

AI Assurance and Accountability in Africa: A Legal Framework for Military Intelligence, Security, and Economic Forecasting.

Remy Takang, LLM, MSc, CAIO, DPO

Member, Cameroon Bar Association

Founder: RTivara Advisory

Email: r.takang@rtivara-advisory.com

Abstract

African states are increasingly deploying artificial intelligence in military intelligence, security operations, and economic forecasting, yet legal systems still lack adequate mechanisms to verify whether such systems comply with human rights standards, public law duties, and institutional accountability requirements. This paper addresses that gap by asking what evidence states and institutions must produce to demonstrate that AI deployment is lawful, necessary, proportionate, traceable, and subject to meaningful oversight.

The paper develops an original African Legal AI Assurance Framework organised around five pillars: legal authorisation and purpose limitation; risk-tiered impact assessment; evidentiary traceability and documentation; independent audit and certification; and remedy and judicial review. It applies this framework to high-stakes public uses of AI in Nigeria, Kenya, South Africa, Rwanda, Egypt, Morocco, and Cameroon, with particular attention to military modernisation, border surveillance, and fiscal forecasting.

Using comparative doctrinal analysis, documentary case studies, and international standards, the paper shows that existing African instruments, including the AU Continental Artificial Intelligence Strategy and the Malabo Convention, provide important policy direction but do not yet constitute a robust assurance regime. The paper also draws on UNESCO's Recommendation on the Ethics of Artificial Intelligence, ISO/IEC 42001, OHCHR guidance, and the IMF's AI Preparedness Index to identify practical safeguards that African legislatures, looregulators, procurement authorities, and courts can adapt.

The paper concludes that Africa's AI governance challenge is increasingly one of enforceable accountability rather than policy aspiration. The proposed framework offers a doctrinally grounded and institutionally practical basis for regulating high-risk AI in the public sector while anchoring oversight in legality, proportionality, transparency, and remedy.

1. Introduction

Artificial intelligence is no longer a peripheral tool in African public governance; it is being written directly into the architecture of the state. Nigeria's Ministry of Defence has signed a USD 190 million agreement for a Multi-Domain Hybrid Intelligence Shield that fuses drone, radar and sensor data into a single AI-driven command picture¹, while its navy has begun

¹'Nigeria Shifts to Algorithmic Warfare with New AI Defence System Deployment'

integrating AI into navigation, threat detection and fleet management². Kenya is deploying artificial intelligence, biometrics and drones along its borders and has committed, under a national strategy running to 2030, to embed AI across security and public administration³⁴. South Africa's National Treasury and central bank increasingly rely on machine-learning nowcasting and municipal distress-prediction models to steer fiscal policy⁵⁶. Rwanda, Egypt and Morocco are, in different ways, folding AI into intelligence services, defence modernisation and continental diplomacy⁷⁸⁹.

This proliferation has outpaced the legal instruments meant to govern it. The African Union's Continental Artificial Intelligence Strategy, endorsed in July 2024, is deliberately non-binding and development-focused¹⁰; the Malabo Convention, Africa's only continent-wide instrument touching cybersecurity and data protection, entered into force only in June

Technology Times (Lagos, 13 May 2026) <<https://technologytimes.ng/nigeria-shifts-to-new-ai-defence-system/>> accessed 13 July 2026.

²'Nigerian Navy Plans for Technology-Driven Fleet' Africa Defense Forum (7 July 2026) <<https://adf-magazine.com/2026/07/nigerian-navy-plans-for-technology-driven-fleet/>> accessed 13 July 2026.

³'Kenya Unveils Border Security Modernization with Drones, Biometrics, and AI' (ID Tech, 4 September 2025) <<https://idtechwire.com/kenya-unveils-border-security-modernization-with-drones-biometrics-and-ai/>> accessed 13 July 2026.

⁴Kenya Ministry of Information, Communications and the Digital Economy, National Artificial Intelligence Strategy 2025–2030 (2025) <<https://ict.go.ke/sites/default/files/2025-03/Kenya%20AI%20Strategy%202025%20-%202030.pdf>>

⁵'Forecasting Municipal Financial Distress in South Africa: A Machine Learning Approach' (2026) 8 Forecast (MDPI) <<https://doi.org/10.3390/forecast8010018>>

⁶'GDP Nowcasting with Machine Learning: Evaluating Forecast Accuracy for South Africa during Economic Crises' ScienceDirect (7 July 2026) <<https://www.sciencedirect.com/science/article/abs/pii/S0313592626002456>> accessed 13 July 2026.

⁷'Integrating Artificial Intelligence into African Defence Strategy' (Military Africa, 10 September 2025) <<https://www.military.africa/2025/09/integrating-artificial-intelligence-into-african-defence-strategy/>> accessed 13 July 2026.

⁸'Egypt and Rwanda Move to Build African AI Partnership' (Middle East Observer, 29 June 2026) <<https://meobserver.news/technology/2026/06/29/egypt-and-rwanda-move-to-build-african-ai-partnership/>> accessed 13 July 2026.

