African Journal of Legal Research [AJLR] (2026) Vol. 4, No 2
https://africanjournaloflegalresearch.com [ISSN: 1595 – 5966]

ARTIFICIAL INTELLIGENCE AND HUMAN RIGHTS IN AFRICA: RETHINKING PROTECTION UNDER THE AFRICAN CHARTER SYSTEM

Feyisayo A. Folorunso*

Abstract

Artificial intelligence (AI) is increasingly shaping governance, security, and socio-economic life across Africa, from biometric systems and financial technologies to predictive policing, border control and public service delivery. While AI is often framed as a tool of efficiency and development, its deployment in contexts of weak institutions raises significant human rights concerns, including mass surveillance, exclusion of marginalised populations and violations of privacy, dignity, equality, fair hearing and freedom of expression. This article examines whether the African human rights system, anchored in the African Charter on Human and Peoples' Rights, can protect individuals and communities against AI-related rights violations. Using a doctrinal and comparative methodology, it analyses Charter provisions, regional jurisprudence, and soft law while situating Africa's regulatory challenges within global debates on algorithmic governance, private power, and digital colonialism. The article argues that the Charter's people-centred and communitarian conception of rights provides a viable foundation for rights-based AI governance but is constrained by weak enforcement, fragmented digital regulation, and private technology influence. It calls for progressive Charter interpretation, an African Union-led AI and human rights framework, strengthened oversight and data protection, and enhanced collaboration between states, human rights institutions and civil society. Such measures can enable Africa to harness AI for development while resisting digital authoritarianism and external control.

Keywords: African Charter, Artificial intelligence, Human right

1.0 INTRODUCTION

Artificial intelligence has moved with remarkable speed from the margins of technical experimentation to the centre of governance, security, and economic organisation across Africa. Algorithmic systems are now routinely deployed for biometric identification, migration control, predictive policing, credit scoring, social welfare allocation, and electoral administration. These technologies are frequently justified in the language of efficiency, innovation, and development, particularly in contexts marked by administrative capacity constraints and large populations.[1] Yet beneath this narrative of technological promise lies a more troubling reality: artificial intelligence is increasingly shaping how power is exercised over individuals and communities, often in ways that are opaque, unaccountable, and deeply consequential for the enjoyment of fundamental human rights.

Across the continent, AI-driven systems have been implicated in mass surveillance practices, discriminatory profiling, exclusion from essential services, and the erosion of procedural guarantees.[2] Biometric digital identification schemes risk rendering individuals 'invisible' where data is inaccurate or incomplete; predictive policing tools may reproduce historical biases embedded in colonial and post-colonial law enforcement practices; automated decision-making in finance and welfare can entrench socio-economic marginalisation under the guise of technical neutrality.[3] These risks are not merely hypothetical. They are

* LL.B (OAU), B.L (Lagos), LL.M (ABUAD), Ph.D. Candidate in International Human Rights and Development Law (UNIABUJA), Managing Partner, Isaac-Dennis Folorunso &Co., Email: feyisayofolorunso1@gmail.com, feyisayo@folorunsoandco.com, 09160009463, ORCID iD: 0009-0006-9739-8626

[1] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015) 3-7

[2] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Public Affairs 2019) 376–380.

[3] Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (St Martin's Press 2018) 11-15.

amplified by weak regulatory environments, limited data protection safeguards, and a growing dependence on foreign technology firms that design, own, and control the underlying infrastructures of algorithmic governance in Africa.[4]

Globally, the human rights implications of artificial intelligence have prompted significant normative and regulatory responses. The European Union has adopted a comprehensive regulatory approach through the Artificial Intelligence Act, grounded in risk classification and fundamental rights protection.[5] At the international level, United Nations bodies, including the Office of the High Commissioner for Human Rights and UNESCO, have articulated principles linking AI governance to existing human rights obligations.[6] Africa, however, remains comparatively underprepared.

Despite the presence of an established regional human rights system, there is no binding African instrument that explicitly addresses artificial intelligence or algorithmic decision-making from a human rights perspective. Existing African Union digital policy frameworks gesture towards innovation and development, but largely sidestep the deeper structural risks AI poses to dignity, equality, and accountability.[7]

---

[4] Nanjala Nyabola, *Digital Democracy, Analogue Politics: How the Internet Era Is Transforming Politics in Kenya* (Zed Books 2018) 92–95.

[5] European Union, 'Regulation (EU) 2024/1689 -Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)' (2024) OJ L 1689, arts 1-5, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689> accessed 10 January 2026.

[6] UN Human Rights Council, 'The Right to Privacy in the Digital Age' UN Doc A/HRC/48/31 (13 September 2021) paras 18–25 <https://undocs.org/A/HRC/48/31> accessed 10 January 2026; UNESCO, 'Recommendation on the Ethics of Artificial Intelligence' (2021) paras 7–12, <https://www.unesco.org/en/artificial-intelligence/ethics> accessed 10 January 2026.

