



Artificial Intelligence Sovereignty in Africa: Legal, Ethical and Strategic Challenges and Policy Pathways

Oladipupo Saburi Abdurrahman FASHINA

National Open University of Nigeria (NOUN)

ace26140003@noun.edu.ng / fash2025@gmail.com / 08024552893

ORCID: <https://orcid.org/0009-0007-0741-3560>

DOI : <https://doi.org/10.5281/zenodo.22917819>

Abstract

Artificial intelligence (AI) has emerged as a decisive terrain of twenty-first-century geopolitical competition, and Africa's engagement with this terrain raises urgent questions about sovereignty, self-determination, and equitable participation in global technological governance. This paper examines the legal, ethical, and strategic challenges to AI sovereignty in Africa, defined as the continent's capacity to govern, own, and direct the development and deployment of AI technologies within its territories according to its own values and developmental priorities. The analysis is based on a qualitative, doctrinal and interpretive desk-based review of six primary continental and national instruments which principally include the African Union's Continental Artificial Intelligence Strategy (2024), Nigeria's National Artificial Intelligence Strategy (2025), and the Nigeria Data Protection Act (2023) read alongside twelve peer-reviewed and policy publications by African and diaspora scholars, published between 2020 and 2025 and identified through targeted searches of Google Scholar, SSRN and the institutional repositories of the African Union, Research ICT Africa, and the Strathmore University Centre for Intellectual Property and Information Technology Law (search terms and selection criteria are set out in full in Section 4). The paper's principal contribution is an integrated analytical model that treats African AI sovereignty as constituted by the interaction of four dimensions which are legal authority, ethical authority, infrastructural capacity, and epistemic standing rather than as a single attribute a state either possesses or lacks. Applying this model, the paper argues that Africa's AI sovereignty is constrained by fragmented and unevenly enforced legal regimes, infrastructural and compute dependency on external powers, a persistent brain drain of AI talent, and epistemic marginalisation within global AI ethics discourse, while showing how African institutions and scholars are actively reconstructing sovereignty through relational ethical frameworks such as Ubuntu, harmonised data-governance proposals, and assertive continental strategy documents. As a desk-based doctrinal and interpretive review rather than an empirical study, the paper's principal limitation is that its conclusions are interpretive readings of a purposively selected corpus rather than statistically representative findings across all fifty-five African states. The paper closes with prioritised, actor-specific recommendations for the African Union, regional economic communities, national governments with particular reference to Nigeria covering regulators, universities, and private-sector actors.

Keywords: Artificial Intelligence Sovereignty; Digital Colonialism; Data Governance; Ubuntu Ethics; African Union AI Strategy



1. Introduction

The global diffusion of artificial intelligence has reconfigured the terms on which states negotiate economic advantage, security, and cultural influence. Where earlier waves of technological change were mediated largely through trade and telecommunications policy, the current moment is distinguished by the extent to which AI systems depend on control over three scarce resources: data, computational infrastructure, and technical talent. Nations that command these resources are positioned to shape the rules, standards, and applications that govern AI globally, while nations that do not risk becoming perpetual consumers of externally designed systems (African Union, 2024; Okolo, 2024). For Africa, a continent of fifty-five states with divergent legal traditions, infrastructural capacities, and developmental priorities, this asymmetry is not new; it echoes older patterns of resource extraction and epistemic marginalisation that scholars have termed algorithmic or digital colonialism (Birhane, 2020).

The concept of AI sovereignty has consequently gained purchase in African policy and scholarly circles as a way of framing the continent's response to this asymmetry. It denotes more than mere national ownership of technology; it encompasses the legal authority to regulate data flows and algorithmic systems within a jurisdiction, the ethical authority to define what constitutes responsible and beneficial AI according to local values, and the strategic capacity to negotiate favourable terms with external technology powers rather than accept dependency by default (Awolaye, 2021; Venske, 2023). The African Union's adoption of the Continental Artificial Intelligence Strategy in July 2024, alongside a wave of national strategies including Nigeria's National Artificial Intelligence Strategy, signals a deliberate continental effort to assert this sovereignty (African Union, 2024; National Information Technology Development Agency [NITDA] & National Centre for Artificial Intelligence and Robotics [NCAIR], 2024).

Yet the pursuit of AI sovereignty in Africa unfolds against considerable legal, ethical, and strategic constraints. Legally, data protection regimes across the continent remain fragmented, with over forty countries possessing some form of data protection legislation but inconsistent implementation and more than ten states lacking legislation altogether, undermining the harmonised cross-border data governance that meaningful AI regulation requires. Ethically, the dominant AI ethics discourse continues to be shaped by Western rationalist and individualist assumptions about personhood, autonomy, and harm, a framework that African scholars argue inadequately captures the relational and communitarian values embodied in philosophies such as Ubuntu (Gwagwa et al., 2022; Mhlambi, 2020). Strategically, Africa's AI ambitions are pursued from a position of profound infrastructural dependency: the continent hosts a small fraction of global data centre and computing capacity, and its digital infrastructure is substantially financed and built by external actors, principally Chinese telecommunications firms and, increasingly, American hyperscale technology companies, raising questions about whose interests ultimately govern the continent's digital future.

Before turning to the paper's research questions, it is necessary to distinguish five related but analytically separable concepts that are frequently conflated in both policy and scholarly usage. National sovereignty denotes the classical Westphalian authority of a state over its territory and population. Digital sovereignty extends this authority to a state's right to govern data, infrastructure, and digital services within its jurisdiction (Venske, 2023). Data sovereignty is narrower still, referring specifically to the principle that data generated within a jurisdiction



remains subject to that jurisdiction's laws irrespective of where it is stored or processed. Technological sovereignty concerns a state's capacity to develop, manufacture, or independently access the hardware and software on which digital and AI systems depend, rather than merely to regulate data flows. AI sovereignty, the paper's central concept, is best understood as a composite of the preceding categories: it requires the legal authority captured by digital and data sovereignty, the technological and infrastructural capacity denoted by technological sovereignty, the ethical authority to define locally legitimate standards of responsible AI, and a fourth, distinct requirement of epistemic standing which is the capacity to help shape, rather than merely receive, the global norms, benchmarks, and research agendas that define what counts as legitimate AI. Distinguishing these terms clarifies, for example, that a state may possess considerable data sovereignty through a robust data protection statute while still lacking AI sovereignty in the fuller sense addressed by this paper, precisely because infrastructural or epistemic capacity remains externally controlled.