⁹'Morocco Designs Its New Generation of Intelligence for 2030' Atalayar (19 August 2025) <<https://www.atalayar.com/en/articulo/politics/morocco-designs-its-new-generation-of-intelligence-for-2030/20250819090017217548.html>> accessed 13 July 2026.

¹⁰African Union, 'Continental Artificial Intelligence Strategy' (endorsed by the AU Executive Council, 45th Ordinary Session, Accra, 18–19 July 2024) <https://au.int/sites/default/files/documents/44004-doc-EN-Continental_AI_Strategy_July_2024.pdf> ('AU Continental AI Strategy').

2023 and remains unratified by several major economies, including South Africa¹¹; and no African state has yet adopted a binding, sector-specific statute governing the use of AI in defence, security or fiscal decision-making. The result is a widening gap between the operational reality of algorithmic governance and the doctrinal apparatus—legality, necessity, proportionality, traceability, oversight and remedy, that public law has historically used to discipline the exercise of state power.

This paper asks how that gap can be closed. It examines the existing African legal and policy architecture for AI, situates it against international assurance standards, and tests both against three clusters of practice: Nigerian military AI, Kenyan and South African security and fiscal AI, and a comparative set of additional deployments across Rwanda, Egypt and Morocco. From this analysis it proposes an African Legal AI Assurance Framework built on five pillars, and it sets out how that framework might be implemented and enforced through procurement law, incident reporting, audit and judicial review.

The paper's contribution is threefold. First, it demonstrates that the AU's strategic instruments, while valuable as policy signals, do not by themselves constitute an assurance regime capable of producing evidentiary trails, audit rights or remedies for affected persons. Second, it shows that the case-study jurisdictions are moving fastest in precisely the domains—military intelligence, border security and fiscal forecasting—where accountability gaps are most consequential and least studied. Third, it offers a doctrinally grounded, evidence-based framework that African legislatures, regulators and procurement officers can adapt to close those gaps without stalling the continent's legitimate ambition to build indigenous AI capacity¹³.

The remainder of the paper proceeds as follows. Section 2 sets out the conceptual and doctrinal foundations of AI assurance. Section 3 maps the African legal and policy framework. Section 4 turns to comparative international standards. Section 5 explains the methodology. Section 6 presents the case studies. Section 7 proposes the African Legal AI Assurance Framework. Sections 8 and 9 address implementation, enforcement and policy implications, and Section 10 concludes.

2. Conceptual and Doctrinal Foundations

'AI assurance' is used here to mean the combination of technical, organisational and legal measures by which a state or an oversight body can verify, before and after deployment,

¹¹African Union Convention on Cyber Security and Personal Data Protection (adopted 27 June 2014, entered into force 8 June 2023) ('Malabo Convention').

¹²*ibid*, noting that South Africa has not ratified the Convention.

¹³AU Continental AI Strategy (n 10).

that an AI system used in the exercise of public power behaves as intended, remains within its authorised purpose, and can be traced, audited and challenged. Assurance is therefore narrower than 'AI governance', which encompasses the whole ecosystem of strategy, investment and skills policy, and broader than mere 'compliance', which implies only a checklist against a known standard. Assurance sits at the intersection of administrative law's traditional accountability doctrines and the technical practice of AI risk management standardised in instruments such as ISO 42001¹⁴.

Four doctrinal building blocks recur across African and international administrative law and are directly transferable to AI-enabled state action. Legality requires that the power to deploy a given AI system, and the purposes for which its outputs may be used, be traceable to a specific legal authorisation rather than inferred from a general executive mandate; this matters acutely for military AI, where constitutional war powers were not drafted with autonomous sensor fusion in mind. Necessity and proportionality require that the intrusiveness of an AI system, for example, continuous biometric surveillance at a border post—be justified by, and calibrated to, the security or administrative objective it serves, rather than deployed simply because the technology exists. Traceability and explainability require that decisions materially affected by an AI system's output be reconstructable after the fact, so that an affected person, a court, or an oversight body can identify which data, model version and human decision-maker produced a given outcome. Oversight and remedy require an institutional mechanism, independent of the deploying agency, empowered to review AI-assisted decisions and to grant redress where they are unlawful, discriminatory or disproportionate.

These four elements map closely onto the values embedded in the UNESCO Recommendation on the Ethics of Artificial Intelligence, which frames human oversight, transparency and accountability as core ethical requirements running through the entire AI lifecycle¹⁵, and onto the structured risk-management cycle required by ISO/IEC 42001, whose clause 6.1 requires organisations to identify and evaluate AI-specific risks and whose clause 9 requires ongoing performance measurement against defined indicators¹⁶. The doctrinal and technical vocabularies are, in other words, largely compatible; the difficulty is that African legal systems have not yet built the institutional bridges—regulators, auditors, procurement clauses, judicial competence—that would allow doctrinal requirements to be

¹⁴ISO/IEC 42001. <https://www.iso.org/standard/42001>

¹⁵UNESCO, 'Recommendation on the Ethics of Artificial Intelligence' (adopted by the General Conference, 41st session, 23 November 2021) <<https://www.unesco.org/en/artificial-intelligence/recommendation-ethics>> accessed 13 July 2026 ('UNESCO Recommendation').

