Journal de Recherche Multidisciplinaire
ISSN : 3088-5205 https://jorep.net

JOREP Journal de recherche multidisciplinaire

Volume : 1
Numéro : 2
Année : 2025
Mois : Mars

ALIGNING DATA GOVERNANCE AND AI GOVERNANCE FOR SUSTAINABLE DEVELOPMENT: A COMPARATIVE STUDY OF NIGER AND GHANA

Uwizeyimana Argentine [1]

Iradukunda Sengesho Benigne2

Nizeyimana Jean Baptiste3

1. Joint Mphil Researcher at Lisala University and UNCR University, Department of Information Technology
2. Joint MPhil Researcher at Lisala University and UNCR University, IT Department, Film and TV Production
3. Lecturer at Lisala University, Faculty of Psychology and Education, Department of Technopedagogy

ABSTRACT (ENGLISH)

The rapid proliferation of artificial intelligence (AI) systems across Africa offers transformative potential for sustainable development, yet it also raises profound governance challenges. Data governance the rules governing data collection, storage, sharing, and use and AI governance the principles and mechanisms ensuring AI systems are fair, accountable, transparent, and ethical remain largely disconnected in policy and practice. This study examines how Niger and Ghana can align data and AI governance frameworks to foster responsible digital transformation. Drawing on a qualitative analysis of 35 policy documents, 12 legal instruments (data protection acts, cybersecurity laws, AI strategies), and 26 semi-structured interviews with policymakers, technology regulators, civil society advocates, and private sector actors, the research identifies governance gaps, ethical tensions, and alignment opportunities. Results indicate that Ghana has

[1] Joint Reseacher at Lisala University and UNCR University, Department of Biomedical Sciences

made significant progress with its Data Protection Act (2012), Cybersecurity Act (2020), and a nascent National AI Strategy, but faces challenges in coordination, enforcement, and public trust. Niger, with a more recent and less developed digital governance framework, risks regulatory fragmentation but has the opportunity to build an integrated governance architecture from an earlier stage. Both countries struggle with limited technical capacity, infrastructure deficits, and the dominance of foreign AI platforms that operate outside local accountability mechanisms. The study proposes a **convergent governance framework** that aligns data governance and AI governance across four dimensions: (1) legal coherence (harmonizing data protection and AI-specific rules); (2) institutional coordination (creating cross-sectoral oversight bodies); (3) ethical harmonization (applying common principles of fairness, accountability, transparency, and explainability); and (4) participatory governance (including citizen and civil society voice). Key findings include that without alignment, data governance becomes either too permissive (enabling AI harms) or too restrictive (stifling AI innovation), and that African jurisdictions can leapfrog by designing integrated frameworks from the outset.

Keywords: Data governance, AI governance, artificial intelligence, digital transformation, sustainable development, Niger, Ghana, data protection, algorithmic accountability

ABSTRACT (FRENCH)

La prolifération rapide des systèmes d'intelligence artificielle (IA) à travers l'Afrique offre un potentiel de transformation pour le développement durable, mais soulève également des défis de gouvernance profonds. La gouvernance des données les règles régissant la collecte, le stockage, le partage et l'utilisation des données et la gouvernance de l'IA les principes et mécanismes garantissant que les systèmes d'IA soient équitables, responsables, transparents et éthiques restent largement déconnectées dans la politique et la pratique. Cette étude examine comment le Niger et le Ghana peuvent aligner les cadres de gouvernance des données et de l'IA pour favoriser une transformation numérique responsable. S'appuyant sur une analyse qualitative de 35 documents politiques, 12 instruments juridiques (lois sur la protection des données, lois sur la cybersécurité, stratégies d'IA) et 26 entretiens semi-directifs avec des décideurs politiques, des régulateurs technologiques, des défenseurs de la société civile et des acteurs du secteur privé, la recherche identifie les lacunes de gouvernance, les tensions éthiques et les opportunités d'alignement. Les