[7] African Union, '*Digital Transformation Strategy for Africa' (2020–2030)* <https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030>accessed 10 January 2026

This absence is particularly concerning given Africa's historical and contemporary governance challenges. Weak institutional oversight, limited judicial capacity, and patterns of authoritarianism in some states heighten the danger that AI technologies will be deployed as tools of control rather than empowerment.[8] Moreover, Africa's subordinate position within the global digital economy raises additional concerns about digital colonialism, whereby data extracted from African populations is processed, monetised, and governed externally, with minimal local control or benefit.[9] In such contexts, artificial intelligence does not merely introduce new technical risks; it reconfigures longstanding asymmetries of power in ways that strain existing human rights frameworks.

Against this backdrop, this article interrogates whether the African human rights system, anchored primarily in the African Charter on Human and Peoples' Rights can respond effectively to the challenges posed by artificial intelligence. It advances the central argument that while the African Charter was adopted long before the emergence of modern AI technologies, its broadly framed, people-centred, and communitarian conception of rights provides a viable foundation for protecting human rights in the age of algorithmic governance. The Charter's emphasis on human dignity, equality, collective welfare, and peoples' rights offers normative resources that are particularly well suited to addressing AI-related harms that operate at structural and communal levels rather than through isolated individual violations.[10]

[8] Michela Wrong, *Do Not Disturb: The Story of a Political Murder and an African Regime Gone Bad* (PublicAffairs 2021) 41-44.
[9] Nick Couldry and Ulises Mejias, *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism* (Stanford University Press 2019) 153-160.
[10] African Charter on Human and Peoples' Rights (1981) arts 1, 2, 3, 5, 19-24.

However, the paper contends that this potential remains largely unrealised. Interpretive inertia, weak enforcement mechanisms, fragmented digital governance, and the expanding role of private technology actors operating beyond traditional accountability frameworks have limited the capacity of African human rights institutions to engage meaningfully with AI-related harms. Rethinking protection under the African Charter system therefore requires both normative imagination and institutional adaptation. It calls for a purposive and evolutionary interpretation of the Charter, informed by contemporary technological realities and grounded in Africa's socio-political context, rather than the uncritical transplantation of foreign regulatory models.

This article analyses key provisions of the African Charter implicated by artificial intelligence, examines relevant jurisprudence and soft law developed by African regional bodies, and situates Africa's regulatory challenges within broader global debates on algorithmic governance, private power, and digital colonialism. The article proceeds in six parts. Following this introduction, Part II situates artificial intelligence within the African socio-technical context. Part III examines the normative scope and limitations of the African Charter in relation to AI. Part IV analyses institutional and accountability gaps within the African human rights system. Part V explores pathways for bridging these gaps through rights-based AI governance. Part VI sets out concrete recommendations, before the article concludes by reflecting on the implications of artificial intelligence for Africa's human rights future.

2.0 ARTIFICIAL INTELLIGENCE AND THE AFRICAN CONTEXT

Artificial intelligence in Africa is not emerging in a regulatory or institutional vacuum alone; it is unfolding within a socio-technical landscape shaped by historical inequality, fragile governance structures,

and uneven access to digital infrastructure. Unlike jurisdictions where AI governance debates are largely framed around optimisation and innovation, the African context is defined by more fundamental concerns: legal capacity, accountability, inclusion, and power. Algorithmic systems are often introduced as technical solutions to deeply political problems, including identity management, security, welfare distribution, and electoral credibility.[11] In such environments, the risks posed by artificial intelligence are not incidental; they are structurally embedded.

Across the continent, AI deployment is closely tied to biometric data collection. National digital identity programmes in countries such as Nigeria, Kenya, Ghana, and South Africa rely on facial recognition, fingerprinting, and automated verification systems to regulate access to voting, banking, telecommunications, and social services.[12]While these systems are presented as tools of inclusion, their operation in contexts marked by poor data quality, limited remedies, and weak oversight has resulted in exclusion rather than empowerment. Individuals whose biometric data is inaccurate or unrecognised may be denied essential services with little or no procedural recourse. [13] The opacity of algorithmic decision-making further compounds these harms, rendering affected persons unable to understand, challenge, or correct adverse outcomes.

Law enforcement and security sectors have likewise embraced artificial intelligence with minimal public scrutiny. Predictive policing tools,

[11] Lina Dencik, *Digital Citizenship and Surveillance Society* (Polity Press 2020) 21-24.

[12] Privacy International, 'Identity Systems and Human Rights in Africa' (2020) <https://privacyinternational.org/report/3756/identity-systems-and-human-rights-africa> accessed 10 January 2026.