¹⁶ISO/IEC 42001, cl 6.1 and cl 9, discussed in 'The Risk-Adjusted Intelligence Dividend: A Quantitative Framework for Measuring AI Return on Investment Integrating ISO 42001 and Regulatory Exposure' (arXiv, 2025) <<https://arxiv.org/pdf/2511.21975>> accessed 13 July 2026.

applied to a specific deployed system rather than remaining aspirational.

A further conceptual distinction matters for this paper's case selection: the difference between AI used for decision support, where a human retains final authority and the AI system informs but does not determine an outcome, and AI used for decision automation, where the system's output is acted upon with minimal human review. Nigeria's Hybrid Intelligence Shield and Kenya's border analytics are, on current public information, decision-support systems, but the pace of investment in autonomous threat-identification and interception technology suggests the line between support and automation is moving quickly, and any assurance framework must anticipate rather than merely react to that shift.

3. The African Legal and Policy Framework

3.1 The AU Continental Artificial Intelligence Strategy

The Continental Artificial Intelligence Strategy, endorsed by the AU Executive Council at its 45th Ordinary Session in Accra in July 2024, is the first continent-wide instrument to address AI comprehensively. It is explicitly development-focused: its five stated focus areas are harnessing AI's benefits, building AI capabilities, minimising risks, stimulating investment and fostering cooperation, translated into fifteen underlying action points¹⁷. The Strategy is a policy instrument rather than a treaty; it creates no binding obligations, establishes no supranational enforcement body, and leaves implementation to member states operating within a five-year plan running to 2030¹⁸. Its principal legal significance for this paper is interpretive: it signals the AU's preferred normative frame—Africa-centric, development-oriented, harmonising—against which national legislation and, ultimately, the assurance framework proposed in Section 7 should be read so as to remain politically and institutionally credible across the continent.

3.2 The Malabo Convention

The African Union Convention on Cyber Security and Personal Data Protection, commonly called the Malabo Convention, is the closest instrument Africa has to a binding continental data governance treaty. Adopted in 2014, it required fifteen ratifications to enter into force under its Article 36, a threshold reached only in May 2023 when Mauritania ratified, bringing

¹⁷Future of Privacy Forum, 'The African Union's Continental AI Strategy: Data Protection and Governance Laws Set to Play a Key Role in AI Regulation' (18 November 2024) <<https://fpf.org/blog/the-african-unions-continental-ai-strategy-data-protection-and-governance-laws-set-to-play-a-key-role-in-ai-regulation/>> accessed 13 July 2026.

¹⁸UNESCO, 'UNESCO's Support to AU's Continental AI Framework and Strategy' (28 August 2024) <<https://www.unesco.org/en/articles/unescos-support-aus-continental-ai-framework-and-strategy>> accessed 13 July 2026.

the Convention into force on 8 June 2023¹⁹. Article 8(1) commits states parties to strengthen protection of personal data and to punish violations of privacy, and Articles 11, 13 and 16 to 19 extend further data-governance and cybercrime obligations²⁰. However, the Convention was drafted before the current generation of AI systems existed, contains no AI-specific provisions, lacks a dedicated monitoring or enforcement mechanism, and as earlier noted, it has not been ratified by several of the continent's largest economies, including South Africa²¹. It therefore supplies a partial, uneven foundation: useful for data-protection aspects of AI assurance, but silent on algorithmic accountability, military AI or fiscal modelling specifically.

3.3 Regional human rights institutions

The African Commission on Human and Peoples' Rights has begun a draft study on the human rights implications of AI, robotics and other emerging technologies in Africa, examining impacts on civil, political, economic and social rights across the continent²². Although not yet finalised into binding guidance, the study signals that the regional human rights system regards AI deployment by public authorities, including in security and military contexts—as squarely within its supervisory competence under the African Charter on Human and Peoples' Rights. This is significant because it offers a plausible forum, alongside domestic courts, for the remedy element of the assurance framework proposed below.

3.4 National AI strategies

At the national level, a small number of states have adopted formal AI policies or strategies, including Kenya, Egypt, Rwanda, Mauritius, Senegal, Benin, Ghana and Tunisia, with Nigeria and South Africa reported to be in advanced drafting stages. Kenya's National Artificial Intelligence Strategy 2025–2030, formally launched in March 2025, is the most detailed of these, expressly naming security among its priority sectors and calling for a governance framework, algorithmic impact assessments for high-risk systems, and data-localisation rules²³. These national strategies are, like the AU Strategy, generally aspirational documents

¹⁹Malabo Convention (n 11) art 36. <https://ccdcoe.org/uploads/2018/11/AU-270614-CSConvention.pdf>

²⁰*ibid* art 8(1) and arts 11, 13, 16–19.