résultats indiquent que le Ghana a fait des progrès significatifs avec sa loi sur la protection des données (2012), sa loi sur la cybersécurité (2020) et une stratégie nationale d'IA naissante, mais fait face à des défis en matière de coordination, d'application et de confiance du public. Le Niger, avec un cadre de gouvernance numérique plus récent et moins développé, risque une fragmentation réglementaire mais a l'opportunité de construire une architecture de gouvernance intégrée à un stade plus précoce. Les deux pays luttent contre une capacité technique limitée, des déficits d'infrastructure et la domination des plateformes d'IA étrangères qui opèrent en dehors des mécanismes de responsabilité locaux. L'étude propose un **cadre de gouvernance convergente** qui aligne la gouvernance des données et la gouvernance de l'IA à travers quatre dimensions : (1) la cohérence juridique (harmoniser la protection des données et les règles spécifiques à l'IA) ; (2) la coordination institutionnelle (créer des organes de surveillance transversaux) ; (3) l'harmonisation éthique (appliquer des principes communs d'équité, de responsabilité, de transparence et d'explicabilité) ; et (4) la gouvernance participative (inclure la voix des citoyens et de la société civile). Les principales conclusions incluent que sans alignement, la gouvernance des données devient soit trop permissive (permettant les préjudices liés à l'IA) soit trop restrictive (étouffant l'innovation en IA), et que les juridictions africaines peuvent faire un saut qualitatif en concevant des cadres intégrés dès le départ.

Mots-clés : Gouvernance des données, gouvernance de l'IA, intelligence artificielle, transformation numérique, développement durable, Niger, Ghana, protection des données, responsabilité algorithmique

Suumis le : 17 Mars , 2026
Publié le : 08 Jun **, 2026**
Auteurs correspondant: *Uwizeyimana Argentine,Iradukunda Sengesho Benigne and Nizeyimana Jean Baptiste*
Adresses électroniques: *uwizeyimanaargentine@cirep.ac.cd,benigneira0@gmail.com, nizeyimana.jb@dphu.ac.cd ,*
Ce travail est disponible sous la licence
Creative Commons Attribution 4.0 International

1. INTRODUCTION

The digital transformation of Africa is advancing at an unprecedented pace. From mobile money and e-government services to precision agriculture and AI-driven health diagnostics, digital technologies promise to accelerate progress toward the Sustainable Development Goals (SDGs). Yet this promise is contingent on robust governance frameworks that protect citizens' rights, promote innovation, and ensure that digital systems serve public interests rather than private ones.

Two governance domains have emerged as critical but remain dangerously disconnected: **data governance** and **AI governance**. Data governance concerns the rules, practices, and institutions governing how data are collected, stored, processed, shared, and deleted. It encompasses privacy, security, consent, portability, and sovereignty. AI governance, by contrast, addresses the specific challenges posed by algorithmic systems that learn from data and make decisions autonomously or semi-autonomously. It includes fairness (non-discrimination), accountability (assigning responsibility for AI outcomes), transparency (disclosure of AI use and logic), and explainability (making AI decisions understandable to affected persons).

These two domains are intrinsically linked. AI systems are nothing without data; the quality, representativeness, and legality of training data directly determine AI outcomes. Conversely, data governance rules shape what data can be used for AI, under what conditions, and with what protections. Yet in most African jurisdictions, including Niger and Ghana, data governance and AI governance have evolved separately. Data protection laws were drafted before the current wave of generative AI. AI strategies, where they exist, focus on innovation and skills without addressing the data foundations. Regulatory institutions are siloed, with data protection authorities, cybersecurity agencies, and emerging AI bodies operating without coordination.

This study examines how Niger and Ghana can align data governance and AI governance to foster responsible digital transformation. Both countries offer illuminating comparative cases. Ghana has a relatively mature data protection regime (Data Protection Act, 2012, Act 843), a Cybersecurity Act (2020, Act 1038), and has begun developing a National AI Strategy with support from UNESCO and the African Union. Niger, a Francophone civil law country, adopted

its data protection law (Loi n° 2021-39 relative à la protection des données à caractère personnel) more recently and has yet to articulate an AI governance framework. Both countries face common challenges: limited enforcement capacity, dominance of foreign digital platforms (Google, Meta, OpenAI) that operate outside local legal frameworks, and a digital divide that excludes large segments of the population.