[13] World Bank, 'Identification for Development (ID4D) Global Dataset' (World Bank 2019) <https://id4d.worldbank.org/global-dataset>accessed 10 January 2026.

automated risk assessment systems, and surveillance technologies are increasingly deployed to manage crime, terrorism, and border control.[14] These systems frequently draw on historical datasets shaped by colonial policing practices and contemporary patterns of discrimination, raising serious concerns about bias, disproportionate targeting, and the erosion of the presumption of innocence. In the absence of clear legal standards governing necessity, proportionality, and accountability, AI-driven security technologies risk normalising forms of digital authoritarianism under the guise of efficiency and public order.[15]

The African context is further distinguished by a high degree of dependence on foreign technology providers. Core AI infrastructures ranging from data storage and cloud computing to algorithm design and system maintenance are predominantly controlled by multinational corporations headquartered outside the continent.[16] This dependency has significant human rights implications. Data generated from African populations is frequently processed and monetised elsewhere, limiting domestic regulatory control and exacerbating asymmetries of power between states, private actors, and affected communities. This phenomenon can be described as digital colonialism, a contemporary extension of extractive relationships in which data replaces raw materials as the primary resource.

Weak or uneven data protection regimes intensify these risks. Although several African states have adopted data protection legislation,

[14] Sarah Brayne, *Predict and Surveil: Data, Discretion, and the Future of Policing* (Oxford University Press 2020) 58-62.
[15] UN Special Rapporteur on the Promotion and Protection of Human Rights while Countering Terrorism, 'Human Rights Implications of the Use of Artificial Intelligence in Counter-Terrorism' (UN Doc A/HRC/46/36(22 January 2021) <https://undocs.org/A/HRC/46/36> accessed 10 January 2026.
[16] African Development Bank Group, *Digital Economy Report: Africa* (AfDB 2022) 71-75 <https://www.afdb.org/en/documents/digital-economy-report-africa> accessed 10 January 2026.

enforcement remains inconsistent, and many laws lack specific provisions addressing automated decision-making, algorithmic transparency, or meaningful consent.[17] At the regional level, the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention) has suffered from low ratification rates, limiting its normative and practical impact.[18]As a result, individuals subjected to AI-driven harms often fall through regulatory gaps, unable to invoke effective remedies at either national or regional levels.

These challenges are compounded by structural socio-economic inequalities. High levels of poverty, limited digital literacy, and restricted access to legal remedies reduce the capacity of affected populations to resist or contest algorithmic harms. AI systems deployed in welfare, finance, and migration contexts therefore tend to disproportionately affect marginalised communities, reinforcing patterns of exclusion while appearing administratively neutral. In such settings, artificial intelligence does not merely automate decision-making; it automates inequality.

Understanding artificial intelligence within the African context thus requires moving beyond technical descriptions to interrogate the power relations embedded in algorithmic systems. AI governance in Africa is inseparable from questions of development, sovereignty, and human dignity. Any attempt to regulate artificial intelligence through a human rights lens must therefore grapple with the continent's historical experiences, institutional realities, and collective vulnerabilities. It is against this backdrop that the African Charter's people-centred and

[17] Teki Akuetteh Falconer, 'Data Protection and Privacy in Africa' (2019) 3 *African Journal of Law and Technology* 45, 52-55.
[18] African Union, 'Convention on Cyber Security and Personal Data Protection' *(*Malabo Convention*)* (adopted 27 June 2014, not yet in force) <https://au.int/en/treaties/convention-cyber-security-and-personal-data-protection > accessed 10 January 2026.

communitarian framework assumes particular significance, offering normative resources capable of addressing harms that are structural, collective, and transnational in nature.

3.0 THE AFRICAN CHARTER AND ARTIFICIAL INTELLIGENCE: SCOPE, PROMISE AND LIMITS

The African Charter on Human and Peoples' Rights represents a singularly ambitious attempt to integrate individual and collective rights within a single normative framework. Adopted in 1981, the Charter predates the digital era, yet its broad articulation of rights, duties, and peoples' protections provides a potentially powerful foundation for addressing contemporary challenges posed by artificial intelligence (AI). Unlike highly technocratic instruments in other jurisdictions, the Charter emphasises a communitarian and people-centred conception of rights[19], embedding human dignity, equality, and development within a collective vision of social justice.

AI technologies in Africa intersect with a wide spectrum of human rights, both individual and collective. At the level of **i**ndividual rights, Articles 2 and 3 guarantee non-discrimination and equality before the law, which are immediately implicated by algorithmic decision-making. AI systems, particularly those deployed in policing, welfare, finance, and border management, rely on historical and demographic datasets. These datasets frequently encode systemic inequalities and biases, which AI reproduces and, in some cases, amplifies.[20] For instance, predictive policing systems may disproportionately target ethnic minorities or marginalised communities, while automated credit scoring

[19] Frans Viljoen, *International Human Rights Law in Africa* (2nd edn, Oxford University Press 2012) 230-233

[20] African Commission on Human and Peoples' Rights, 'Principles and Guidelines on the Implementation of Economic, Social and Cultural Rights in the African Charter*'* (2010) <https://www.achpr.org/legalinstruments/detail?id=18> accessed 15 January 2026.

may deny financial access to low-income populations, reinforcing structural inequities.[21] In *Zimbabwe Lawyers for Human Rights v Zimbabwe***,** the African Commission emphasised that equality under the Charter requires protection against both formal and substantive discrimination, which extends to practices that, while neutral on paper, produce discriminatory effects in reality.