²¹*ibid* (n 12)

²²Police and Human Rights Resources (2025). DRAFT Study on human and peoples' rights and artificial intelligence, robotics, and other new and emerging technologies in Africa. <https://policehumanrightsresources.org/draft-study-on-human-and-peoples-rights-and-artificial-intelligence-robotics-and-other-new-and-emerging-technologies-in-africa>

²³White & Case LLP, 'AI Watch: Global Regulatory Tracker — Kenya' <<https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-kenya>> last accessed 29 July 2026.

rather than enforceable law; Kenya's own legal commentators note that the country currently has no AI-specific statute, leaving the Constitution, the Data Protection Act 2019 and the Consumer Protection Act 2012 to do what work they can²⁴.

4. Comparative and International Standards

4.1 UNESCO's Recommendation on the Ethics of Artificial Intelligence

Adopted unanimously by UNESCO's General Conference in November 2021, the Recommendation is the first global standard-setting instrument on AI ethics. It is grounded in respect for human rights and human dignity and advances principles of transparency, fairness, environmental sustainability and human oversight²⁵. Crucially for this paper, it goes beyond abstract values to propose concrete policy actions, including a model of data governance and a call on member states to establish the institutional and legal frameworks necessary to give the Recommendation domestic effect. Although non-binding, its status as a universally adopted instrument gives it persuasive authority that African legislatures can draw upon when drafting domestic AI statutes, much as soft-law human rights instruments have historically informed subsequent binding treaties.

4.2 ISO/IEC 42001:2023

ISO/IEC 42001 is the first international management-system standard for artificial intelligence, specifying requirements for establishing, implementing, maintaining and continually improving an AI management system within an organisation²⁶. Its clauses 4 to 10 cover organisational context, leadership, planning, support, operation, performance evaluation and improvement, with an annex of reference AI controls. Unlike the UNESCO Recommendation, ISO/IEC 42001 is certifiable: an organisation can be independently audited and certified as conformant, giving it direct relevance to the traceability and evidentiary requirements this paper treats as central to assurance. It is, however, a management-system standard rather than a technical specification for individual systems, so certification alone does not guarantee that any specific deployed system, for example, a border-surveillance model, is itself safe, fair or lawful; it guarantees only that the surrounding organisational processes exist.

4.3 OHCHR guidance on AI and human rights

²⁴Mohammed Muigai LLP, 'The Impact of Artificial Intelligence on Data Protection in Kenya' (27 August 2025) <<https://mohammedmuigai.com/the-impact-of-artificial-intelligence-on-data-protection-in-kenya/>> last accessed 29 July 2026.

²⁵UNESCO Recommendation (n 15).

²⁶International Organization for Standardization, ISO/IEC 42001:2023; Information Technology; Artificial Intelligence; Management System (ISO 2023) ('ISO/IEC 42001').

The UN High Commissioner for Human Rights has repeatedly stressed that any governance response to AI must be grounded in the existing international human-rights framework, warning as early as February 2023 that recent advances in AI put human agency, dignity and rights at serious risk absent effective guardrails²⁷, and specifically flagging that AI-enabled surveillance in some countries produces systematic violations of the right to privacy and chills freedom of expression and association²⁸. This guidance is directly applicable to the Nigerian, Kenyan and Moroccan security deployments examined in Section 6, all of which combine biometric identification with continuous monitoring of public space.

4.4 Comparative regional models

The AU Strategy itself draws explicitly on comparative regional frameworks, citing the European Union's risk-tiered AI Act, the ASEAN Guide on AI Governance and Ethics, and the 2024 Santiago Declaration for Latin America and the Caribbean as models of harmonised regional governance. None of these models can be transplanted wholesale into the African context, given differences in institutional capacity, resource availability and constitutional structure, but each illustrates a different regulatory technique, binding risk tiers in the EU model, voluntary common principles in the ASEAN model—that the African Legal AI Assurance Framework proposed in Section 7 draws upon selectively.

5. Methodology

This paper adopts a comparative doctrinal methodology combined with documentary case-study analysis. The doctrinal component analyses primary legal instruments, the AU Continental AI Strategy, the Malabo Convention, national AI strategies and applicable constitutional and statutory provisions, using standard techniques of legal interpretation to establish their scope, binding status and gaps. The comparative component situates these African instruments against the UNESCO Recommendation, ISO/IEC 42001 and OHCHR guidance, in order to identify assurance elements that are internationally recognised as good practice but absent from the African instruments.

The case-study component draws on contemporaneous government statements, defence-sector reporting, specialist policy commentary and peer-reviewed and working-paper literature published between 2024 and 2026. Jurisdictions were selected purposively rather

²⁷Volker Türk, 'Comment by UN High Commissioner for Human Rights Volker Türk on Advances in Artificial Intelligence' (OHCHR, 18 February 2023) <<https://ohchr.org/en/statements/2023/02/comment-un-high-commissioner-human-rights-volker-turk-advances-artificial>> accessed 13 July 2026.