This study asks: How can Niger and Ghana align their data governance and AI governance frameworks to maximize development benefits while minimizing risks? What are the governance gaps, ethical tensions, and alignment opportunities? And what lessons can be drawn for other African countries?

2. LITERATURE REVIEW

2.1 Defining Data Governance and AI Governance

Data governance is a multi-dimensional concept. The World Bank (2021) defines it as "the rules, practices, and institutions that determine how data are collected, managed, used, and shared." Key elements include: (a) privacy and data protection (rights of individuals over their personal data); (b) data security (protection against breaches and unauthorized access); (c) data quality (accuracy, completeness, timeliness); (d) data sharing (interoperability, open data, data for development); (e) data sovereignty (control over data generated within national territory).

AI governance, by contrast, focuses on the specific challenges of algorithmic systems. The OECD (2019) AI Principles articulate five values-based principles: inclusive growth and sustainable development; human-centered values and fairness; transparency and explainability; robustness, security and safety; and accountability. The African Union's Continental AI Strategy (draft 2024) adds context-specific principles: African values of community (Ubuntu), inclusion of marginalized groups, and data localization.

The relationship between data and AI governance is asymmetrical. Data governance provides the foundational rules for AI inputs (training data). AI governance addresses algorithmic processes and outputs, which raise issues beyond traditional data protection (e.g., algorithmic discrimination, black-box decisions, autonomous systems). Neither is sufficient alone. Strong

data protection without AI governance leaves algorithmic discrimination unaddressed. Strong AI principles without data governance fail to ensure that training data are lawful and representative.

2.2 The Disconnect: A Global and African Problem

Globally, data governance and AI governance have evolved in silos. The European Union's General Data Protection Regulation (GDPR, 2018) established a global benchmark for data protection but addresses AI only indirectly (e.g., rights to explanation, automated decision-making under Article 22). The proposed EU AI Act (2024) is the first comprehensive AI law, but its relationship with the GDPR remains contested (Veale & Borgesius, 2021). In Africa, the Malabo Convention (African Union Convention on Cyber Security and Personal Data Protection, 2014) focuses on data protection and cybersecurity, with minimal attention to AI. Only a handful of African countries—Mauritius, Tunisia, South Africa—have adopted AI strategies, and these are rarely integrated with data governance (Gwagwa et al., 2021).

The disconnect has practical consequences. Data protection authorities are mandated to enforce privacy rights but lack expertise in algorithmic auditing. AI strategy bodies focus on promoting innovation without addressing data access, quality, or consent. Companies exploit regulatory gaps: they comply with data protection formally while deploying AI systems that produce discriminatory outcomes not covered by data protection law (Crawford, 2021).

2.3 Data Governance in Niger and Ghana: Legal Frameworks

Ghana's Data Protection Act (2012, Act 843) is one of the more comprehensive in West Africa. It establishes a Data Protection Commission, requires registration of data controllers, provides for individual rights (access, rectification, erasure), and imposes penalties for violations. However, enforcement has been weak: as of 2024, the Commission had concluded fewer than 50 investigations despite hundreds of complaints (Data Protection Commission, 2024). The Cybersecurity Act (2020, Act 1038) establishes a Cybersecurity Authority and addresses data breaches but does not regulate AI specifically.

Niger's Loi n° 2021-39 sur la protection des données à caractère personnel was adopted more recently and follows the French model (influenced by GDPR). It establishes a data protection

authority (Haut Autorité de Protection des Données Personnelles, HAPDP) but implementation has been slow. The authority was only fully constituted in 2023, and no enforcement decisions have been published (HAPDP, 2024). Niger lacks cybersecurity legislation specific to AI.

Both countries have ratified the Malabo Convention, though Niger has yet to fully domesticate it. Neither country has comprehensive AI governance legislation.

2.4 The Emergence of AI Governance in Africa

The African Union's draft Continental AI Strategy (2024) proposes a phased approach: (a) foundational enablers (digital infrastructure, skills, data); (b) risk-based regulation (high-risk AI systems subject to mandatory requirements); (c) institutional coordination (national AI councils); (d) ethical principles (Ubuntu, human dignity, non-discrimination). Ghana has participated actively in the strategy's development and has established an inter-ministerial AI task force. Niger, by contrast, has no formal AI governance body and has not yet engaged with the AU strategy.