This paper addresses these intersecting challenges through the following core questions: What does AI sovereignty mean in the African context, and how has it been conceptualised in continental and national policy instruments? What legal obstacles impede the exercise of that sovereignty, particularly with reference to Nigeria's data protection and AI governance architecture? What ethical tensions arise between globally dominant AI governance paradigms and African moral traditions? And what strategic vulnerabilities does Africa face as a participant, rather than a mere object, of the global AI race? In addressing these questions, the paper gives sustained attention to African and Nigerian scholarship, situating this literature not as a supplement to Western AI ethics and governance debates but as an independent and increasingly influential body of thought in its own right.

The paper is structured as follows. Section 2 develops the conceptual and theoretical framework, defining AI sovereignty, situating it within the literatures on digital colonialism and Ubuntu ethics, and setting out an integrated analytical model. Section 3 reviews the continental and national policy architecture and the emerging body of African AI scholarship. Section 4 outlines the paper's methodology. Section 5 presents the main analysis, organised around legal, ethical, and strategic challenges. Section 6 offers a critical evaluation of competing scholarly positions, and Section 7 sets out prioritised, actor-specific implications and recommendations before the paper concludes in Section 8.

2. Conceptual and Theoretical Framework

2.1 Defining AI Sovereignty

Sovereignty, in its classical Westphalian sense, denotes the supreme authority of a state over its territory and population. Digital sovereignty extends this authority into cyberspace, asserting a state's right to govern the data, infrastructure, and digital services operating within its jurisdiction (Venske, 2023). AI sovereignty is a further specification of this concept, referring to the capacity of a state or regional bloc to determine how AI systems are developed, trained, deployed, and regulated within its territory, and to do so according to its own developmental priorities and value commitments rather than those imposed by external technology providers (Awolaye, 2021). Understood this way, AI sovereignty has at least three interlocking dimensions: a legal dimension, concerning jurisdiction over data and algorithmic accountability; an ethical dimension, concerning



the normative frameworks used to define responsible AI; and a strategic dimension, concerning control over the material infrastructure, capital, and talent that AI development requires.

Research ICT Africa (2024) frames sovereignty as existing along a continuum rather than as a binary state, with countries retaining agency to decide which categories of data to share, under what conditions, and with whom. This framing is instructive because it avoids an unrealistic autarkic conception of sovereignty that would be unattainable for most African states given their current infrastructural constraints, while still preserving the normative core of the concept: that African states and institutions, rather than external corporations or governments, should hold the decisive authority over AI's terms of engagement with African societies.

2.2 Digital and Algorithmic Colonialism as an Analytical Lens

A substantial body of scholarship analyses Africa's contemporary technological dependency through the lens of colonialism. Birhane (2020), in an influential and widely cited paper, coined the term algorithmic colonisation to describe how Western technology corporations import AI-driven solutions into African contexts with minimal adaptation or regulatory scrutiny, reproducing colonial-era patterns of extraction in which African populations and their data function as raw material for systems whose benefits accrue disproportionately elsewhere. Whereas traditional colonialism operated through direct political domination, Birhane (2020) argues that algorithmic colonialism operates through corporate control of digital infrastructure and data ecosystems, a form of domination that is less visible but no less consequential, since it simultaneously discourages the development of local technology industries and entrenches dependency on imported software and platforms.

This analysis resonates with subsequent work on data sovereignty and digital transformation. Calzati (2022) examines Chinese involvement in Kenya's information and communication technology sector and interrogates whether infrastructural partnerships that promise 'data sovereignty' in fact risk substituting one form of external control for another, given that data centres, network hardware, and standards are frequently supplied and financed by foreign firms even where formal legal ownership rests with the host state. Awolaye (2021), writing from within a Nigerian research institution, extends this concern by asking whether African states should pursue the assertive digital sovereignty strategies associated with countries such as China, Russia, and Brazil, or risk remaining permanently on the periphery of global data governance. The digital and algorithmic colonialism literature thus provides an important corrective to techno-optimistic narratives that treat AI adoption in Africa as an unambiguous developmental good, insisting instead that the terms, ownership, and beneficiaries of AI systems be subjected to critical scrutiny.

At the same time, this literature should not be read as counselling withdrawal from AI development. Eke and Ogoh (2022) caution that dominant narratives about AI in Africa, whether celebratory or catastrophist, tend to be authored externally and to obscure the continent's own long history of technological innovation and adaptation. They call for the recovery of what they term forgotten African AI narratives, arguing that African engagement with AI should be understood



not solely as a story of victimhood or dependency but also as one of agency, experimentation, and locally grounded innovation, even amid genuine structural constraints.

2.3 Ubuntu as a Relational Ethical Framework

A third conceptual pillar of this paper is the Southern African philosophical concept of Ubuntu, frequently glossed through the Zulu and Xhosa maxim *umuntu ngumuntu ngabantu*, meaning that a person is a person through other persons. Mhlambi (2020) develops Ubuntu into a systematic ethical and human rights framework for AI governance, arguing that dominant Western AI ethics discourse is built on a conception of personhood grounded in individual rationality, a legacy traceable to Cartesian philosophy, which lends itself to the optimisation of individual efficiency at the expense of collective wellbeing and thereby facilitates outcomes such as surveillance capitalism and data extraction. Ubuntu, by contrast, grounds personhood in relationality: one's humanity is constituted through one's relationships with others, and ethical AI governance must therefore attend to AI's effects on the interconnected social fabric rather than solely on discrete individual harms.

Gwagwa et al. (2022) build on this relational framework to argue that Ubuntu offers a normative resource for making global AI ethics discourse more inclusive of Sub-Saharan African perspectives, which have historically been marginalised in the formulation of supposedly universal AI ethics principles. They contend that Ubuntu-derived action-guiding principles could help reconcile competing cultural values in AI design and provide African stakeholders with a distinctive contribution to global governance debates rather than positioning Africa as a passive recipient of externally formulated standards. Complementary work by Djiberou Mahamadou et al. (2024) applies an Ubuntu lens specifically to healthcare AI, arguing that data ethics frameworks emphasising individual informed consent and autonomy require adaptation to account for communitarian conceptions of data ownership and benefit-sharing prevalent in many African societies.