²⁸Volker Türk, 'Artificial Intelligence Must Be Grounded in Human Rights' (OHCHR, 12 July 2023) <https://www.ohchr.org/en/statements-and-speeches/2023/07/artificial-intelligence-must-be-grounded-human-rights-says-high> accessed 13 July 2026.

than randomly, on two criteria: first, documented and continuing deployment of AI in one of three high-stakes public functions—military intelligence, security and border operations, or fiscal and economic forecasting; and second, availability of sufficiently detailed public reporting to support doctrinal analysis. Nigeria, Kenya and South Africa satisfy both criteria most fully and form the primary case studies; Rwanda, Egypt and Morocco are treated as a secondary comparative set illustrating variation across the continent in AI-enabled intelligence and defence practice. Evidentiary criteria for inclusion of a specific deployment required corroboration across at least two independent sources wherever possible, and explicit attribution to a named government official, ministry or institution.

The methodology has acknowledged limits. Much of the primary evidence on military and security AI comes from government and industry announcements rather than independent technical audit, meaning the paper can describe stated capability and intent with confidence but cannot verify operational performance, error rates or actual rights impact. Where sources conflict or a claim rests on a single outlet, this is flagged in the text rather than resolved by assumption.

6. Case Studies

6.1 Nigeria: military and security AI

Nigeria offers the most extensively documented example of AI-enabled military modernisation on the continent. In March 2026 the Ministry of Defence signed a USD 190 million memorandum of understanding with the UK-based MARSS Group for a Multi-Domain Hybrid Intelligence Shield, a sensor-fusion platform intended to integrate drone feeds, radar, thermal imaging and other sensor data into a single AI-analysed operational picture known as NiDAR²⁹. The Defence Minister has described the programme as covering border security, urban protection and counter-drone interception, supported by new national and regional command-and-control centres³⁰. The Nigerian Navy has separately begun integrating Turkish AYBARS-2 drones and American unmanned surface vessels, and has stated an intention to use AI in navigation, threat detection and predictive maintenance.

The strategic driver is a genuine and escalating security threat: insurgent groups including

²⁹'Nigeria Accelerates AI-Driven Defence Modernisation with National Hybrid Intelligence Network' (Trends N Africa, 6 July 2026) <<https://trendsnafrica.com/nigeria-accelerates-ai-driven-defence-modernisation-with-national-hybrid-intelligence-network/>> accessed 13 July 2026.

²⁹ibid.

³⁰'Nigeria to Deploy AI, Anti-Drone Technology for Military Operations' TheCable (Lagos, 14 May 2026) <<https://www.thecable.ng/nigeria-to-deploy-ai-anti-drone-technology-for-military-operations/>>

ISWAP and Boko Haram have themselves begun using low-cost first-person-view drones, progressing from surveillance to attacks on military positions, with ISWAP reported to have acquired around thirty-five commercial drones³¹. A parallel, less formal ecosystem of private Nigerian drone and surveillance firms, such as Terra Industries, has emerged to fill capability gaps, winning infrastructure-security contracts that blur the line between commercial protection and defence procurement, and operating with what one industry analysis describes as no shared data-sharing protocols or integration framework across competing private operators³². From an assurance perspective, this is precisely the scenario the doctrinal framework in Section 2 is designed to address: a technology procured under emergency security pressure, deployed by both state and quasi-private actors, with authorisation, proportionality and oversight questions arising faster than legislative or judicial capacity to answer them.

6.2 Kenya: border security and public-sector analytics

Kenya has pursued a more centrally planned approach. Its National Artificial Intelligence Strategy 2025–2030, launched in March 2025 after public consultation, names security as one of the priority sectors for AI adoption alongside agriculture, healthcare and education, and explicitly calls for algorithmic impact assessments for high-risk systems and a governance framework tied to the AU's continental agenda. In parallel, Kenya's Interior Ministry has announced a border-security modernisation programme combining drones, biometric identity verification and AI-driven analytics intended to detect and anticipate irregular crossings, alongside interoperable platforms for real-time intelligence sharing between security agencies. A related domestic surveillance rollout, building on an earlier Sh12.3 billion Integrated Public Safety Communication and Surveillance System, extends CCTV and analytics capability to major cities and border counties, with mandatory camera installation planned for all police stations³³.

Kenyan legal commentary is candid that this expansion is running ahead of regulation: as of 2025 Kenya had no AI-specific statute, relying instead on the Constitution, the Data Protection Act 2019 and the Consumer Protection Act 2012, none of which was drafted with algorithmic security decision-making in mind. Academic security-studies literature

³¹Ezenwa E Olumba, 'Nigeria's Armed Groups Are Entering the Drone Age and the State Must Respond' (Africa at LSE, 18 February 2026) <<https://blogs.lse.ac.uk/africaatlse/2026/02/17/nigerias-armed-groups-are-entering-the-drone-age-and-the-state-must-respond/>>

³¹ibid.