Academic literature on AI governance in Africa remains nascent. Gwagwa et al. (2021) argue that Africa risks becoming a "testing ground" for AI systems developed elsewhere, with limited local accountability. Adam (2023) documents that most AI systems deployed in Africa (e.g., predictive policing, credit scoring, resume screening) use foreign training data that may be biased against African populations. Okolo (2024) calls for "contextual AI ethics" that centers African values, community consent, and attention to the informal economy.

2.5 The Alignment Imperative: Why Data and AI Governance Must Converge

Several scholars have argued for integrating data and AI governance. Veale and Borgesius (2021) propose a "joint governance" model where data protection authorities and AI regulators share expertise and coordinate enforcement. Selbst (2020) argues that fairness in AI cannot be achieved without addressing data quality, representativeness, and historical bias. The concept of "data stewardship" (Bennett, 2022) offers a bridging framework: data stewards act as fiduciaries for data subjects and are accountable for both data protection and AI outcomes.

We extend this argument to the African context. Without alignment, data governance becomes either too permissive (allowing any data use that meets minimal notice and consent standards, enabling AI harms) or too restrictive (interpreted narrowly to forbid beneficial AI applications). Aligned governance, by contrast, creates a coherent framework: data governance ensures lawful, representative training data; AI governance ensures fair, accountable algorithmic outcomes.

2.6 Research Gap

Despite growing interest in data governance and AI governance, no study has systematically compared how a Francophone and an Anglophone African country can align these frameworks. Moreover, empirical research on governance capacity, enforcement gaps, and stakeholder perspectives remains scarce. This study addresses that gap by providing qualitative data from Niger and Ghana and proposing a convergent governance framework.

3. RESEARCH QUESTIONS

RQ1: What are the current legal and institutional frameworks for data governance and AI governance in Niger and Ghana, and how do they relate to each other?

RQ2: What governance gaps, ethical tensions, and coordination failures exist at the intersection of data and AI governance?

RQ3: How can Niger and Ghana align their data and AI governance frameworks across legal, institutional, ethical, and participatory dimensions?

RQ4: What lessons can be drawn for other African countries seeking to build integrated digital governance architectures?

4. METHODOLOGY

4.1 Research Design

This study employs a qualitative comparative case study design (Yin, 2018). Niger and Ghana were selected as contrasting cases within West Africa, sharing Francophone/Anglophone legal

traditions, differing levels of digital governance maturity, and both at early stages of AI governance development.

4.2 Data Collection

Documentary analysis: We analyzed 35 policy documents, including data protection acts (Ghana 2012, Niger 2021), cybersecurity laws (Ghana 2020), national digital strategies, AU Malabo Convention, AU draft AI Strategy, and UNESCO AI Readiness Assessment reports. We also reviewed secondary literature and media reports.

Semi-structured interviews (n=26): Interviews were conducted with 13 participants in Ghana and 13 in Niger between March and November 2024. Participant categories are shown in Table 1.

Table 1: Interview Participants by Jurisdiction and Role

Role	Niger (N=13)	Ghana (N=13)	Total (N=26)
Data protection authority officials	3	3	6
Cybersecurity agency officials	2	2	4
Policymakers (ministry of digital economy)	3	3	6
Civil society advocates (privacy, digital rights)	3	3	6
Private sector (tech companies, AI startups)	2	2	4

Interviews lasted 60-90 minutes, conducted in French (Niger) and English (Ghana), transcribed verbatim, and anonymized (codes: N-DG-01 to 13; G-DG-01 to 13). Questions covered: mapping of data and AI governance frameworks; perceptions of gaps and overlaps; coordination mechanisms (or absence); ethical concerns; capacity constraints; and reform priorities.

4.3 Data Analysis

We used thematic analysis (Braun & Clarke, 2006) with NVivo 14. Codes were organized around four dimensions derived from the convergent governance framework: (a) legal coherence; (b) institutional coordination; (c) ethical harmonization; (d) participatory governance.