This scholarship is not without internal contestation, a point taken up more fully in the critical evaluation in Section 6. Yilma (2025) offers a searching critique of the uncritical invocation of Ubuntu in continental AI governance documents, observing that Ubuntu is a philosophical and political concept most closely associated with southern Africa and that its salience even within that sub-region, including within South Africa's own constitutional history, has been contested and is not self-evidently generalisable to a continent as culturally heterogeneous as Africa. This critique does not vitiate the analytical value of Ubuntu as one important African ethical resource, but it cautions against treating it as a uniform pan-African alternative capable of single-handedly resolving the epistemic asymmetries in global AI ethics.

2.4 An Integrated Analytical Model

The preceding discussion suggests an explicit analytical model rather than a loose juxtaposition of concepts, and it is this model that constitutes the paper's central theoretical contribution. In the model, AI sovereignty is the central, dependent construct, and four conditions function as its explanatory dimensions. The first is legal-jurisdictional control: the capacity to enact and enforce binding rules over data and algorithmic systems (examined in Section 5.1). The second is ethical-normative authority: the capacity to define, rather than merely adopt, the value commitments like the Ubuntu-derived relational principles alongside established rights-based principles such as



autonomy, privacy, fairness, and accountability against which AI systems are judged legitimate (Section 5.2). The third is infrastructural-material capacity: ownership of, or negotiated control over, the compute, cloud, and talent base required for AI development (Section 5.3). The fourth, cutting across the first three, is epistemic standing: the capacity to help shape global AI research agendas, benchmarks, and governance norms rather than simply to receive them (Sections 3.3 and 5.2). Coloniality, in this model, is not itself a fifth dimension of sovereignty but the historical and structural condition that has systematically weakened all four dimensions simultaneously; Ubuntu and cognate relational ethics function as one, but not the only, resource for reconstructing the second dimension. This model is used to organise the analysis in Section 5 and the critical evaluation in Section 6, and it reframes single-indicator claims — a data protection statute, a foreign-owned data centre, a rhetorical invocation of Ubuntu — as partial evidence bearing on one dimension rather than conclusive evidence about sovereignty overall.

3. Literature Review

Read cumulatively, the literature reviewed in this section converges on three points of consensus: that Africa's continental and national AI strategies mark a genuine, if uneven, assertion of policy agency (African Union, 2024; NITDA & NCAIR, 2024); that legal fragmentation and enforcement deficits constrain the practical realisation of that agency (Research ICT Africa, 2024); and that African-authored scholarship on algorithmic colonialism and Ubuntu ethics constitutes an independent intellectual contribution rather than a derivative gloss on Western debates (Birhane, 2020; Mhlambi, 2020; Eke & Ogoh, 2022). The literature divides, however, on two questions that the analysis in Sections 5 and 6 revisits directly: first, whether foreign-financed digital infrastructure is compatible with sovereignty when negotiated on favourable terms, or whether it constitutes dependency regardless of terms (compare Awoleye, 2021, with Calzati, 2022); and second, whether Ubuntu can function as a generalisable pan-African ethical resource or should instead be treated as one regionally specific tradition among several (compare Gwagwa et al., 2022, with Yilma, 2025). What remains unresolved, and what this paper accordingly addresses, is how these legal, ethical, and infrastructural threads interact within a single analytical account of AI sovereignty, rather than being treated, as in most of the literature reviewed below, as separate subfields.

3.1 The Continental Policy Architecture

The African Union's Continental Artificial Intelligence Strategy, endorsed by the AU Executive Council in July 2024 during its 45th Ordinary Session in Accra, Ghana, represents the most comprehensive continental effort to date to assert African agency over AI governance (African Union, 2024). The Strategy, developed through a Continental AI Working Group process beginning in 2023 and involving over 130 ministers and stakeholders, is organised around five focus areas, namely harnessing AI's benefits, building AI capabilities, minimising risks, stimulating investment, and fostering cooperation, which are elaborated into fifteen concrete policy action points. Aligned with the African Union's Agenda 2063 and the United Nations Sustainable Development Goals, the Strategy sets out a five-year implementation period running from 2025 to 2030, with a mid-term review scheduled for 2027 and the development of an African AI readiness index to track progress (African Union, 2024).



The Strategy explicitly situates itself within a comparative field of regional AI governance instruments, referencing the European Union's AI Act, the Association of Southeast Asian Nations' Guide on AI Governance and Ethics, and the 2024 Santiago Declaration for Latin America and the Caribbean, while insisting that African AI governance must be development-focused and grounded in ethical principles, democratic values, human rights, and the rule of law rather than a wholesale importation of external regulatory templates (Future of Privacy Forum, 2024). It further identifies data governance as a foundational prerequisite for responsible AI regulation, building on the AU Data Policy Framework and the Malabo Convention on Cyber Security and Personal Data Protection, and calls for a multi-tiered governance framework spanning continental, regional, and national levels.

Notwithstanding this ambition, independent assessments of the Strategy's implementation reveal significant constraints. An eighteen-month review of implementation data from July 2024 to October 2025 found that funding for AI initiatives remained starkly concentrated, with roughly eighty-three per cent of continental AI funding directed to only four countries, alongside minimal mobilisation of private capital relative to the estimated five hundred billion dollars in continental infrastructure needs, prompting the characterisation of a development-governance paradox in which ambitious regulatory architecture coexists with severe capacity and resource constraints. This paradox, and the argument that AU strategy documents function partly as symbolic 'governance as strategy' exercises rather than binding regulatory instruments, is echoed in comparative work examining North African AI governance trajectories in Egypt, Morocco, Mauritania, Algeria, Libya, and Tunisia, which similarly finds descriptive policy proliferation running ahead of enforceable institutional capacity.

3.2 National Frameworks: Nigeria as a Case Study

Nigeria's engagement with AI governance illustrates both the promise and the limitations of national-level sovereignty assertions within the continental architecture. The National Information Technology Development Agency, through its National Centre for Artificial Intelligence and Robotics, published a draft National Artificial Intelligence Strategy in August 2024, articulating a vision for Nigeria to become a global leader in ethical and inclusive AI innovation (NITDA & NCAIR, 2024). The final National Artificial Intelligence Strategy, published in September 2025 under the leadership of the Federal Ministry of Communications, Innovation and Digital Economy, sets a five-year vision for 2025 to 2029 organised around three overarching goals, namely economic growth and competitiveness, social development and inclusion, and technological advancement and leadership, delivered through five operational pillars covering infrastructure, ecosystem development, sectoral adoption, responsible AI, and governance (OECD.AI Policy Observatory, 2026).

