	Relative Gap (%)
States with data protection laws ³⁵	39 of 55 states	-	70.9%
States with dual policy adoption (AI + Data) ^{27,28}	8 of 55 states	-	14.8%
AI-policy pioneers ¹⁹	3 (5.6%)	67.0%	44.8%
EGDI Composite ^{4,36}	≈0.405	0.610	33.6%
Internet penetration rate	≈37.0%	67.0%	44.8%

Sources: Researcher's computation based on the reviewed documents

Toward an Integrated Regional Framework

Synthesising the empirical, legal and technical findings yields a four-pillar regional governance framework designed to move African AI adoption from aspirational policy to enforceable administrative practice. Unlike existing soft-law declarations, this model establishes operational prerequisites that sequence technological deployment behind institutional and legal readiness³. The framework operationalised four interrelated pillars:

Pillar 1: Binding continental legal instruments: converts non-binding declarations into enforceable obligations through standardised data sovereignty, algorithmic accountability and cross-border privacy protocols.

Pillar 2: Interoperable digital public infrastructure: prioritises foundational broadband access, reliable energy grids, and digital identity systems before deploying predictive AI oversight modules.

Pillar 3: Harmonised regional institutional mandates: establishes mutual recognition of digital trust services across regional economic communities, granting independent data protection authorities cross-border supervisory powers.

Pillar 4: Outcome-based monitoring and citizen redress: anchors administrative evaluation in measurable anti-corruption metrics, mandatory algorithmic audits, and statutory avenues for citizens' appeals.

This structure expands upon the AU Continental AI strategy by translating high-level principles into enforceable administrative mandates across member states.

To operationalise the fourth pillar, the framework introduces the Digital Anti-Corruption Effectiveness Index (DAEI), a composite metric measuring the administrative impact of public sector AI deployment. Governance components and operational dimensions are defined as follows: public service coverage ($C = 0.35$), data integrity ($D = 0.30$), and algorithmic accountability ($A = 0.25$) against human rights and privacy risk ($R = 0.20$):

$$DAEI = 0.30C + 0.25D + 0.25A - 0.20R$$

Applied illustratively, states with high GRS and connected infrastructure may exhibit conditions for DAEI scores above 0.60, whereas low-readiness states where connectivity, data governance, and accountability are jointly absent cannot credibly exceed 0.30 without sequenced investment³⁷. The analysis suggests that good, regulated and streamlined governance of digital infrastructure and AI constitutes the conversion mechanism through which technology becomes a sustainable anti-corruption and service-delivery asset rather than a parallel channel for rent-seeking.

DISCUSSION OF RESULTS

Government Digital Infrastructure and Regional Public Services

The empirical findings confirm that digital infrastructure serves as the essential substrate for public sector modernisation, administrative transparency, and regional integration across Africa. Foundational systems including broadband networks, cloud facilities, interoperable digital identity databases, and electronic payment gateways directly dictate state capacity to deliver public services across the eight target nations evaluated, including Kenya, Ghana, Rwanda, and South Africa⁸. Translating physical connectivity into automated public administration requires structural legal frameworks, supervisory capacity, and sustained political leadership, directly reinforcing the theoretical models of state capacity established in the literature review. Within the Governance Readiness Score framework ($GRS_i = 0.40L_i + 0.35I_i + 0.25T_i$) outlined in the methodology, technical infrastructure (T_i) carries a weight of 0.25, demonstrating that expanding hardware without primary legal (L_i) and institutional (I_i) readiness fails to deliver measurable anti-corruption outcomes or improve administrative delivery³⁴.

Established literature confirms a positive relationship between digital infrastructure and governance results when paired with structural administrative reforms. Digital public infrastructure (DPI) creates shared technical protocols across public agencies, departing from the legacy model of fragmented, siloed digital projects. For example, integrating the Ghana Card into national public administration databases generated concrete efficiency gains by expanding health insurance registration by 14 to 15 percentage points while eliminating fraudulent payees from civil service payrolls³⁸. Centralising service delivery through Kenya's eCitizen platform similarly reduced administrative processing times from weeks to days while making public transactions traceable, thereby eliminating discretionary spaces where informal fee extraction typically thrives. Mismanaged digital infrastructure produces structural risks, including administrative exclusion, unauthorised state surveillance, and entrenched digital inequality³⁹. This operational hazard directly aligns with the empirical weighting in the Governance Readiness Score (GRS_i), where Legal Readiness (L_i , 0.40) and Institutional Capacity (I_i , 0.35) together constitute 75% of total state readiness, demonstrating that technical infrastructure alone cannot guarantee equitable governance.