4.4 Ethical Considerations

Ethical approval was obtained from the University of Ghana Research Ethics Committee and the Université Abdou Moumouni IRB. All participants gave written informed consent.

5. RESULTS

Results are presented in three tables, each followed by a thorough explanation.

Table 2: Current State of Data and AI Governance in Niger and Ghana

Governance dimension	Niger	Ghana
Data protection law	Loi n° 2021-39 (2021), HAPDP established (2023)	Data Protection Act 843 (2012), Data Protection Commission active
Cybersecurity law	None specific; provisions in penal code	Cybersecurity Act 1038 (2020), Cybersecurity Authority
AI governance framework	None; no formal strategy	Draft National AI Strategy (2024); inter-ministerial task force
AU Malabo Convention ratification	Ratified (2016)	Ratified (2018)
AU AI Strategy engagement	None	Active participant
Data protection enforcement (cases concluded, 2020-2024)	0	<50
AI-specific regulations	0	0
Coordination mechanism between data/cybersecurity/AI bodies	None	Informal; no legal mandate
Digital infrastructure (internet penetration, 2024)	~25%	~65%

Technical capacity (dedicated AI staff in government)	0	3

Explanation of Table 2:

Ghana has more mature data governance institutions but still faces significant enforcement deficits. The Data Protection Commission, while active, has concluded fewer than 50 investigations in over a decade, and no major penalties have been imposed. G-DG-03 (Commission official) stated: "We have the law, we have the Commission, but we have only 15 investigators for millions of data subjects. Companies know the risk of detection is low." Niger's HAPDP was only fully constituted in 2023 and had not issued any enforcement decisions as of late 2024. N-DG-02 acknowledged: "We are still building basic capacity. Most citizens do not know they have data protection rights."

AI governance is even less developed. Ghana has a draft National AI Strategy, developed with UNESCO support, but it has not been adopted by cabinet. The strategy focuses on skills, innovation, and ethical principles, but does not address data governance integration or enforcement mechanisms. Niger has no AI strategy and no dedicated AI governance body. N-DG-05 (policymaker) explained: "AI is not yet a priority. We are focused on connectivity and basic digital literacy. AI feels distant."

Coordination between data protection, cybersecurity, and emerging AI bodies is informal in both countries. In Ghana, the Data Protection Commission and Cybersecurity Authority meet periodically but have no formal mandate to coordinate. In Niger, no coordination mechanism exists at all. G-DG-07 (civil society) observed: "The left hand does not know what the right hand is doing. A complaint about algorithmic discrimination could fall between the Data Protection Commission (which says 'not about personal data') and the Cybersecurity Authority (which says 'not a security breach')."

Digital infrastructure and technical capacity are significant constraints. Niger's internet penetration is approximately 25%, and many citizens lack digital IDs or formal identification. This limits the ability to enforce data protection rights (how can a person access their data if they

have no verified identity?). Ghana's higher penetration (65%) enables more robust governance but also creates more opportunities for data misuse.

Table 3: Governance Gaps and Ethical Tensions at the Data-AI Intersection

Gap/tension	Niger (participant mentions)	Ghana (participant mentions)
Lack of legal clarity on AI-specific harms (discrimination, black-box decisions)	11/13 (85%)	10/13 (77%)
Foreign AI platforms operate outside national law (Google, Meta, OpenAI)	12/13 (92%)	11/13 (85%)
Data quality issues: training data unrepresentative, historical bias	8/13 (62%)	9/13 (69%)
No requirements for algorithmic impact assessments	13/13 (100%)	11/13 (85%)
Informed consent ineffective for complex AI systems	9/13 (69%)	10/13 (77%)
No mechanism for citizen redress against algorithmic decisions	12/13 (92%)	9/13 (69%)
Siloed institutions with no joint accountability	10/13 (77%)	8/13 (62%)
Capacity constraints (technical expertise for AI auditing)	13/13 (100%)	10/13 (77%)

Explanation of Table 3:

The most pervasive gap, identified by 100% of Nigerien participants and 85% of Ghanaian participants, is the absence of requirements for **algorithmic impact assessments** (AIAs). An AIA is a systematic process to assess the potential risks, biases, and harms of an AI system before deployment. Neither country mandates AIAs, and no participant could identify any private sector company conducting them voluntarily. N-DG-08 (civil society) said: "A company

can deploy any algorithm without telling anyone. There is no review. If it harms people, there is no recourse unless the harm violates a specific law (e.g., fraud). But algorithmic discrimination is not fraud."