Dignity, enshrined in Article 5, is equally at risk. The African Commission has long emphasised that dignity underpins all Charter rights.[22] AI-driven surveillance, profiling, and automated risk scoring may reduce individuals to data points, stripping them of agency and subjecting them to pervasive monitoring. In *SERAC v Nigeria*[23], the Commission underscored that state actions undermining human living conditions and autonomy violate dignity even in the absence of physical harm.In the AI context, surveillance infrastructure, biometric ID systems, and algorithmic welfare decisions may produce dehumanising experiences, particularly for marginalised communities.

Privacy, though not explicitly codified in the Charter as a standalone article has been interpreted in conjunction with dignity, personal security, and freedom of expression.[24] The African Commission's Resolution 473 on AI and emerging technologies highlights that algorithmic systems can intrude upon personal and communal spaces, creating continuous observation networks that undermine the right to

[21] *Zimbabwe Lawyers for Human Rights v Zimbabwe* (2009) AHRLR 268

[22] African Commission on Human and Peoples' Rights, 'General Comment No 3 on the African Charter on Human and Peoples' Rights: The Right to Life' *(Article 4)* (2015) para 4, <https://www.achpr.org/legalinstruments/detail?id=17>accessed 15 January 2026

[23] *Social and Economic Rights Action Centre (SERAC) and Another v Nigeria* (2001) AHRLR 60

[24] African Commission on Human and Peoples' Rights, 'Resolution 473: Human Rights and Artificial Intelligence, Robotics and Emerging Technologies' (2021), <https://www.achpr.org/sessions/resolutions> accessed 15 January 2026.

private life. In contexts such as national digital ID systems or AI-driven social welfare platforms, inadequate safeguards may expose sensitive personal data to misuse, data breaches, and third-party commercial exploitation.[25] The Charter's emphasis on state responsibility under Article 1 to "adopt legislative or other measures" provides a legal basis for compelling states to regulate both public and private AI actors to prevent privacy violations.[26]

Procedural rights, particularly the right to a fair hearing under Article 7, face acute challenges under AI governance. Algorithmic systems often operate opaquely, providing no explanation or recourse to individuals affected by automated decisions. Denial of welfare benefits, bank loans, or access to justice on the basis of AI determinations without explanation contravenes procedural fairness. The African Commission has repeatedly stressed that fair hearing entails access to information, intelligibility of decisions, and remedies for incorrect or arbitrary determinations.[27]

Freedom of expression and access to information under Article 9 of the Charter are similarly implicated. AI-powered content moderation, automated censorship, and surveillance of online communications may chill political speech and public participation.[28] This risk is heightened in countries with historical constraints on civic space. The African Commission's Declaration of Principles on Freedom of Expression

[25] World Bank, *Identification for Development (ID4D) Global Dataset* (World Bank 2019) 33–36, <https://id4d.worldbank.org/global-dataset>accessed 15 January 2026.
[26] African Charter on Human and Peoples' Rights (adopted 27 June 1981, entered into force 21 October 1986) OAU Doc CAB/LEG/67/3/Rev.5, arts 1, 2, 3, 5, 7, 9, 19–24,
[27] *Media Rights Agenda v Nigeria* (2000) AHRLR 200 (ACHPR) paras 60–62.
[28] African Commission on Human and Peoples' Rights, '*Declaration of Principles on Freedom of Expression and Access to Information in Africa* (2019)' <https://www.achpr.org/legalinstruments/detail?id=69> accessed 15 January 2026

underscores that restrictions must be lawful, necessary, and proportionate standards often absent in AI-mediated regulation.

Beyond individual rights, the **c**ollective or peoples' rights framework of the Charter (Articles 19-24) offers a distinctive lens for addressing structural harms of AI. Algorithmic systems frequently produce collective impacts: entire communities may be surveilled, excluded from essential services, or deprived of agency over their communal data.[29] The right to development under Article 22, interpreted as both a process and an outcome, requires participatory inclusion, empowerment, and equitable distribution of benefits. AI systems deployed in development contexts may paradoxically deepen exclusion if they rely on opaque algorithms or foreign-controlled infrastructures.

Articles 20 and 21 on peoples' self-determination and resource control acquire renewed relevance in the age of AI. African populations generate massive quantities of data: biometric, social, and economic which increasingly constitute a strategic resource. [30] Where foreign technology corporations control AI infrastructure and data storage, local communities may lose agency over these resources, echoing the structural imbalances of digital colonialism. [31] In this context, the Charter provides both a normative and legal anchor for asserting digital sovereignty, ensuring that communities participate meaningfully in decisions affecting algorithmic governance.