The strategy is notable for its candid acknowledgement of Nigeria's structural constraints, including limited and unreliable electricity and broadband infrastructure, public research and development investment of approximately 0.2 per cent of gross domestic product against a global average of 2.2 per cent, a persistent shortage of skilled AI professionals compounded by brain drain, and gaps in data quality and governance (OECD.AI Policy Observatory, 2026). Independent policy analysis situates Nigeria's starting position as comparatively weak, noting the country's



ranking of ninety-fourth out of the assessed states in the 2024 Oxford Insights Government AI Readiness Index, and its bottom-ranked position among twenty-five countries in the Top Ranked AI Nations Index published by Tufts University's Fletcher School, underscoring the scale of the capacity-building challenge that Nigeria's AI ambitions confront.

Complementing the AI strategy is Nigeria's Data Protection Act 2023, which establishes the Nigeria Data Protection Commission and creates a comprehensive framework of principles, lawful bases for processing, data subject rights, and enforcement mechanisms (Federal Republic of Nigeria, 2023). Section 41 of the Act prohibits the transfer of personal data outside Nigeria by default, subject to exceptions where the receiving jurisdiction demonstrates adequate protection through legislation, binding corporate rules, standard contractual clauses, codes of conduct, or explicit data subject consent. Entities classified as data controllers or processors of major importance face fines of up to ten million naira or two per cent of annual gross revenue, whichever is higher, alongside potential criminal sanctions including imprisonment of up to one year for serious violations. This restrictive default position has generated debate among legal commentators regarding its practical operability given Nigeria's heavy reliance on foreign-hosted cloud and software-as-a-service infrastructure, with some analysts noting that Section 2(c) of the Act, which extends jurisdiction to foreign processors handling Nigerian data regardless of their physical location, creates a degree of redundancy with the cross-border transfer rules while also complicating compliance for American software providers whose platforms underpin much of Nigeria's digital economy.

3.3 African Scholarship on AI Governance, Data Regulation, and Ethics

A distinctive and increasingly influential strand of scholarship on AI governance in Africa is produced by African and diaspora researchers working across law, computer science, philosophy, and public policy. Okolo (2024), a Nigerian-American computer scientist and public policy researcher, argues that data protection regulation is foundational to any credible AI governance regime in Africa, given that the effectiveness of AI oversight ultimately depends on the quality of the underlying data governance regime; she further contends that AI and data regulation should not be left to governments alone but should incorporate advisory participation from civil society, academia, and industry, mirroring emerging multi-stakeholder governance models elsewhere. Her broader body of work, including contributions to the African Union Development Agency's white paper on the regulation and responsible adoption of AI in Africa, situates Nigerian and African expertise at the centre, rather than the periphery, of global AI governance debates.

Research ICT Africa (2024), a leading Cape Town-based policy research network, provides a critical assessment of the African Digital Compact, a companion instrument endorsed alongside the Continental AI Strategy, arguing that while the Compact rightly identifies digital sovereignty, human rights, and regional cooperation as common African negotiating positions in global digital governance forums, it stops short of anchoring these commitments in established regional human rights instruments such as the African Charter on Human and Peoples' Rights, and risks reducing digital rights to a narrow focus on personal data protection at the expense of broader concerns such as access to information and freedom of expression.



On the ethics front, the special collection on AI, Ethics and Policy Governance in Africa, and associated volumes such as *Responsible AI in Africa: Challenges and Opportunities*, bring together African scholars, technologists, and policy thinkers whose work, the editors note, remains under-represented in mainstream Western AI ethics publications despite its direct relevance to regulatory and governance gaps on the continent. Within this literature, Eke and Ogoh (2022) and subsequent collaborative work advance the concept of epistemic injustice in global AI ethics, arguing that African perspectives are frequently solicited only after ethical frameworks have already been substantially formulated elsewhere, reducing African participation to a validating rather than a constitutive role. Health-focused contributions, such as Thaldar's (2024) editorial on data governance in African health research, extend these concerns to genomic and biomedical AI applications, highlighting unresolved questions of informed consent, data ownership, and benefit-sharing that intersect closely with AI-driven diagnostic and research tools increasingly deployed on the continent.

Taken together, this literature establishes that African scholarship on AI is neither derivative of, nor secondary to, Western AI ethics and governance debates. Rather, it constitutes an increasingly coherent and self-critical field that interrogates both external technological domination and the limitations of purely continental or national policy responses, providing the analytical foundation on which the remainder of this paper builds.

4. Methodology and Approach

This paper adopts a qualitative, doctrinal, and interpretive desk-based research methodology appropriate to a legal-policy analysis of an emerging and fast-evolving regulatory field. The analysis proceeds through three complementary methods. First, doctrinal legal analysis is applied to primary legal and policy instruments, including the African Union's Continental Artificial Intelligence Strategy, the AU Data Policy Framework, Nigeria's National Artificial Intelligence Strategy, and the Nigeria Data Protection Act 2023, to identify their scope, structure, and internal coherence. Second, comparative policy analysis situates these African instruments alongside international reference points, including the European Union's regulatory approach and global governance instruments such as the Global Digital Compact, in order to assess convergence and divergence in regulatory philosophy. Third, critical literature synthesis draws on peer-reviewed journal articles, working papers, and policy reports, with particular emphasis on scholarship authored by African and Nigerian researchers, to construct a theoretically grounded account of the ethical and strategic dimensions of AI sovereignty that purely doctrinal legal analysis would not capture on its own.

To make this review reproducible, the following protocol was applied. Document identification proceeded through targeted searches of Google Scholar, SSRN, arXiv, and the institutional repositories of the African Union, Research ICT Africa, the African Union Development Agency, and the Strathmore University Centre for Intellectual Property and Information Technology Law, using the search terms 'AI sovereignty Africa', 'digital sovereignty Africa', 'algorithmic colonialism', 'Ubuntu AI ethics', 'data protection Africa', and 'Nigeria AI strategy', restricted to material published between January 2020 and October 2025 so as to capture the period since the AU's initial continental AI policy deliberations. Primary legal and policy instruments were included where they were formally adopted or officially published continental, regional, or



Nigerian instruments (n = 6: the AU Continental AI Strategy, the AU Data Policy Framework, the Malabo Convention, Nigeria's National AI Strategy, the NITDA/NCAIR draft strategy, and the Nigeria Data Protection Act 2023). Secondary scholarly sources were included where peer-reviewed or produced by a recognised policy research institution and where the source substantively addressed AI or digital sovereignty, data governance, or AI ethics in an African context (n = 12); sources addressing AI governance solely outside Africa, or addressing African digital policy without reference to AI or data governance, were excluded. Doctrinal legal analysis was applied to the six primary instruments, while critical literature synthesis was applied to the twelve secondary sources, with the two analytical products triangulated in Sections 5 and 6. This protocol is reproducible but modest in scale, and the paper's conclusions should accordingly be read as an interpretation of a purposively selected corpus rather than as the product of a systematic or exhaustive review.