Empirical evaluation reveals pronounced disparities in technical infrastructure across the sampled African states. Top-tier performers identified in the empirical sample include Mauritius, Rwanda, Kenya, South Africa, and Egypt demonstrating advanced broadband penetration, integrated e-government portals, and scalable digital identity registries. Lower-tier states exhibit severe structural constraints, characterised by restricted broadband coverage, erratic electrical grid power, prohibitive data costs, and limited public digital literacy⁸. Expanding connectivity across underserved rural regions requires targeted capital allocation into shared network infrastructure. Persistent capital deficits restrict universal access and create divergent governance outcomes,

leaving states with low Technical Infrastructure scores (Ti) structurally incapable of deploying automated public services or supporting complex digital transformation initiatives³.

Deploying artificial intelligence across foundational digital infrastructure unlocks advanced capabilities in predictive analytics, automated decision-making, fraud detection, healthcare delivery, urban management, border security, judicial processing, and revenue administration. Automated systems present operational risks, including algorithmic opacity, arbitrary administrative discretion, training data bias, and compromised public accountability, particularly in jurisdictions with weak statutory protections⁴⁰. Digital sovereignty presents an additional operational challenge for African public administration. Reliance on foreign data centers, proprietary software, external cloud platforms, and multinational technology vendors create severe vulnerabilities regarding data ownership, national cybersecurity, and strategic autonomy³. Addressing these dependencies requires African states to build sovereign computing infrastructure, robust domestic regulatory frameworks, and local innovation ecosystems. Strengthening local cloud infrastructure and data sovereignty directly elevates Technical Infrastructure (Ti) and Institutional Capacity (Ii) scores across the empirical sample, securing the sovereign control required for sustainable public sector AI deployment.

Fragmented national systems create operational bottlenecks to African regional integration, underscoring the necessity of coordinated cross-border governance. Key regional agreements analysed in the literature review include the African Continental Free Trade Area (AfCFTA), the AU Digital Transformation Strategy (2020–2030), the AU Data Policy Framework, and the Continental AI Strategy explicitly establish digital interoperability as a prerequisite for economic integration³⁹. Standardising digital protocols, establishing cross-border digital identity verification, integrating payment clearinghouses, harmonising cybersecurity regulations, and coordinating data governance directly accelerate trade flows, labour mobility, financial inclusion, and regional public service delivery³⁹. Aligning national legal structures (Li) with continental guidelines converts fragmented domestic systems into an integrated regional digital economy. Adopting an integrated, four-pillar governance framework ensures that digital transformation advances sustainable development without worsening existing administrative disparities across states.

AI, Anti-corruption, Public Sector Efficiency

Artificial intelligence plays an increasingly critical role in expanding anti-corruption operations and improving public sector efficiency across African public administrations. Governments, anti-corruption agencies, and research institutions deploy machine learning algorithms, natural language processing, and predictive analytics to detect fraudulent transactions, monitor public procurement, analyse financial registries, and secure whistleblower platforms⁴¹. This shift moves national anti-corruption strategies from reactive investigations to predictive risk prevention before financial losses occur. Automated algorithms process massive administrative datasets, including procurement bids, customs declarations, tax returns, civil service payrolls, and public expenditure ledgers, to isolate systemic anomalies and flag high-risk transactions²⁰. Supervised machine learning models evaluate behavioural and organisational indicators to help anti-corruption institutions target investigative resources effectively. Rather than supplanting human oversight, automated systems supplement human investigators by identifying complex patterns that bypass manual reviews¹².