[29] *Centre for Minority Rights Development (Kenya) and Minority Rights Group International v Kenya (Endorois case)* (2010) AHRLR 75 (ACHPR) paras 277-281.
[30] African Union, *Data Policy Framework* (2022) 9-11 <https://au.int/en/documents/20220731/african-union-data-policy-framework>accessed 15 January 2026.
[31] Nick Couldry and Ulises A Mejias, *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism* (Stanford University Press 2019) 159-165.

Despite these potentials, the African Charter's engagement with AI remains **la**rgely implicit. The African Commission and Court is yet to develop systematic jurisprudence addressing AI harms. Soft law instruments, such as resolutions on AI and digital rights, offer guidance but remain non-binding. The interpretive silence raises practical challenges: states and private actors operate in regulatory uncertainty, while affected communities have limited avenues for redress.

Comparative perspectives illustrate the Charter's potential. The European Union AI Act adopts a risk-based approach tied to fundamental rights protection.[32] The Charter, by contrast, embeds rights in a communitarian ethos, offering interpretive space to address structural harms, collective inequalities, and the broader societal impacts of algorithmic governance. Similarly, UN principles on AI ethics emphasise human-centric approaches, transparency, and accountability, which resonate with the Charter's value-driven framework. [33] The challenge is to translate these principles into enforceable mechanisms within Africa's regional and national institutional architectures.

The African Charter thus provides a robust but underutilised normative foundation for AI governance. Its people-centred vision, integration of individual and collective rights, and flexible interpretive ethos offer tools to address algorithmic harms in ways that purely technocratic frameworks cannot. Fully realising this potential requires evolutionary interpretation, proactive institutional engagement, and integration of AI-specific oversight mechanisms. Only then can the Charter serve as

[32] European Union, 'Regulation (EU) 2024/1689'-Artificial Intelligence Act' arts 1-5, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>accessed 15 January 2026.

an effective safeguard for human rights in Africa's rapidly digitalising societies.

4.0 INSTITUTIONAL AND ACCOUNTABILITY GAPS IN AI GOVERNANCE IN AFRICA

While the African Charter provides a compelling normative foundation for human rights protection in the AI context, its institutional architecture presents significant constraints. The effectiveness of AI governance under the African human rights system depends not only on the content of rights but also on the capacity of institutions to monitor, adjudicate, and enforce these rights. Across the continent, African human rights institutions, both regional and national face **s**tructural, procedural, and resource-based limitations that undermine their ability to address complex technological harms.

i. The African Commission and the African Court

The African Commission on Human and Peoples' Rights (ACHPR) is the primary regional body tasked with interpreting and supervising the implementation of the Charter. Despite its centrality, the Commission's enforcement powers are limited. It can issue recommendations, develop general comments, and adopt resolutions, but these are largely non-binding on states. Consequently, even when the Commission identifies violations of the Charter, including those arising from emerging technologies, it relies on states' voluntary compliance.

The African Court on Human and Peoples' Rights offers a judicial mechanism for addressing Charter violations, including cases involving structural or collective harms.[34] However, access to the Court is restricted. Only states and African intergovernmental organisations may bring cases directly, while individuals can only access the Court after

[34] Protocol to the African Charter on Human and Peoples' Rights on the Establishment of an African Court on Human and Peoples' Rights (1998) arts 3-5

exhausting domestic remedies and if their country has made a special declaration under Article 34(6) of the Court Protocol.[35] In practice, this procedural complexity and the low number of ratifications of the Court's jurisdiction have limited access, particularly for communities affected by AI-driven harms.

The institutional capacity of both the Commission and the Court is further constrained by resource limitations, procedural delays, and gaps in technical expertise. AI-related cases often require specialised knowledge in data analytics, algorithmic bias, and information systems fields in which regional human rights bodies currently have limited expertise.[36]Without dedicated AI or digital rights units, the Commission and Court face difficulties in evaluating technical evidence, understanding algorithmic processes, and formulating practical remedies.

ii. National Human Rights Institutions

National Human Rights Institutions (NHRIs) in African states are theoretically positioned to enforce rights domestically, investigate complaints, and monitor state compliance with the Charter.[37] However, their independence, capacity, and authority vary widely. In many cases, NHRIs are under-resourced, lack legal authority to compel disclosure from private companies, or operate within politically constrained environments. These limitations are particularly salient in the context of AI, where private technology companies dominate system design, data storage, and service delivery, often with minimal state oversight.

---

[35] Ibid, art 34(6).

[36] UN Special Rapporteur on the Promotion and Protection of Human Rights while Countering Terrorism, 'Report on Artificial Intelligence and Human Rights*'* {UN Doc A/HRC/46/36 -2021)
< https://undocs.org/A/HRC/46/36> accessed 15 January 2026.