Consistent with the objectives of the paper, source selection deliberately prioritised African-authored and African-institution-affiliated scholarship, including work published by Research ICT Africa, the Strathmore University Centre for Intellectual Property and Information Technology Law, the African Union Development Agency, and individual African and diaspora scholars, while retaining internationally recognised comparative and theoretical literature where it provides indispensable context. This approach is consistent with calls in the literature for African AI governance scholarship to resist treating Western sources as a default analytical baseline (Eke & Ogoh, 2022). The paper does not undertake primary empirical fieldwork, such as interviews or surveys, and this constitutes an acknowledged limitation; its contribution lies instead in the synthesis, critical evaluation, and theoretically informed interpretation of an already substantial but dispersed body of primary instruments and secondary scholarship.

5. Main Analysis and Discussion

The three sub-sections that follow present analytical themes emerging from the reviewed legal instruments and scholarship, organised around the legal, ethical, and strategic dimensions of the integrated model set out in Section 2.4. They are presented as analytical themes rather than as empirical findings derived from a systematic dataset, consistent with the desk-based methodology described in Section 4; each claim is anchored, as far as possible, to a specific primary instrument or a specific piece of scholarly evidence rather than presented as an unqualified continent-wide generalisation.

5.1 Legal Challenges to AI Sovereignty

It is important, at the outset, to distinguish legislative divergence from regulatory incompatibility. That fifty-five jurisdictions have adopted differing data protection statutes, at different times and to differing standards, is legislative divergence; this is a feature of legal pluralism common to any large multi-state region, including the European Union prior to the General Data Protection Regulation, and is not by itself evidence that African AI sovereignty is unattainable. Regulatory incompatibility is the narrower and more consequential problem: instances where divergent rules actively conflict — for example, where one jurisdiction's cross-border transfer prohibition cannot be satisfied by the adequacy mechanisms recognised in a partner jurisdiction — producing a genuine deadlock rather than merely inconsistent standards. The evidence reviewed in this paper substantiates divergence more strongly than it substantiates systemic incompatibility:



harmonisation instruments such as the Malabo Convention and the AU Data Policy Framework aim precisely at converting divergence into interoperable, mutually recognised standards, and Nigeria's own default prohibition under Section 41, discussed below, is compatible in principle with a differentiated regional model provided adequacy and certification mechanisms are operationalised.

The foremost legal challenge to AI sovereignty in Africa is the fragmentation of data protection and cross-border data governance regimes across fifty-five jurisdictions with divergent legal traditions, institutional capacities, and enforcement records. While over forty African countries have enacted data protection legislation, implementation remains inconsistent and more than ten states continue to operate without any legislative framework, a gap that is particularly consequential for AI systems, which routinely require the aggregation, pooling, and cross-border movement of large datasets for training and validation purposes. Regional harmonisation instruments, including the African Union Convention on Cyber Security and Personal Data Protection, commonly known as the Malabo Convention, and the more recent AU Data Policy Framework, articulate ambitious harmonisation objectives, but continental initiatives such as the African Continental Free Trade Area's Digital Trade Protocol and the AU Data Policy Framework have yet to translate into operative, harmonised cross-border data transfer mechanisms.

Nigeria's own regulatory posture exemplifies the tension between asserting sovereign control over data and maintaining the cross-border data flows on which much of the digital economy, and AI development specifically, depends. The default prohibition on cross-border personal data transfer under Section 41 of the Data Protection Act 2023, while a legitimate and arguably necessary assertion of sovereign authority over Nigerian citizens' data, imposes considerable compliance burdens on both domestic and foreign entities. Because so much of Nigeria's digital ecosystem runs on United States-based cloud infrastructure and software-as-a-service platforms, compliance with the Act's cross-border provisions requires firms to demonstrate adequate safeguards for essentially all routine international data processing, a requirement whose practical enforceability remains uncertain in the absence of a fully resourced and technically capable Nigeria Data Protection Commission. This illustrates a broader structural challenge for AI sovereignty across the continent: robust data protection legislation, however well designed on paper, cannot by itself secure sovereignty where the underlying computational infrastructure, the servers, cloud platforms, and processing capacity on which AI systems run, remains predominantly foreign-owned and foreign-hosted.

A second legal challenge concerns the absence, in most African jurisdictions, of AI-specific legislation addressing algorithmic accountability, liability for AI-related harms, intellectual property in AI-generated outputs, and sector-specific regulation of high-risk AI applications such as facial recognition, credit scoring, and predictive policing. Nigeria's National Artificial Intelligence Strategy signals an intention to develop responsible AI governance mechanisms, including consideration of internationally recognised risk-management frameworks such as the United States National Institute of Standards and Technology framework, but as of the Strategy's publication these mechanisms remained largely aspirational rather than codified in binding law (NITDA & NCAIR, 2024). This legislative gap creates uncertainty for both AI developers seeking regulatory clarity and citizens seeking redress for algorithmic harm, and it leaves African jurisdictions structurally dependent on foreign regulatory precedents, most prominently the



European Union's AI Act, as reference points, a dependency that itself raises sovereignty concerns insofar as regulatory standards developed for European social, economic, and infrastructural conditions may be poorly suited to African contexts (Future of Privacy Forum, 2024).

A third and related legal challenge concerns enforcement capacity. Even where comprehensive legislation exists, as with Nigeria's Data Protection Act, meaningful sovereignty requires regulatory institutions with the technical expertise, financial resources, and political independence to investigate violations, impose sanctions, and adjudicate disputes involving powerful multinational technology firms. The literature on AI governance in North Africa similarly finds that policy proliferation, the drafting of strategies, frameworks, and guidelines, has substantially outpaced the development of institutional enforcement capacity, a pattern that appears to recur across the continent's AI governance landscape more broadly.