Public procurement represents a primary expenditure channel highly vulnerable to administrative corruption, making it an ideal deployment case for predictive AI monitoring systems. Automated monitoring algorithms detect irregular bidding patterns, long agency supplier relationships, inflated contract valuations, hidden conflicts of interest, and bid-rigging cartels²⁰. AI-enabled whistleblower platforms enhance public participation by reviewing incoming complaints, filtering duplicate submissions, prioritising urgent allegations, tracking emerging corruption schemes, and safeguarding informant identities through encrypted networks. Empirical observations from South Africa, Kenya, and Ethiopia confirm that digital reporting platforms increase civic engagement and improve institutional response times. Deployers must balance top-down, state-controlled algorithms with bottom-up civil society systems to prevent state surveillance, political targeting, or algorithmic bias rooted in incomplete or historically skewed training data³.

Generative AI offers specialised capabilities for integrity institutions by accelerating document analysis, legal research, complaint processing, risk assessment, and policy evaluation. Generative systems significantly reduce administrative overhead and standardise investigative procedures across regulatory bodies. Operating reliance on generative models introduces technical vulnerabilities, including algorithmic hallucinations, data security breaches, cybersecurity risks, and automated misclassification³⁹. Mitigating these vulnerabilities requires binding legal frameworks ($L_i = 0.40$) and independent administrative oversight ($I_i = 0.35$), ensuring human scrutiny remains central to all automated decision-making. These legal and institutional safeguards constitute 75 percent of the overall Governance Readiness Score ($GRS_i = 0.40L_i + 0.35I_i + 0.25T_i$), proving that technical deployment without regulatory control remains structurally ineffective.

Deploying AI tools effectively depends entirely on trustworthy underlying digital infrastructure and well-prepared administrative institutions. High-performing AI models require reliable broadband connectivity, cloud computing infrastructure, secure digital identity systems, and unified government databases³. In many African states, structural bottlenecks, including fragmented databases, paper-based records, inconsistent data standards, grid instability, and civil service skills deficits, restrict the operational benefits of AI³. Since corruption schemes frequently operate across international borders through illicit financial flows and tax evasion, regional collaboration under the African Union and AfCFTA framework is essential. Establishing cross-border data-sharing rules, joint cybersecurity standards, and legal algorithmic accountability converts fragmented domestic efforts into a unified regional defence against corruption. Artificial intelligence serves as an operational tool rather than a standalone solution, leaving prosecution, judicial independence, and political accountability as the ultimate responsibility of human institutions.

Institutional Barriers to Digital Transformation

Institutional and governance deficits represent the primary structural bottlenecks restricting the deployment of digital infrastructure and artificial intelligence across African public sector organisations. Technological innovation fails to produce administrative efficiency when implemented within environments lacking formal governance arrangements, supervisory capacity, and regulatory enforcement³. Public sector organisations encounter persistent implementation challenges rooted in low administrative readiness, severe shortages of specialised technical professionals, and fragmented civil service capabilities⁴². Many electronic governance projects collapse not from physical technological failures, but because public institutions lack the structural capacity to sustain operations³⁹. Furthermore, national AI policy formulation across African states remains inconsistent, leaving implementation haphazard and heavily reliant on external frameworks unsuited to domestic administrative realities. Inter-agency fragmentation exacerbates these operational failures, as ministries routinely operate on disconnected software platforms with minimal data integration. Since effective artificial intelligence relies on unified, high-quality administrative data, this operational silo structure prevents automated predictive platforms from functioning effectively¹⁰.

Compounding institutional challenges include political instability, shifting policy priorities across state administrations, corrupt procurement practices, weak civil service accountability, low public digital literacy, and severe financial constraints³. Given that digital initiatives require long-term political continuity and sustained capital investment, administrative turnover frequently disrupts multi-year technology projects. Heavy reliance on foreign technology vendors, external cloud hosting, and proprietary software raises immediate questions regarding national digital sovereignty, institutional autonomy, and long-term state authority³⁹. Mitigating these risks requires establishing localised innovation ecosystems, regional cloud data centres, and contextually relevant governance frameworks to secure sovereign control over public administration data. These institutional requirements validate the empirical weighting within the Governance Readiness Score ($GRS_i = 0.40L_i + 0.35I_i + 0.25T_i$), where Institutional Capacity ($I_i = 0.35$) and Legal Readiness ($L_i = 0.40$) together form 75 percent of overall state readiness. Establishing independent oversight, transparent procurement rules, and robust legal protections pre-emptively ensures digital transformation delivers sustainable public value rather than expanding state surveillance or administrative inequality⁴³.