³²Techpoint Africa, 'Inside Nigeria's Shadow Defence Ecosystem' (2 January 2026) <<https://techpoint.africa/insight/inside-nigerias-shadow-defence-ecosystem/>>

³³'Kenya Rolls Out New High-Tech Security System' (Streamline, 20 January 2026) <<https://streamlinefeed.co.ke/news/kenya-rolls-out-new-high-tech-security-system>>

reinforces the point, recommending investment in AI-based analytics for early-warning systems while acknowledging that Kenya's National Intelligence Service, National Police Service and border authorities do not yet share a common data or oversight architecture³⁴. Kenya therefore illustrates a jurisdiction with unusually well-developed policy intent but the same enforcement gap identified continentally in Section 3.

6.3 South Africa: fiscal and economic-forecasting AI

South Africa's most consequential public-sector AI use is in fiscal and economic forecasting rather than security. The South African Reserve Bank and National Treasury have increasingly incorporated machine-learning nowcasting into real-time monitoring of GDP growth, with recent academic work applying penalised regression, random forest and gradient-boosted models, together with explainable-AI techniques, across South Africa's major macroeconomic cycles from the global financial crisis through the COVID-19 shock. A parallel strand of research has applied machine learning to predict municipal financial distress one year ahead, using the National Treasury's thirteen financial-health indicators together with socio-economic variables, explicitly designed to support risk-based prioritisation of interventions. The Reserve Bank's Monetary Policy Committee has itself revised growth forecasts in response to model outputs during 2026, in a context of heightened uncertainty around investment and household consumption³⁵.

These are lower-visibility deployments than military drones, but their assurance stakes are substantial: a mis-specified nowcasting or distress-prediction model can misallocate national or municipal budget support, with direct consequences for service delivery to the poorest communities. The COVID-19 experience is instructive here—resurgence-monitoring and vaccination-cost models directly informed a budget allocation of approximately USD 1.42 billion, illustrating both the value of algorithmic decision support and the scale of harm a flawed model could cause if unaudited³⁶. Notably, none of the literature reviewed for this paper describes a dedicated legal or audit framework specific to fiscal AI in South Africa; oversight currently rests on general public-finance management law and ordinary budgetary scrutiny, neither of which was designed with model risk in mind.

³⁴'Enhancing Kenya's National Security: Optimizing Early Warning and Response Surveillance Systems' (2024) International Journal of Research and Innovation in Social Science <<https://rsisinternational.org/journals/ijriss/articles/enhancing-kenyas-national-security-optimizing-early-warning-and-response-surveillance-systems/>>

³⁵Deloitte, 'South Africa's Economic Recovery Might Be Delayed, But Not Derailed' (Deloitte Insights, June 2026) <<https://www.deloitte.com/us/en/insights/topics/economy/emea/africa-economic-outlook.html>> , citing South African National Treasury, Budget Review 2026 and South African Reserve Bank, Monetary Policy Committee Forecast Report (May 2026).

³⁶The Role of Modelling and Analytics in South African COVID-19 Planning and Budgeting' (medRxiv, 2022) <<https://www.medrxiv.org/content/10.1101/2022.08.23.22279123.full.pdf>>

6.4 Comparative jurisdictions: Rwanda, Egypt, Morocco, and Cameroon

Beyond the three primary case studies, several other African states are adopting AI for military intelligence, security operations or economic planning, illustrating the range of institutional models available to the proposed framework. Rwanda, an early mover on drone logistics since 2016, has extended AI into scheduling of medical drone deliveries and, more recently, epidemic-response robotics, and has approved a National Artificial Intelligence Agency to coordinate investment, innovation and governance³⁷³⁸. Egypt continues to implement a National Artificial Intelligence Strategy 2025–2030 aimed at integrating AI into public services and building a specialised workforce, and participates actively in the AU's AI working group and the Smart Africa Alliance's AI Council. In March 2025 the two countries, together with Burundi, Cameroon, Ethiopia, Ghana, Morocco, Namibia, Senegal, South Africa, Tanzania and Uganda, took part in a multinational workshop on the responsible military use of AI, at which Kenya's Defence Cabinet Secretary called explicitly for AI in defence to be reconciled with justice, peace and human dignity³⁹.

Morocco presents a distinct model built around intelligence-service modernisation rather than battlefield technology: its General Directorate of National Security and General Directorate of Territorial Surveillance have pursued a 'new generation' intelligence strategy for 2030, combining risk-based internal security methods with counter-terrorism, cybercrime and hybrid-threat capabilities, operating under a constitutional framework—Articles 24 and 27 of the 2011 Constitution—that expressly anchors intelligence activity in privacy and communications-secrecy protections, subject to security and defence exceptions⁴⁰. Cameroon is beginning to align with the broader continental pattern of AI uptake in high-stakes public functions, but the evidentiary record remains at the level of policy discussion rather than operational transparency. Defence-sector reporting indicates that AI is being framed by Cameroonian officials as relevant to military effectiveness and security modernisation, including intelligence support and drone-enabled capabilities, while official digital-economy messaging places AI within the financial sector as a tool for risk management, fraud detection and predictive analysis.⁴¹ Cameroon's participation in a

³⁷ibid.