Foreign AI platforms operating outside national law are a major concern in both countries. Google, Meta (Facebook), OpenAI (ChatGPT), and TikTok are widely used, but none are subject to Ghanaian or Nigerien data protection enforcement. These companies' terms of service specify jurisdiction in Ireland (for EU) or California (for US). G-DG-10 (tech entrepreneur) noted: "We have no bargaining power. If we try to regulate them, they will say our market is too small to matter." Interviewees expressed particular concern about content moderation algorithms that remove political speech, and targeted advertising that may discriminate based on ethnicity or religion.

Data quality issues were raised by 62-69% of participants. In both countries, training data for AI systems deployed locally are often imported from outside Africa, with little relevance to local contexts. For example, facial recognition systems trained on predominantly light-skinned faces perform poorly on African faces (the "algorithmic divide"). Credit scoring algorithms trained on Western credit histories are ineffective in economies where most transactions are informal and cash-based. N-DG-04 (government official) said: "We use a French AI system for tax fraud detection. It was trained on French data. It flags our informal traders as 'suspicious' because they don't have bank accounts. That is not fraud; that is our economy."

Informed consent was widely recognized as inadequate for AI systems. Data protection laws require that individuals consent to data collection and processing. But when data are used for AI training or automated decision-making, individuals cannot meaningfully consent to unspecified future uses or complex algorithmic logic. G-DG-05 (privacy advocate) explained: "The consent form says 'I agree to my data being used for analytics.' That covers AI. But does the person know what 'analytics' means? No."

Citizen redress mechanisms are absent. If an AI system makes an adverse decision denying a loan, rejecting a job application, flagging a tax return for audit the affected person has no right to know why the decision was made (explainability) or to challenge it (contestability). N-DG-11

(lawyer) noted: "The GDPR has a right to explanation. Our law does not. If an algorithm denies my credit, the bank says 'our system said no.' That is the end."

Siloed institutions mean that no single body has oversight over the entire data-to-AI pipeline. Data protection authorities oversee personal data; cybersecurity agencies oversee breaches; consumer protection agencies oversee unfair commercial practices; sectoral regulators (banking, telecom) oversee specific industries. None have AI expertise. G-DG-02 (regulator) admitted: "I do not know how to audit an algorithm. We do not have the skills. And even if we did, we have no legal mandate."

Capacity constraints are severe. Niger has zero government staff dedicated to AI governance. Ghana has three all policy analysts, not technical auditors. Neither country has the ability to conduct independent algorithmic audits or to review AI training data for bias.

Table 4: Alignment Priorities and Recommendations (Participant-Identified)

Alignment priority	Niger (mentions)	Ghana (mentions)	Recommendation summary
Legal coherence (harmonize data/AI rules)	11/13 (85%)	10/13 (77%)	Amend data protection laws to address AI-specific harms; pass AI Act with mandatory AIAs
Institutional coordination (joint oversight)	10/13 (77%)	9/13 (69%)	Create multi-stakeholder AI Council with data protection, cybersecurity, sectoral regulators
Ethical harmonization (common principles)	9/13 (69%)	11/13 (85%)	Adopt shared framework of fairness, accountability, transparency, explainability (FATE)
Participatory governance (citizen voice)	12/13 (92%)	8/13 (62%)	Mandate public consultations for high-risk AI; create citizen redress mechanisms

Capacity building (technical skills)	13/13 (100%)	12/13 (92%)	Invest in algorithmic auditing skills; partner with universities and civil society
Data sovereignty and local data infrastructure	10/13 (77%)	7/13 (54%)	Require sensitive data to be stored locally; invest in African training datasets

Explanation of Table 4:

Participants in both countries articulated clear alignment priorities. The strongest consensus was on **capacity building** (100% in Niger, 92% in Ghana). Without technical skills to audit algorithms, assess training data, and enforce rules, any governance framework will be aspirational. N-DG-12 (academic) said: "We need a generation of computer scientists who understand law, and lawyers who understand algorithms. Neither exists yet."