CONCLUSION AND RECOMMENDATION

Conclusion

This study confirms that digital infrastructure forms the technical backbone of modern government and regional integration across Africa, though its impact on governance outcomes remains strictly conditional. Evidence synthesised across target nations demonstrates that broadband networks, digital identity registries, and electronic payment systems enhance tax collection, public procurement, and social protection when accompanied by robust institutional quality, statutory regulatory capacity, and sustained political commitment. Shifting from siloed electronic applications to interoperable Digital Public Infrastructure (DPI) provides a lasting governance approach by enabling multiple public services to operate on shared platforms³⁸. However, ungoverned DPI creates new vectors for administrative exclusion and state surveillance, proving that physical infrastructure expansion must be matched with primary data protection laws and independent oversight rather than pursued as an isolated goal.

The composite Governance Readiness Score ($GRS_i = 0.40L_i + 0.35I_i + 0.25T_i$) exposes severe structural divides across the region, contrasting high-readiness nations like Mauritius ($GRS_i = 0.86$), Egypt ($GRS_i = 0.81$), and Rwanda ($GRS_i = 0.80$) with lower-tier performers like Ethiopia ($GRS_i = 0.57$). A closer look at the empirical data explains why this gap persists: while 39 of 55 African Union member states have passed data protection laws, only eight states (14.8) pair national AI strategies with active data protection authorities. Furthermore, Africa's average UN e-Government Development Index score (EGDI = 0.405) trails the global benchmark (0.610) by 33.6, exposing a widespread "sequencing paradox" where public sector agencies attempt to deploy advanced artificial intelligence applications amid unstable power grids, weak broadband access, and high data costs³.

In public integrity operations, artificial intelligence acts as an algorithmic guardian, running machine learning models across procurement records, tax registers, and payrolls to expose information gaps through auditable records. Empirical evidence from South Africa, Kenya, Ghana, and Nigeria proves that automated risk models, integrated ID platforms, and single-window portals like eCitizen effectively uncover ghost workers, flag bidding cartels, and accelerate service delivery⁸. However, without independent judicial oversight, mandatory human review, and statutory redress, unmonitored algorithms risk automating administrative bias, deepening discrimination, or expanding state surveillance. AI serves strictly as an analytical tool, leaving prosecution, judicial independence, and political accountability as non-delegable human responsibilities.

Bridging Africa's digital divide requires resolving key structural barriers, including administrative silos, civil service skill deficits, low rural literacy, and mismatched foreign legal models. Regional alignment through the AU Continental AI Strategy, the AfCFTA Digital Trade Protocol, and the AU Data Policy Framework establishes the unified standards, cross-border data governance, and cybersecurity protocols necessary to overcome these national limits²⁸. Ultimately, sustainable transformation relies on three core pillars: legal legitimacy, Ubuntu-centred ethical integrity, and administrative adaptability to ensure AI fosters accountable, inclusive public governance.

Recommendations

Establishing Binding Statutory Frameworks

African states must formulate comprehensive national policies and legislative frameworks on artificial intelligence aligned with the AU Continental AI Strategy while tailored to domestic administrative realities. These statutory frameworks must establish mandatory requirements for algorithmic transparency, institutional accountability, human oversight, and public interest utilisation. Core public sector deployment domains include procurement monitoring, tax administration, civil service payroll cleanup, policing, and social protection systems.

Establishing these binding statutory safeguards directly operationalises the Legal Readiness indicator ($L_i = 0.40$), which carries the single highest weight in the Governance Readiness Score (GRS_i). Empirical evidence demonstrates that technology deployment preceding legal reform consistently fails. Expanding physical digital infrastructure without primary legal controls cannot suppress systemic corruption or improve administrative service delivery across state institutions.

Sequencing and Infrastructure Investments

Governments must concurrently target capital investments into interoperable digital public infrastructure, prioritising reliable power, enterprise broadband access, and universal civil registries before scaling AI-driven public services. This phased, stacked approach to Digital Public Infrastructure (DPI) prevents superimposing advanced algorithms on fragile baseline infrastructure. Key priority areas include national payment gateways, secure data exchange protocols, continuous electrical grid infrastructure, and domestic cloud services.