[37] Teki Falconer, "Data Protection and Privacy in Africa" (2019) 3 *African Journal of Law and Technology* 45, 50-52.

iii. Accountability Gaps for Private Technology Actors

A significant gap in Africa's AI governance is the limited accountability of private technology actors. Multinational corporations control cloud infrastructure, AI algorithms, and data analytics systems deployed across the continent.[38] These actors often operate beyond the reach of national law, exploiting regulatory gaps and weak enforcement mechanisms. Their involvement raises issues not only of privacy and security but also of equitable development; data extracted from African populations is frequently monetised abroad, echoing patterns of historical exploitation described as digital colonialism.

While some African countries have adopted data protection laws, these laws often do not address algorithmic decision-making, AI oversight, or corporate accountability. [39] Moreover, enforcement is inconsistent. Without binding obligations or clear regulatory frameworks, corporations may implement AI systems that violate fundamental rights without consequence.

iv. Fragmented Regulatory Frameworks

The regulatory landscape in Africa is fragmented, with states enacting inconsistent laws regarding data protection, cybersecurity, and digital governance.[40] At the regional level, instruments such as the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) remain unratified by most states, limiting their

[38] Nick Couldry and Ulises A Mejias, *The Costs of Connection* (Stanford University Press 2019) 159-165.

[39] African Union, 'Data Policy Framework' (2022) 9-11 <https://au.int/en/documents/20220731/african-union-data-policy-framework.> accessed 15 January 2026.

[40] Privacy International, 'Identity Systems and Human Rights in Africa' (2020) <https://privacyinternational.org/report/3756/identity-systems-and-human-rights-africa>accessed 15 January 2026

impact.[41] This fragmentation produces gaps in oversight, leaving AI systems in a legal grey zone where neither state nor regional mechanisms can enforce rights effectively.

v. Structural Barriers

Institutional weaknesses are compounded by structural and socio-economic barriers. High poverty rates, limited digital literacy, and restricted access to legal remedies reduce the capacity of affected populations to assert their rights.[42] AI systems deployed in welfare allocation, social protection, or migration may inadvertently or deliberately exacerbate exclusion, disproportionately affecting marginalised communities. Moreover, dependence on foreign AI technologies reinforces asymmetries of power, as decisions about data storage, algorithmic design, and system governance are made outside Africa.

This constellation of factors, that is, weak regional and national institutions, accountability gaps for private actors, fragmented regulations, and socio-economic vulnerability creates a systemic governance vacuum. AI systems are thus deployed in contexts where both enforcement and oversight are minimal, heightening the risk of human rights violations.

5.0 TOWARDS STRENGTHENING INSTITUTIONAL ACCOUNTABILITY

Bridging the existing institutional gaps in AI governance requires multi-layered reforms that address both technical capacity and legal authority. Regional bodies, such as the African Commission and the African Court,

---

[41] African Union, 'Convention on Cyber Security and Personal Data Protection' (Malabo Convention, 2014) art 1, <https://au.int/en/treaties/convention-cyber-security-and-personal-data-protection> accessed 15 January 2026

[42] Virginia Eubanks, *Automating Inequality* (St Martin's Press 2018) 39-41.

must develop specialised expertise in artificial intelligence, algorithmic auditing, and digital forensics. Establishing dedicated AI units within these institutions would enable credible evaluation of algorithmic evidence and strengthen oversight of AI deployment.

At the national level, Human Rights Institutions should be empowered to supervise AI systems actively, compel transparency from private corporations, and investigate complaints from affected communities. Strengthening the powers and independence of NHRIs is critical for ensuring that AI deployment does not escape scrutiny and that rights violations can be addressed promptly.

Accountability for private technology actors is equally essential. Binding regulatory standards should govern corporations operating AI systems in Africa, while public-private cooperation frameworks could enforce rights-based deployment without undermining development objectives. In parallel, harmonisation of regional and national laws is necessary to create a coherent regulatory environment. States should ratify regional instruments such as the Malabo Convention and adopt AI-specific legislation addressing data protection, algorithmic transparency, and accountability.

Participatory governance mechanisms must be established to ensure that communities have meaningful channels for consultation and oversight. This approach ensures that AI deployment respects both individual and collective rights, allowing affected populations to influence decision-making processes that shape the technologies governing their lives. Without these comprehensive reforms, the limitations of current institutions will continue to weaken the African Charter's protective potential, leaving citizens exposed to the structural harms of algorithmic governance and digital colonialism.

6.0 BRIDGING THE GAPS: TOWARDS RIGHTS-BASED AI GOVERNANCE IN AFRICA

Effectively addressing human rights challenges posed by artificial intelligence (AI) in Africa requires a context-sensitive, rights-based approach grounded in the African Charter on Human and Peoples' Rights. Rather than simply transplanting foreign regulatory models, such an approach must integrate progressive legal interpretation, regional coordination, national legislation, corporate accountability, and participatory governance to ensure that AI technologies support development while safeguarding human rights.