³⁸'Rwanda and Egypt to Draft AI Cooperation Agreement after Cairo Talks' (iAfrica, 2026) <<https://iafrica.com/rwanda-and-egypt-to-draft-ai-cooperation-agreement-after-cairo-talks/>>

³⁹'Military Grapple With Power of AI' Africa Defense Forum (27 January 2025) <<https://adf-magazine.com/2025/01/military-grapple-with-power-of-ai/>>

⁴⁰ibid.

⁴¹Ministry of Defence of Cameroon, 'Artificial Intelligence: Int'l War College trainees drilled on opportunities, threats' (30 May 2024) <https://theguardianpostcameroon.com/post/3044/fr/artificial-intelligence-int-l-war-college-trainees-drilled-on-opportunities-thr> accessed 5 August 2026

multinational workshop on the responsible military use of AI further shows engagement with regional norm-building on security AI⁴². However, the IMF's AI Preparedness Index places Cameroon at 0.34, with an observed score of 0.341 and a predicted score of 0.328, suggesting that the country's institutional, digital and regulatory readiness for AI remains modest rather than mature⁴³. Cameroon therefore illustrates the same structural problem identified elsewhere in this paper: growing AI ambition without a clearly documented assurance regime capable of securing legality, traceability and accountability⁴⁴. At the continental level, the AU Peace and Security Council itself has recognised the scale of the challenge, establishing in 2025 an Advisory Group on Artificial Intelligence and its Impact on Peace, Security and Governance, drawing on experts from all five African regions^{45,46,47}. Taken together, these comparative examples show that no single African state has yet built a comprehensive assurance regime for military or security AI; the variation lies only in how far each has progressed on policy, and in which institution, a ministry of defence, an intelligence directorate or a continental advisory body—currently holds informal responsibility for oversight.

7. The African Legal AI Assurance Framework

Drawing on the doctrinal foundations in Section 2, the instruments surveyed in Sections 3 and 4, and the operational realities documented in Section 6, this paper proposes a five-pillar African Legal AI Assurance Framework intended for adoption or adaptation at national level, with AU-level coordination to preserve interoperability across the continent's regional economic communities.

Pillar I: Legal authorisation and purpose limitation

Every AI system used by a public authority in a security, military or fiscal decision-making capacity should be traceable to an explicit statutory or executive authorisation naming its permitted purpose, data sources and decision type (support or automation). This responds

⁴² *ibid*

⁴³ International Monetary Fund, 'AI Preparedness Index (API)' https://www.imf.org/external/datamapper/AI_PI@API/ADVEC/EME/LIC accessed 5 August 2026.

⁴⁴ Militaries Grapple With Power of AI, Africa Defense Forum (27 January 2025) <https://adf-magazine.com/202501/militaries-grapple-with-power-of-ai/> accessed 5 August 2026.

⁴⁵ Amani Africa, 'Artificial Intelligence and Its Impact on Peace, Security and Governance' (19 March 2025) <<https://amaniafrica-et.org/artificial-intelligence-and-its-impact-on-peace-security-and-governance/>>

⁴⁶ *ibid*, on the AU Peace and Security Council's establishment of an Advisory Group on Artificial Intelligence and its Impact on Peace, Security and Governance (Terms of Reference, February 2025).

⁴⁷ Brookings Institution, 'How AI Is Impacting Policy Processes and Outcomes in Africa' (16 May 2024) <<https://www.brookings.edu/articles/how-ai-is-impacting-policy-processes-and-outcomes-in-africa/>> accessed 13 July 2026.

directly to the legality gap identified in Nigeria's and Kenya's security deployments, both of which currently proceed under general executive and procurement authority rather than AI-specific statute.

Pillar II: Risk-tiered impact assessment

Before deployment, and periodically thereafter, high-risk systems—defined to include biometric surveillance, autonomous target identification and any system materially informing budget allocation, should undergo a documented algorithmic impact assessment modelled on the assessment obligation Kenya's own National AI Strategy already contemplates, adapted from the risk-identification and evaluation cycle in ISO/IEC 42001 clause 6.1.

Pillar III: Evidentiary traceability and documentation

Deploying agencies should maintain an auditable record—model version, training data provenance, decision logs, sufficient to reconstruct any individual AI-assisted decision. This pillar operationalises the UNESCO Recommendation's transparency and human-oversight principles in a form usable by courts, oversight bodies and the African Commission's emerging AI-related human-rights supervision.

Pillar IV: Independent audit and certification

An independent national or regional body—drawing on the AU's proposed Advisory Group on AI and its Impact on Peace, Security and Governance as a plausible continental anchor, should periodically audit high-risk deployments against a certifiable management-system standard equivalent to ISO/IEC 42001, with findings reported to the legislature and, for military systems, to a designated parliamentary defence committee.