5.2 Ethical Challenges to AI Sovereignty

The ethical dimension of AI sovereignty concerns Africa's capacity to define, rather than merely receive, the normative standards by which AI systems are judged responsible, fair, and beneficial. As discussed in Section 2.3, a significant body of African scholarship contends that dominant global AI ethics discourse, encapsulated in instruments such as the European Union's Ethics Guidelines for Trustworthy AI and various international principle-based frameworks, is grounded in a Western, individualist conception of personhood and harm that inadequately captures relational and communitarian African moral traditions (Mhlambi, 2020; Gwagwa et al., 2022). This is not merely an abstract philosophical concern; it has concrete implications for how AI systems are designed and evaluated. An AI system optimised to protect individual privacy and autonomy according to Western liberal norms may nonetheless produce outcomes that are experienced as ethically deficient within communities that understand data, identity, and benefit as fundamentally shared and relational, as Djiberou Mahamadou et al. (2024) illustrate with reference to healthcare AI and questions of communal consent and benefit-sharing.

This framing should not be read as positing a clean binary between a monolithic 'Western' individualist ethics and a unified 'African' relational ethics. Africa itself encompasses Islamic, Christian, indigenous, and secular legal-philosophical traditions whose positions on privacy, consent, and collective welfare vary considerably, and Ubuntu itself is most directly associated with southern Africa rather than the continent as a whole (Yilma, 2025). The more defensible claim, and the one this paper adopts, is narrower: established rights-based principles of autonomy, privacy, fairness, and accountability are not rendered inapplicable in African contexts, but they require supplementation, and in some cases reweighting, where relational conceptions of personhood and communal data ownership are salient. Ubuntu, on this reading, does not replace autonomy or accountability as governance principles; it reframes how they are operationalised — for example, by treating community-level consent and benefit-sharing as a legitimate complement to individual informed consent in the healthcare AI context discussed by Djiberou Mahamadou et al. (2024), rather than as a substitute for it.

A second ethical challenge concerns epistemic injustice in the production of AI ethics knowledge itself. Eke and Ogoh (2022) argue that African voices are too often invited into global AI ethics conversations only after foundational frameworks have already been settled elsewhere, positioning African contributors as commentators on, rather than co-authors of, global standards. This dynamic



is compounded by the well-documented underrepresentation of African researchers in the major AI research venues, journals, and funding bodies that shape the field's mainstream ethical vocabulary, meaning that even well-resourced African ethical scholarship faces structural barriers to achieving comparable global visibility and influence.

A third ethical challenge, related to but distinct from questions of philosophical framing, concerns the material conditions of AI production that occur within Africa but largely serve external markets. The continent has become a significant site for data annotation, content moderation, and other forms of what has been termed data work, activities essential to training large-scale AI systems but frequently characterised by low wages, psychologically taxing content exposure, and limited labour protections. Birhane's (2020) analysis of algorithmic colonisation is directly pertinent here: the extraction of low-cost cognitive labour from African workers to train AI systems whose profits and benefits accrue substantially to foreign technology corporations reproduces, in digital form, the extractive economic relationships characteristic of historical colonialism, even where the workers themselves are nominally free wage labourers rather than colonial subjects.

Finally, the Ubuntu-centred response to these ethical challenges, while valuable, is itself subject to important internal critique, as Yilma (2025) demonstrates. Treating Ubuntu as a ready-made, pan-African ethical solution risks two errors: first, essentialising a culturally and historically specific southern African philosophical tradition as representative of a continent characterised by enormous religious, linguistic, and philosophical diversity; and second, allowing continental policy documents to invoke Ubuntu rhetorically, as a gesture toward cultural authenticity, without translating its relational commitments into operational governance mechanisms. A mature account of AI ethics sovereignty in Africa must therefore draw on Ubuntu and cognate relational philosophies as important but partial resources within a broader, pluralistic African ethical landscape, rather than as a singular substitute for the difficult work of context-specific ethical deliberation.

5.3 Strategic Challenges to AI Sovereignty

This section distinguishes six related but non-identical concepts that are frequently collapsed in policy discourse: dependency (reliance on a single external source with limited alternatives), interdependence (mutual reliance in which both parties hold some leverage), bargaining power (the capacity to negotiate favourable terms irrespective of ownership), ownership (formal title to infrastructure or capital), regulatory control (the capacity to impose binding conditions on operators regardless of ownership), and strategic autonomy (the composite capacity to pursue an independent developmental trajectory). Foreign ownership of data-centre and cloud infrastructure is evidence of a lack of asset ownership; it is not, by itself, evidence of a lack of strategic autonomy, provided host states retain regulatory control and sufficient bargaining power to negotiate terms — for example, data-localisation conditions, technology-transfer commitments, or local-employment requirements — that serve domestic developmental priorities. The scholarly disagreement identified in Section 3.1 between infrastructural pragmatists and infrastructural sceptics is, on this reading, substantially a disagreement about how much bargaining power African states in practice hold vis-à-vis Chinese and American infrastructure providers, rather than a disagreement about whether foreign ownership is compatible with sovereignty in principle.



The strategic dimension of AI sovereignty concerns Africa's position within the broader geopolitical competition over AI infrastructure, standards, and markets, a competition increasingly dominated by the United States and China, with the European Union pursuing a distinctive regulatory-power strategy. Africa's digital infrastructure, including the data centres, fibre networks, and cloud computing capacity on which AI training and deployment ultimately depend, has been substantially financed and constructed through partnerships with external powers, most prominently Chinese telecommunications firms, whose infrastructure underpins a majority of the continent's third- and fourth-generation mobile networks, alongside a growing presence of American hyperscale cloud providers establishing data centres in markets such as South Africa. This infrastructural dependency creates a strategic vulnerability: irrespective of the sophistication of African data protection or AI governance legislation, sovereignty over the legal and ethical dimensions of AI cannot be fully realised while the physical infrastructure and, in many cases, the underlying AI models themselves remain externally owned, controlled, and serviced.

Scholarly assessment of this infrastructural dependency is divided over its implications. Some analysts argue that Africa's digital sovereignty must remain paramount regardless of which foreign partner, whether Chinese or Western, is involved in infrastructure development, emphasising that African agency lies in the terms negotiated for such partnerships rather than in an unrealistic aspiration toward complete infrastructural self-sufficiency. Others caution that the framing of a binary choice between Chinese and Western digital partners risks obscuring the more fundamental question of whether any foreign-financed infrastructure model can deliver genuine sovereignty, given that data centres built with foreign capital typically remain embedded in commercial and, in some cases, security relationships that persist well beyond the initial construction phase (Calzati, 2022).