Strengthening these foundational assets elevates the Technical Infrastructure score ($T_i = 0.25$), bridging the gap between top-tier performers like Mauritius, Rwanda, and Kenya and lower-tier states struggling with connectivity deficits. Physical deployments require clear, enforceable primary legislation governing data protection, cross-border data transfers, data minimisation, and authorised database access.

Compliance, Oversight, and AI-Driven Anti-Corruption Deployment

Building on single-window digital portals like Kenya's eCitizen and Ghana's integrated ID registries, high-risk public AI applications require strict compliance protocols. Agencies must mandate compulsory technical documentation, systematic audit trails, pre-deployment impact assessments, algorithmic explainability, mandatory human review, formal complaint channels, and legal redress mechanisms to protect civil rights. Low-risk and limited-scope public sector AI applications should be limited initially to fraud detection, procurement anomaly flags, and administrative case triage where human supervision and independent review are maintained for consequential decisions.

Public sector artificial intelligence requires independent oversight by data protection authorities, supreme audit institutions, specialised AI ethics commissions, and parliamentary review committees. To mitigate operational risks, public agencies should utilise controlled regulatory sandboxes and phased pilot deployments. Testing low-risk applications, such as document automation, fraud detection algorithms, judicial case triage, and service routing, allows states to evaluate systems before executing full-scale national implementations.

Institutional Capacity, Subnational Inclusion, and Ubuntu Ethics

Building sustainable institutional capacity ($I_i = 0.35$) necessitates continuous public sector investment in civil service digital skills. Priority areas include AI literacy, cybersecurity protocols, algorithmic accountability, and specialised technical training for public workers, auditors, regulators, and data protection officers. Resolving internal skill shortages and coordinating inter-ministerial digital governance bodies eliminates administrative silos and ensures that anti-corruption machine learning models operate with long-term efficacy rather than collapsing due to institutional neglect.

Local and subnational authorities must treat rural connectivity and digital proficiency as prerequisites for equitable service delivery rather than as secondary byproducts of digital reform. Digital expansion without inclusive design widens the urban-rural divide, providing convenience to connected populations while further marginalising underserved communities. Grounding technology governance in Ubuntu ethics redefines data as a collective public resource, establishes algorithmic accountability as a shared public responsibility, and protects citizens against automated bias and administrative exclusion.

Regional Governance, Integration, and Digital Sovereignty

At the regional level, the African Union and Regional Economic Communities must turn the AU Continental AI Strategy into a concrete coordination mechanism by harmonising technical protocols, procurement guidelines,

data governance frameworks, cybersecurity rules, and public sector AI standards to overcome cross-border administrative bottlenecks. Establishing regional observatories and shared repositories to archive model legislation, open-source software applications, procurement techniques, and empirical anti-corruption outcomes will accelerate knowledge transfer across member states. As corruption often transcends national borders through illicit financial flows and procurement cartels, regional bodies must emphasise joint investigative frameworks and cross-border data sharing.

Governments and international development partners must fund African universities, research institutions, technology startups, and regional innovation hubs to build contextually relevant, multilingual, and cost-effective AI solutions. Investing in regionally owned AI capabilities addresses persistent digital sovereignty risks and reduces reliance on foreign data infrastructure. These targeted interventions accelerate economic integration under the AfCFTA framework, improve public service delivery, and guarantee that automated systems advance accountable, inclusive governance across Africa.