A first step involves progressive interpretation of the Charter. Although the Charter predates modern AI, its provisions on dignity, equality, non-discrimination, freedom of expression, and collective rights provide a flexible framework for responding to algorithmic harms. Articles 2 and 3 can be applied to address bias in algorithmic decision-making, while Article 7 supports procedural safeguards such as transparency, contestability, and human oversight. The African Commission and Court have already demonstrated the capacity for purposive interpretation in contexts such as environmental justice and digital rights[43], indicating that AI-related harms could similarly be addressed within this framework.

Strengthening regional frameworks and soft law instruments is essential. Although the Charter provides the normative foundation, AI-specific rules are largely absent, leaving states and private actors operating in a regulatory vacuum. The African Union could lead the development of a **c**ontinental AI and human rights framework, harmonising standards across member states. Such a framework would draw on instruments

[43] African Commission on Human and Peoples' Rights, 'General Comment No 3 on the African Charter' (2015) <https://www.achpr.org/legalinstruments/detail?id=17>accessed 15 January 2026.

including the Malabo Convention on Cybersecurity and Personal Data Protection, the Digital Transformation Strategy for Africa, and the African Data Policy Framework. It should set minimum rights-based standards for AI deployment, covering algorithmic transparency, privacy protection, non-discrimination, human oversight, and community consultation, while remaining sensitive to Africa's developmental and infrastructural realities.

At the national level, legislation must ensure that AI deployment respects both individual and collective rights. Laws on data protection, cybersecurity, and algorithmic governance must address automated profiling, predictive analytics, and biometric systems. Mandatory impact assessments for AI systems should evaluate social, economic, and cultural effects before deployment. [44] National human rights institutions should be empowered to audit AI systems, investigate complaints, and enforce accountability. Countries such as Kenya, South Africa, and Ghana illustrate that domestic regulation, when aligned with regional oversight, can mitigate AI-related risks.

Private sector accountability is also crucial. Multinational technology companies control the design, operation, and management of many AI systems in Africa, often operating beyond the reach of traditional oversight.[45] Binding corporate standards, coupled with public-private cooperation frameworks, are necessary to align AI deployment with human rights obligations and development objectives.

[44] Privacy International, 'Identity Systems and Human Rights in Africa' (2020) <https://privacyinternational.org/report/3756/identity-systems-and-human-rights-africa>accessed 15 January 2026.
[45] Nick Couldry and Ulises A Mejias, *The Costs of Connection* (Stanford University Press 2019) 159–165.

Participatory governance is a crucial pillar. Communities affected by AI systems must have channels for consultation and oversight. Participatory mechanisms ensure that AI deployment respects both individual and collective rights, including principles of self-determination, resource control, and development under Articles 19-24 of the Charter. Civic education, digital literacy programs, and community consultation platforms are crucial for enabling meaningful engagement with AI governance.

Capacity-building and technical expertise are essential for both regional and national institutions. Dedicated AI units within the African Commission, African Court, and national human rights institutions could conduct algorithmic audits, assess compliance with human rights standards, and provide guidance on responsible AI deployment. Partnerships with academia, civil society, and technical experts can further strengthen institutional capacity, enabling proactive oversight rather than reactive enforcement.

Together, these measures form a multi-layered governance strategy that addresses both normative and institutional gaps. Algorithmic systems pose not only technical but also structural risks, potentially exacerbating inequalities, entrenching exclusion, and facilitating digital forms of control.[46] Africa's human rights ethos, rooted in communitarian values, social solidarity, and development-oriented rights, provides a distinctive foundation for human-centred AI governance. By integrating individual and collective protections, African institutions can chart a unique path in global AI governance debates, balancing innovation, accountability, and social justice.

[46] Virginia Eubanks, *Automating Inequality* (St Martin's Press 2018) 39–46.

Without doubt, bridging the normative and institutional gaps in Africa's AI governance requires progressive legal interpretation, regional coordination, harmonised national legislation, corporate accountability, participatory governance, and capacity-building. The African Charter provides the normative compass, while regional and national mechanisms operationalise its protections in the AI era. This multi-dimensional approach allows Africa to harness AI for development while mitigating risks to human rights, resisting digital colonialism, and fostering a human-centred technological future.

7.0 RECOMMENDATIONS AND POLICY REFORMS

To ensure that artificial intelligence (AI) deployment in Africa aligns with human rights and development objectives, the following recommendations and policy reforms are proposed. Each addresses the normative, institutional, and operational gaps identified in previous sections.

i. Progressive Interpretation of the African Charter

The African Charter on Human and Peoples' Rights provides a strong normative foundation, but its potential can only be realised through progressive interpretation. Regional bodies, including the African Commission and African Court, should issue formal guidance clarifying how Charter rights apply to AI-driven systems. This guidance should emphasise the application of principles such as human dignity, equality, privacy, and freedom of expression to algorithmic decision-making. By establishing clear interpretive standards, these bodies can reduce uncertainty, guide national legislation, and set expectations for corporate behaviour.