A second strategic challenge is the persistent shortage of African AI talent and the accompanying brain drain, whereby African-trained computer scientists, engineers, and AI researchers frequently pursue careers in North American, European, or Gulf state technology hubs, drawn by higher salaries and better-resourced research environments than most African institutions can currently offer. Nigeria's National Artificial Intelligence Strategy explicitly identifies this brain drain as a structural constraint, alongside chronically low public research and development investment, estimated at roughly 0.2 per cent of gross domestic product against a global average exceeding two per cent (OECD.AI Policy Observatory, 2026). The consequence is that African AI development remains heavily reliant on foreign-trained diaspora researchers and corporate-funded training initiatives, arrangements that can accelerate capacity building in the short term but which may also reinforce longer-term dependency on external funding cycles.

A third strategic challenge concerns Africa's limited leverage in shaping the international AI governance norms increasingly being negotiated in venues such as the United Nations, the Group of Twenty, and plurilateral technology governance initiatives. Although the African Digital Compact and the Continental AI Strategy represent efforts to project a coordinated African position in fora such as the Global Digital Compact process, Research ICT Africa (2024) finds that this coordinated position remains thin in substantive terms, insufficiently anchored in binding regional human rights instruments, and vulnerable to being overtaken by the far greater negotiating capacity and technical resourcing that established powers such as the United States, China, and the European Union bring to these discussions. Without a stronger, more technically resourced, and



more unified African negotiating position, the continent risks being a rule-taker rather than a rule-maker in the emerging international AI governance order, notwithstanding the ambitious language of its own continental strategy documents.

6. Critical Evaluation

Relative to the literature reviewed in Section 3, this paper's synthesis supports the implementation-gap diagnosis advanced by independent assessments of the AU Strategy and by Nigeria's own strategy documents; it contradicts, or at minimum substantially qualifies, accounts that treat any foreign infrastructure ownership as definitionally incompatible with sovereignty (Section 5.3); it extends Yilma's (2025) critique of Ubuntu-as-panacea by integrating it with, rather than treating it as a rejection of, established rights-based ethical principles (Section 5.2); and it reframes the legal-fragmentation literature by distinguishing legislative divergence from regulatory incompatibility, a distinction that is implicit in the sources reviewed but not made explicit by them (Section 5.1).

Assessed cumulatively, the African Union's Continental Artificial Intelligence Strategy and its constituent national strategies, including Nigeria's, represent a genuine and historically significant assertion of African agency in AI governance. Their strengths include an explicitly development-oriented rather than purely risk-oriented regulatory philosophy, sustained engagement with regional human rights and constitutional traditions, and an emerging body of home-grown scholarship that challenges the presumption that AI ethics and governance frameworks must originate in Brussels, Washington, or Beijing before being adapted for African use. The candour with which instruments such as Nigeria's National AI Strategy acknowledge structural weaknesses, in infrastructure, research investment, and talent retention, is itself a strength, since credible policy planning depends on an accurate diagnosis of constraints rather than aspirational rhetoric alone.

Nonetheless, the critical literature reviewed in this paper identifies persistent weaknesses that qualify optimistic readings of Africa's AI sovereignty trajectory. First, there is a demonstrable implementation gap between the ambition of continental and national strategy documents and the funding, institutional capacity, and enforcement mechanisms available to realise them, evidenced by the concentration of continental AI funding in a small number of countries and Nigeria's comparatively low position in independent AI readiness indices. Second, the invocation of African values, whether through references to Ubuntu or to broadly stated commitments to human rights and inclusive development, risks functioning symbolically rather than operationally unless translated into concrete legal standards, technical requirements, and enforceable accountability mechanisms, a concern substantiated by Yilma's (2025) critique of ethics-washing in continental policy documents. Third, the debate between scholars emphasising infrastructural pragmatism, who argue that African states should accept foreign-financed infrastructure on the best available terms while building domestic capacity over time, and scholars emphasising infrastructural caution, who warn that reliance on any single external power for critical digital infrastructure reproduces dependency regardless of that power's identity, remains unresolved and merits continued empirical monitoring as continental data centre and compute capacity expands.

A further point of scholarly disagreement concerns the appropriate relationship between African AI governance instruments and international regulatory templates such as the European Union's AI Act. One position, reflected in the AU Strategy's explicit comparative engagement with the EU framework, holds that African states can benefit from adapting proven international regulatory



architecture, particularly its risk-tiered approach to AI oversight, rather than beginning entirely from first principles (Future of Privacy Forum, 2024). A competing position, informed by the digital colonialism literature, cautions that wholesale adoption of externally designed regulatory templates risks importing assumptions about market structure and enforcement resourcing that do not hold in most African jurisdictions, potentially privileging the compliance capabilities of large foreign firms over smaller domestic AI enterprises (Birhane, 2020). This paper's assessment, consistent with Eke and Ogoh's (2022) call for context-specific governance narratives, is that selective, critically adapted borrowing of international regulatory concepts, combined with genuinely African-authored enforcement design, offers a more defensible middle path than either wholesale importation or wholesale rejection.

The paper's theoretical contribution, accordingly, is not the application of digital colonialism and Ubuntu as pre-existing critical lenses to a current policy problem, but the integrated four-dimensional model set out in Section 2.4, which treats legal, ethical, infrastructural, and epistemic capacity as interacting rather than independent conditions, and which reframes single indicators such as foreign ownership or legal divergence as necessary but not sufficient markers of a sovereignty deficit.

7. Implications and Recommendations

The recommendations below convert the analysis in Sections 5 and 6 into prioritised, actor-specific actions, each with an indicative feasibility and timeframe assessment, in place of the more general aspirations of the original manuscript.

Priority	Recommendation	Responsible Actor(s)	Feasibility / Timeframe
High	Resource and empower the Nigeria Data Protection Commission with technical staff, budget, and institutional independence, and issue clarifying regulatory guidance on how routine cross-border cloud services satisfy Section 41's adequacy exceptions.	Federal Government of Nigeria; Nigeria Data Protection Commission	Short-term (1–2 years); primarily budgetary/administrative, no new legislation required.
High	Pursue sector-by-sector data-governance harmonisation (e.g., health, financial, and identity data) under the AU Data Policy Framework and Malabo Convention rather than a single comprehensive continental instrument.	African Union Commission; Regional Economic Communities	Medium-term (2–5 years); sequencing reduces negotiation complexity relative to a single instrument.
Medium	Integrate Ubuntu-informed relational principles with established autonomy, privacy, fairness and accountability principles into concrete algorithmic impact-assessment tools.	National AI regulators; universities; AI developers	Medium-term; a technical design task, not a legislative one.