REFERENCES

1. African Union. The digital transformation strategy for Africa (2020–2030). (2020).
2. Mickson, M. K., Zilevu, T. K., Asamoah, E. & Kubi, M. AI integration into public administration in Africa: navigating complexities, inclusion, and institutional gaps. *ShodhKosh J. Vis. Perform. Arts* 7, (2026).
3. Plantinga, P. et al. Responsible artificial intelligence in Africa: towards policy learning. *Data Policy* 6, e72 (2024).
4. United Nations, U. N. D. of E. and S. A. United Nations E-Government Survey 2024: Accelerating Digital Transformation for Sustainable Development - With the Addendum on Artificial Intelligence. (United Nations, 2024). doi:10.18356/9789211067286.
5. Kafoe, A. S., Foh, B. M. & Kafoe, M. A. Beyond Panacea: Digital Governance, AI, and the Political Economy of Public Benefit in African Development. *Public Gov. Regul. Law* 2, 1–20 (2026).
6. Mhlanga, D. The Fourth Industrial Revolution and COVID-19 Pandemic in South Africa: The Opportunities and Challenges of Introducing Blended Learning in Education. *J. Afr. Educ.* 2, 15–42 (2021).
7. Langat, S. K., Mwakio, P. M. & Ayuku, D. How Africa Should Engage Ubuntu Ethics and Artificial Intelligence. *J. Public Health Int.* 2, 20–25 (2020).
8. Dzreke, S. S., Dzreke, S. E., Dzreke, E. & Dzreke, F. M. Digital ID as a governance game-changer in African democracies: A comparative analysis of Ghana, Nigeria, and India. *Adv. Res. J.* 8, 82–102 (2025).
9. Yilma, K. & Wodajo, K. Strategy as governance: the governance of AI in Africa. *Sci. Public Policy* 53, 236–244 (2026).
10. Walter, Y. Managing the race to the moon: Global policy and governance in Artificial Intelligence regulation—A contemporary overview and an analysis of socioeconomic consequences. *Discov. Artif. Intell.* 4, 14 (2024).
11. Ismail, O. & Ahmad, N. Ethical and Governance Frameworks for Artificial Intelligence: A Systematic Literature Review. *Int. J. Interact. Mob. Technol. IJIM* 19, 121–136 (2025).
12. Odilla, F. Unfairness in AI Anti-Corruption Tools: Main Drivers and Consequences. *Minds Mach.* 34, 28 (2024).
13. Walle, Y. M., Asifaw, B. G. & Abreha, H. The dual role of AI in whistleblowing systems for anti-corruption in Africa. *Discov. Artif. Intell.* 6, 553 (2026).
14. Sampaio, I. G. B., Bernardini, F. C. & Viterbo, J. Challenges in Addressing the Ethical Aspects of Artificial Intelligence to Detect Fraud in Public Procurement Processes. in *Anais da I Conferência Latino-Americana de Ética em Inteligência Artificial (LAAI-Ethics 2024)* 13–16 (Sociedade Brasileira de Computação - SBC, Brasil, 2024). doi:10.5753/laai-ethics.2024.32440.
15. Banda, L. G. & Du Plessis, D. J. The contingent role of state capacity on the impact of e-government on environmental sustainability in developing countries. *Front. Polit. Sci.* 6, 1459973 (2024).