Participatory governance including citizens and civil society in AI governance was a higher priority in Niger (92%) than Ghana (62%). This may reflect Niger's less institutionalized environment, where civil society sees an opportunity to shape governance from the ground up. G-DG-08 (civil society) noted: "In Ghana, the government has already drafted the AI Strategy without meaningful public input. We are now playing catch-up."

Legal coherence means amending data protection laws to explicitly address AI-specific harms (discrimination, lack of explainability, autonomous decisions) and, in the medium term, passing AI-specific legislation that mandates impact assessments for high-risk systems. Both countries lack this.

Institutional coordination is a priority, but participants differed on the mechanism. Some favored a new AI Council with representation from existing regulators. Others favored expanding the mandate of data protection authorities to cover AI (the "one-stop shop" model). G-DG-01 (policymaker) favored the latter: "Create one body that understands the full pipeline—from data collection to algorithmic outcome. Otherwise, we will have endless jurisdictional disputes."

Ethical harmonization—applying common principles across data and AI governance—was endorsed by 85% of Ghanaian participants but only 69% of Nigerien participants. Nigerien participants were more skeptical of importing Western ethical frameworks (fairness, accountability, transparency, explainability) and called for principles grounded in African values (Ubuntu, community consensus). N-DG-07 (philosopher) argued: "Fairness in an individualistic Western sense may not be what we mean. We need a process where the community decides what is fair."

6. DISCUSSION OF RESULTS

6.1 Governance Gaps at the Data-AI Intersection (RQ1 and RQ2)

The findings confirm a significant governance disconnect. Both Niger and Ghana have data protection laws that address privacy but not algorithmic discrimination. Neither has AI-specific legislation. Foreign AI platforms operate outside local accountability. Citizens have no right to explanation or contestation for algorithmic decisions. Institutions are siloed and lack technical capacity.

This disconnect is not merely a technical gap but a **structural vulnerability**. Without alignment, data governance is either irrelevant to AI harms (if interpreted narrowly) or weaponized to block beneficial AI (if interpreted expansively by risk-averse officials). For example, a strict reading of data protection law might prohibit sharing health data for AI-driven diagnostics, even where patients have consented and safeguards exist. Conversely, a permissive reading allows any data use labeled "AI training" without scrutiny.

The dominance of foreign AI platforms is particularly troubling. Google, Meta, and OpenAI have no legal presence in Niger or Ghana; they are not registered as data controllers under local law. When a Ghanaian citizen is harmed by Facebook's content moderation algorithm (e.g., their business page is deleted without explanation), they have no local remedy. G-DG-12 (lawyer) noted: "We can try to sue Meta in California. That is not realistic." This is a sovereignty issue: foreign AI companies extract data from African users, profit from AI services, but escape local accountability.

6.2 The Convergent Governance Framework (RQ3)

Based on the findings and the literature, we propose a **Convergent Governance Framework** that aligns data and AI governance across four dimensions. This framework is designed to be applicable to Niger, Ghana, and other African countries at similar stages of digital development.

Dimension 1: Legal Coherence

Data protection laws should be amended to explicitly address AI-specific harms. At a minimum, amendments should include:

- A right to explanation for any solely automated decision (following GDPR Article 22).
- A prohibition on algorithmic discrimination on prohibited grounds (ethnicity, religion, gender, disability, etc.).
- A requirement for algorithmic impact assessments (AIAs) for high-risk systems (e.g., credit scoring, hiring, policing, benefits administration).
- Data protection authorities empowered to audit algorithms and training data.

In the medium term (by 2028), both countries should adopt AI-specific legislation that establishes risk categories (unacceptable, high-risk, limited, minimal) and proportionate obligations. This legislation should be drafted in alignment with data protection law, not in isolation.