High	Establish dedicated, ring-fenced R&D appropriation lines to close the gap between Nigeria's approximately 0.2% R&D/GDP ratio and the global average, reducing reliance on episodic donor or corporate funding.	National legislature; Federal Ministry of Finance	Long-term (5+ years); contingent on fiscal capacity and competing budget priorities.
Medium	Ground Africa's negotiating position in international AI governance forums explicitly in the African Charter on Human and Peoples' Rights, rather than in data-protection language alone.	African Union; African Digital Compact negotiators	Medium-term; primarily a drafting and coordination task.
Ongoing	Commission independent monitoring of AU Strategy implementation — funding allocation, enforcement actions, and AI readiness indicators — across the 2025–2030 period.	Independent research institutions (e.g., Research ICT Africa); African Union	Ongoing throughout the implementation period.

8. Conclusion

This paper has examined the legal, ethical, and strategic challenges confronting the pursuit of AI sovereignty in Africa, using an integrated four-dimensional model — legal authority, ethical authority, infrastructural capacity, and epistemic standing — to synthesise a rapidly evolving continental policy architecture and a maturing body of African-authored scholarship. Its principal contribution is this model itself, which reframes single-indicator claims about sovereignty — a data protection statute, a foreign-owned data centre, a rhetorical invocation of Ubuntu — as partial evidence bearing on one dimension rather than as conclusive evidence about sovereignty overall. Applying this model, the paper has argued that Africa's AI sovereignty is constrained legally by fragmented and, in places, only partially harmonised data-governance regimes; ethically by the continued dominance of Western rationalist frameworks even as Ubuntu and cognate relational ethics offer a substantive, if regionally specific and still only partially operationalised, complement rather than a wholesale alternative; and strategically by infrastructural dependency, talent drain, and constrained negotiating leverage, tempered in each case by the bargaining power African states retain through regulatory control even absent asset ownership.

The paper's principal limitation is that, as a doctrinal and interpretive desk-based review of a purposively selected corpus rather than a systematic or empirical study, its conclusions describe patterns discernible in the reviewed instruments and scholarship rather than statistically representative findings across fifty-five heterogeneous states; future research combining this analytical model with country-level empirical fieldwork would substantially strengthen the evidentiary base. Realistically, the coming 2025–2030 implementation period of the AU Continental AI Strategy is likely to produce uneven progress across the four dimensions identified here, with legal harmonisation and infrastructural investment probably advancing more slowly than ethical and epistemic reframing. Tracking this unevenness, rather than resolving it into a



single verdict on whether Africa becomes a 'rule-shaper' or a 'rule-taker', is the more analytically productive and realistic framing for subsequent research and policy monitoring.

References

- African Union. (2024, August 9). Continental Artificial Intelligence Strategy. African Union Commission. <https://au.int/en/documents/20240809/continental-artificial-intelligence-strategy>
- Awoleye, O. M. (2021). Reconfiguring data infrastructure ecosystem in Africa: A primer toward digital sovereignty. arXiv. <https://arxiv.org/abs/2109.14186>
- Birhane, A. (2020). Algorithmic colonization of Africa. *SCRIPTed*, 17(2), 389–409. <https://doi.org/10.2966/scrip.170220.389>
- Calzati, S. (2022). 'Data sovereignty' or 'data colonialism'? Exploring the Chinese involvement in Africa's ICTs: A document review on Kenya. *Journal of Contemporary African Studies*, 40(2), 270–285.
- Djiberou Mahamadou, A. J., Ochasi, A., & Altman, R. B. (2024). Data ethics in the era of healthcare artificial intelligence in Africa: An Ubuntu philosophy perspective. arXiv. <https://arxiv.org/abs/2406.10121>
- Eke, D., & Ogoh, G. (2022). Forgotten African AI narratives and the future of AI in Africa. *International Review of Information Ethics*, 32, 1–8.
- Federal Republic of Nigeria. (2023). Nigeria Data Protection Act, 2023.
- Future of Privacy Forum. (2024, November 18). The African Union's Continental AI Strategy: Data protection and governance laws set to play a key role in AI regulation. <https://fpf.org/blog/global/the-african-unions-continental-ai-strategy-data-protection-and-governance-laws-set-to-play-a-key-role-in-ai-regulation/>
- Gwagwa, A., Kazim, E., & Hilliard, A. (2022). The role of the African value of Ubuntu in global AI inclusion discourse: A normative ethics perspective. *Patterns*, 3(4), Article 100462. <https://doi.org/10.1016/j.patter.2022.100462>
- Mhlambi, S. (2020). From rationality to relationality: Ubuntu as an ethical and human rights framework for artificial intelligence governance (Carr Center Discussion Paper Series 2020-009). Harvard Kennedy School, Carr Center for Human Rights Policy.
- National Information Technology Development Agency & National Centre for Artificial Intelligence and Robotics. (2024). Draft National Artificial Intelligence Strategy 2024. Federal Ministry of Communications, Innovation and Digital Economy.



- OECD.AI Policy Observatory. (2026). National Artificial Intelligence Strategy (NAIS) – Nigeria. <https://oecd.ai/en/dashboards/policy-initiatives/national-artificial-intelligence-strategy-nais>
- Okolo, C. T. (2024). Reforming data regulation to advance AI governance in Africa. In Foresight Africa 2024. The Brookings Institution. <https://www.brookings.edu/articles/reforming-data-regulation-to-advance-ai-governance-in-africa/>
- Research ICT Africa. (2024, October 4). Governing data as a public good: The key to Africa's realisation of the Global Digital Compact? <https://researchictafrica.net/2024/10/04/governing-data-as-a-public-good-the-key-to-africas-realisation-of-the-global-digital-compact/>
- South African Institute of International Affairs. (2025). How to achieve African digital sovereignty. <https://saiia.org.za/research/how-to-achieve-african-digital-sovereignty/>
- Thaldar, D. (2024). Editorial: Data governance in African health research: ELSI challenges and solutions. *Frontiers in Pharmacology*, 15, Article 1525434. <https://doi.org/10.3389/fphar.2024.1525434>
- Venske, T. (2023). Navigating digital sovereignty in Africa: A review of key challenges and constraints. *Africa Governance Papers*, 1(4). Good Governance Africa.
- Yilma, K. (2025). Ethics of AI in Africa: Interrogating the role of Ubuntu and AI governance initiatives. *Ethics and Information Technology*, 27, Article 24. <https://doi.org/10.1007/s10676-025-09834-5>