ii. African Union–Led AI and Human Rights Framework

A continental framework is essential to harmonise AI governance across member states. The African Union should spearhead the development

of an AI and Human Rights Framework that sets minimum standards for algorithmic transparency, human oversight, data protection, and accountability. This framework must balance legal obligations with the practical realities of Africa's digital infrastructure and development priorities. By providing a cohesive set of standards, it can prevent fragmented regulations and promote cross-border consistency in AI deployment, while protecting the rights of individuals and communities.

iii. Strengthened National Legislation

African states must update their domestic legal regimes to address AI-specific risks. Laws should require mandatory algorithmic impact assessments for any AI system affecting public services, social welfare, border control, or financial inclusion. National human rights institutions should have authority to audit AI systems, investigate complaints, and enforce compliance. Harmonisation with regional frameworks is essential to ensure that national laws do not conflict with continental standards and to facilitate coordinated oversight across borders.

iv. Private Sector Accountability

Private technology actors are central to AI deployment in Africa but often operate beyond traditional oversight. Governments should establish binding regulatory standards for corporations, including obligations to ensure transparency, enable independent audits, report publicly on AI operations, and provide remedies for rights violations. Public-private partnerships should also be structured to align commercial objectives with human rights and development goals, ensuring that corporate practices support equitable and rights-respecting technological adoption.

v. Participatory and Inclusive Governance

Communities affected by AI systems must have formal channels for consultation, contestation, and oversight. Participatory governance

mechanisms can include digital platforms, civic education initiatives, and community advisory councils. These measures empower individuals and communities to engage with AI deployment actively, ensuring that collective rights, such as resource management, social development, and self-determination, are respected. Embedding participatory mechanisms in AI governance enhances legitimacy and fosters public trust in technological systems.

vi. Capacity-Building and Technical Expertise

Both regional and national institutions must develop specialised expertise in AI, algorithmic auditing, and human rights law. Dedicated units within the African Commission, African Court, and national human rights institutions can provide technical assessment, guidance, and oversight. Partnerships with academic institutions, civil society, and technical experts are critical to build sustainable capacity. Enhanced technical knowledge ensures that authorities can proactively monitor AI systems, identify potential harms, and respond effectively when violations occur.

vii. Monitoring, Reporting, and Evaluation

To ensure accountability, states and institutions must implement robust monitoring and evaluation mechanisms. This includes public reporting by governments and corporations, independent oversight bodies, and performance benchmarks for AI systems. Regular evaluation enables the identification of emerging risks, the assessment of compliance with human rights standards, and the refinement of policy and regulatory frameworks. Continuous monitoring ensures that AI governance is adaptive, responsive, and capable of keeping pace with technological change.

viii. Multi-Layered Integration

Finally, these recommendations should be understood as interdependent and mutually reinforcing. Progressive legal interpretation guides normative clarity, continental frameworks and national legislation provide enforceable standards, corporate accountability ensures compliance, participatory governance ensures legitimacy, and capacity-building enables effective oversight. Together, these measures create a multi-layered governance system capable of realising the African Charter's promise in the AI era, mitigating risks, and harnessing technology to advance human rights and development across the continent.

8.0 CONCLUSION

Artificial intelligence presents both transformative opportunities and profound challenges for human rights in Africa. While AI can advance development, streamline public service delivery, and expand inclusion, it also carries significant risks including discrimination, surveillance, exclusion, and the entrenchment of digital inequities. Africa's distinctive socio-political context, marked by historical inequalities, infrastructural constraints, and the influence of foreign technology actors, amplifies these risks, making rights-based governance both urgent and essential.

The African Charter on Human and Peoples' Rights, though predating AI, offers a viable normative foundation for addressing these challenges. Its focus on human dignity, equality, social justice, and collective rights provides the conceptual tools to confront algorithmic harms. Yet, the potential of the Charter remains largely unrealised due to normative ambiguity, weak institutional enforcement, and fragmented regulatory systems. Without deliberate intervention, AI could exacerbate structural inequalities and reinforce forms of digital colonialism across the continent.

This article has argued that bridging these gaps requires a multi-layered, context-sensitive approach. Progressive interpretation of the Charter, harmonised regional and national frameworks, corporate accountability, participatory governance, and capacity-building are all essential pillars. By implementing these measures, African states and institutions can transform the African Charter from a declaratory instrument into an operational tool capable of guiding AI governance in a manner consistent with human rights and development objectives.

Importantly, Africa has the opportunity to lead in human-centred AI governance, offering an alternative to purely technocratic or market-driven models prevalent elsewhere. By prioritising both individual and collective rights, embedding participatory mechanisms, and ensuring institutional accountability, the continent can harness AI for inclusive growth while protecting citizens from emerging technological harms.
In conclusion, the task ahead is both legal and moral. Strengthening AI governance is not simply a matter of compliance but a commitment to ensure that technological innovation serves human dignity, equality, and sustainable development. Through coordinated reforms, African institutions can safeguard rights, resist digital authoritarianism, and chart a path toward a responsible, rights-based digital future that reflects the continent's values and priorities.