16. Mhlanga, D. Using artificial intelligence to improve governance and public services in Africa. *Front. Big Data* 9, 1835663 (2026).
17. Ajuzieogu, U. C. Cross-Disciplinary AI Impact Assessment for African Contexts: A Comprehensive Research Framework. (2017).
18. Masiya, T., Lubinga, S. & Musekiwa, T. Barriers to Digital Inclusion in Service Delivery in South Africa: a Systematic Review. *Int. J. Electron. Gov.* 17, 10070710 (2025).
19. Cojocar, A. Governing AI with trust: an adaptive framework for institutional legitimacy in the UK public sector. *Transform. Gov. People Process Policy* 1–22 (2025) doi:10.1108/TG-05-2025-0125.
20. Ayobami, A. T., Mike-Olisa, U., Chidera Ogeawuchi, J., Abayomi, A. A. & Agboola, O. A. Algorithmic Integrity: A Predictive Framework for Combating Corruption in Public Procurement through AI and Data Analytics. *J. Front. Multidiscip. Res.* 4, 130–141 (2023).
21. Sadik-Zada, E. R., Gatto, A. & Niftiyev, I. E-government and petty corruption in public sector service delivery. *Technol. Anal. Strateg. Manag.* 36, 3987–4003 (2024).
22. Mwesha, N. M., Koome, P. & Wachira, T. W. Exploring the Potential of Digital Technology in Addressing Youth Unemployment in Africa: A Scoping Review of Literature. *Afr. Multidiscip. J. Res.* 1, 489–503 (2025).
23. Flynn, R., Stevens, B., Bains, A., Kennedy, M. & Scott, S. D. Identifying existing approaches used to evaluate the sustainability of evidence-based interventions in healthcare: an integrative review. *Syst. Rev.* 11, 221 (2022).
24. Øvrebø, L. J., Dyrstad, D. N. & Hansen, B. S. Assessment methods and tools to evaluate postgraduate critical care nursing students' competence in clinical placement. An integrative review. *Nurse Educ. Pract.* 58, 103258 (2022).
25. De Vries, J. et al. Regulation of genomic and biobanking research in Africa: a content analysis of ethics guidelines, policies and procedures from 22 African countries. *BMC Med. Ethics* 18, 8 (2017).
26. Volk-Jesussek, Dr. H. Cohen's Kappa: Measuring Inter-Rater Agreement. Cohen's Kappa: Measuring Inter-Rater Agreement - numiqo <https://numiqo.com/tutorial/cohens-kappa> (2026).
27. Bangura, S. & Lourens, M. E. A Comparative Analysis of AI HRM Governance Approaches Across African Countries: Continental Patterns and Divergences. *F1000Research* 15, 1051 (2026).
28. Njoroge, J. W. POTENTIAL ROLE OF AFRICAN UNION IN DEVELOPMENT OF AI GOVERNANCE ACROSS THE CONTINENT. *Eur. J. Soc. Sci. Stud.* 10, (2024).
29. Alabani, K., Afful, B., Taale, F. & Abokyi, E. Assessing the performance of national innovation systems (NIS) in Sub-Saharan Africa. *Discov. Glob. Soc.* 4, 43 (2026).
30. Ebers, M., Tupay, P. K., Juksaar, J. & Kohv, K. The Promise and Perils of AI and ML in Public Administration. in *Artificial Intelligence and Machine Learning Powered Public Service Delivery in Estonia* (eds Ebers, M. & Tupay, P. K.) vol. 2 7–33 (Springer International Publishing, Cham, 2023).
31. Vásquez, N. P. & Oja, L. A Change of Narrative: Protecting Sexual and Reproductive Rights in Post-Conflict Criminal Justice. *Columbia J. Gend. Law* 43, 31–66 (2023).
32. Rodima-Taylor, D. Grassroots Data Activism and Polycentric Governance. in *Global Digital Data Governance* 68–87 (Routledge, London, 2024). doi:10.4324/9781003388418-6.
33. Mišić, J., Van Est, R. & Kool, L. Good governance of public sector AI: a combined value framework for good order and a good society. *AI Ethics* 5, 4875–4889 (2025).
34. Das, A., Singh, H. & Joseph, D. A longitudinal study of e-government maturity. *Inf. Manage.* 54, 415–426 (2017).
35. Davis, T. & Trott, W. The regulation of artificial intelligence through data protection laws: Insights from South Africa. *Afr. J. Priv. Data Prot.* 1, (2024).
36. United Nations. E-resilience through e-government: Global and regional perspectives. in *United Nations E-Government Survey 2018* 47–65 (UN, 2018). doi:10.18356/7d337b92-en.
37. Forghani Bajestani, M., Moeini Gharagozloo, M. M. & Li, S. Digital Technologies: Anti or Pro Corruption? *J. Glob. Inf. Technol. Manag.* 27, 182–199 (2024).
38. OECD. AI governance in Africa. Artificial Intelligence Case Studies series https://www.oecd.org/en/publications/oecd-artificial-intelligence-case-studies_c517fcf5-en/ai-governance-in-africa_1ff55135-en.html (2026).
39. Kebe, T. & Ouedrago, B. I. Africa's Digital Transformation Fosters SDGs and Agenda 2063. (2024).

-
40. Schmitz, A. & Zeleznikow, J. Intelligent Legal Tech to Empower Self-Represented Litigants. *Sci. Technol. Law Rev.* 23, 142–191 (2022).
 41. Odilla, F. Bots against corruption: Exploring the benefits and limitations of AI-based anti-corruption technology. *Crime Law Soc. Change* 80, 353–396 (2023).
 42. Shibambu, A. Transformation of digital government services in the public sector in South Africa. *Afr. Public Serv. Deliv. Perform. Rev.* 12, a753 (2024).
 43. Sachs, J., Kroll, C., Lafortune, G., Fuller, G. & Woelm, F. *Sustainable Development Report 2021*. (Cambridge University Press, 2021). doi:10.1017/9781009106559.