Pillar V: Remedy and judicial review

Persons materially affected by an AI-assisted state decision should have a clear route to challenge that decision, whether through ordinary judicial review, a specialist data-protection authority, or the African Commission's human-rights mechanisms, consistent with the accountability language used repeatedly by the UN High Commissioner for Human Rights⁴⁸⁴⁹. Military and intelligence uses will necessarily require calibrated exceptions to protect operational security, but the framework insists that such exceptions be legislated narrowly and reviewed periodically, rather than left as an unstated default.

⁴⁸Türk (n 27).

⁴⁹Türk (n 28).

8. Implementation and Enforcement

Translating the five pillars into practice requires attention to four institutional levers. First, public procurement is the most immediate point of leverage: African states already negotiate large bespoke contracts for AI-enabled defence and security systems, as Nigeria's MARSS Group agreement illustrates, and standard procurement clauses could require vendors to supply documentation sufficient to satisfy Pillar III before contract signature, without requiring new primary legislation in the short term.

Second, incident reporting obligations, modelled on cybersecurity breach-notification duties already found in national data-protection statutes across the continent, should be extended to AI system failures and near-misses in security and fiscal deployments, feeding into the audit function under Pillar IV. Third, oversight institutions need express statutory competence: data-protection authorities, auditors-general and, where they exist, parliamentary defence and security committees should each be given an unambiguous mandate to review AI systems within their sector, closing the institutional gap that currently leaves Kenyan security agencies without a shared oversight architecture and South African fiscal-modelling practice governed only by general public-finance law⁵⁰.

Fourth, judicial capacity must be built deliberately. Existing administrative and constitutional law doctrines—reasonableness, proportionality, procedural fairness—are capable in principle of scrutinising AI-assisted decisions, but judges and litigants need access to independent technical expertise to test vendor and government claims about system accuracy and bias. Specialist judicial training, of the kind UNESCO has piloted on AI and the rule of law, and technical amicus mechanisms attached to constitutional and high courts, would allow Pillar V's remedy guarantee to operate in substance rather than merely on paper.

9. Policy Implications

For legislatures, the priority is model legislation establishing AI-specific authorisation, impact -assessment and audit duties for public-sector deployments, capable of being adopted individually by member states while remaining interoperable under the AU Continental AI Strategy's harmonisation ambition. Regional economic communities such as ECOWAS and the East African Community are natural intermediate fora for such harmonisation, given their existing security-cooperation mandates and Kenya's Strategy's own reference to East African Community coordination.

For regulators, a practical toolkit is needed now, independent of full legislative reform:

⁵⁰South African National Treasury, Budget Review 2024 (National Treasury 2024) <<https://www.treasury.gov.za/documents/national%20budget/2024/review/FullBR.pdf>>

template algorithmic impact assessments, model audit checklists based on ISO/IEC 42001, and standard procurement clauses requiring vendor transparency. For ministries of defence and interior, the framework's exceptions for operational security should be paired with internal, classified oversight mechanisms, akin to inspectors-general, so that the absence of public transparency does not become the absence of any accountability at all.

Capacity building is a precondition for all of the above. The AU Strategy itself recognises that implementation of continental AI ambitions has been geographically concentrated and resource-constrained, with early funding disproportionately flowing to a small number of states. An assurance framework that assumes technical audit capacity uniformly available across fifty-five member states will fail in practice; phased implementation, beginning with the jurisdictions already investing heavily in security and fiscal AI, Nigeria, Kenya and South Africa among them, offers the most realistic path to eventual continental coverage.

10. Conclusion

African states are deploying artificial intelligence in some of the highest-stakes functions of government; military intelligence, border security and fiscal management—faster than they are building the legal instruments to assure that deployment. The AU Continental AI Strategy and the Malabo Convention provide valuable but partial foundations: the former sets a shared normative direction without binding force, and the latter offers a data-protection baseline that predates modern AI and lacks universal ratification. International instruments such as the UNESCO Recommendation and ISO/IEC 42001 supply doctrinal and technical vocabulary that African law can borrow, but they were not drafted with Africa's institutional constraints or security context in mind.

The case studies in this paper show both the scale of the challenge and a path through it. Nigeria's rapid militarisation of AI-enabled sensor fusion, Kenya's comparatively well-planned but still unenforced security strategy, and South Africa's quietly consequential use of machine learning in fiscal forecasting each expose a different facet of the same underlying problem: authorisation, risk assessment, traceability, audit and remedy are not yet built into how African states acquire and operate these systems. The five-pillar African Legal AI Assurance Framework proposed here is offered as a starting point for closing that gap, deliberately built to be adoptable incrementally, through procurement clauses and regulatory toolkits in the short term and through model legislation and judicial capacity-building over the medium term.

Future research should track implementation empirically as national AI statutes are drafted, and should extend the comparative case-study method used here to francophone West Africa and the Southern African Development Community, neither of which is well

represented in the present analysis. The stakes of getting this right are considerable: AI deployed without assurance in military, security or fiscal decision-making does not merely risk technical failure, but risks embedding unaccountable state power in exactly the domains where African constitutional law has fought hardest to establish accountability.