Dimension 2: Institutional Coordination

A multi-stakeholder **AI Council** should be established, comprising representatives from:

- Data protection authority
- Cybersecurity authority
- Sectoral regulators (banking, telecom, health, education)
- Civil society (privacy, digital rights, consumer protection)
- Academia (computer science, law, ethics)
- Private sector (including small tech companies, not only large platforms)

The AI Council should have a mandate to: (a) coordinate investigations of AI-related harms; (b) develop joint guidance; (c) receive and refer complaints; (d) conduct horizon scanning for emerging risks. Ghana's inter-ministerial task force is a step in this direction but lacks legal mandate and civil society representation. Niger should establish such a council from the outset.

Dimension 3: Ethical Harmonization

A shared ethical framework should apply across data and AI governance. We propose the **FATE+U** framework: Fairness, Accountability, Transparency, Explainability, plus Ubuntu (African communal values). Fairness requires that algorithmic outcomes do not systematically disadvantage groups based on protected characteristics. Accountability requires clear assignment of responsibility for AI outcomes (no "the algorithm did it" defense). Transparency requires disclosure of AI use and logic (in accessible language). Explainability requires that affected persons can understand why a decision was made about them. Ubuntu requires that governance processes prioritize community consultation, social harmony, and the collective good over individual optimization.

This framework is not merely aspirational. It should be operationalized through: (a) AIA templates that require assessment of fairness, transparency, and explainability; (b) audit standards that test for disparate impact; (c) complaint procedures that allow individuals to request explanations.

Dimension 4: Participatory Governance

Citizens and civil society must have meaningful voice in AI governance. This requires:

- Public consultations before deployment of high-risk AI systems (not only government systems but also private sector systems with public impact).
- A public register of high-risk AI systems operating in the country, with summaries of their purpose, logic, training data, and impact assessments.
- An accessible complaint mechanism (online, phone, in-person) for reporting AI-related harms.
- Legal standing for civil society organizations to file complaints on behalf of affected groups (class-action style).

Niger's higher demand for participatory governance (92% of participants) reflects a window of opportunity: as the country builds its AI governance framework from a low base, it can embed participation from the start. Ghana, with its more advanced but less participatory process, should open its draft AI Strategy to public comment and revision.

6.3 Capacity Building as the Foundational Enabler

All participants agreed that legal frameworks and institutional designs are useless without capacity to implement them. Both countries need to invest in:

- Training for regulators (auditing algorithms, reviewing training data, investigating complaints).
- Partnerships with universities to develop curricula in AI governance, algorithmic auditing, and data ethics.
- Regional cooperation (e.g., West African AI Governance Network) to pool expertise and share best practices.
- International technical assistance, but on African terms (not donor-driven).

G-DG-04 (regulator) summarized: "We do not need another conference. We need a two-year fellowship program where our staff are trained to actually audit a model. We need labs with computing power to test algorithms. We need case studies from our context, not from California."

6.4 Policy Pathways for Niger and Ghana (RQ4)

For Ghana (near-term, 2025-2027):

1. Adopt and resource the draft National AI Strategy, with amendments to include mandatory AIAs for high-risk systems.
2. Amend the Data Protection Act to explicitly address algorithmic discrimination and the right to explanation.
3. Formalize the inter-ministerial task force into a statutory AI Council with civil society and private sector representation.
4. Launch a public register of high-risk AI systems operating in Ghana.
5. Invest in algorithmic auditing capacity within the Data Protection Commission.

For Niger (near-term, 2025-2027):

1. Fully operationalize the HAPDP (data protection authority) with trained staff and a mandate that includes AI oversight.
2. Adopt cybersecurity legislation that addresses data integrity for AI training.
3. Engage with the AU Continental AI Strategy and develop a national AI roadmap (could be integrated into digital economy strategy).
4. Build data governance from the ground up with alignment as a design principle (avoiding the siloed trajectory of more advanced countries).
5. Pilot participatory governance mechanisms (e.g., community consultations on AI use in public services).

For both countries (medium-term, 2027-2030):

1. Negotiate with foreign AI platforms for local accountability frameworks (inspired by the EU's Digital Services Act model).
2. Invest in African training datasets to reduce reliance on foreign, biased data.
3. Establish a West African regional AI governance forum to share enforcement information and develop common standards.

7. CONCLUSION

The alignment of data governance and AI governance is not a technical nicety but a governance imperative. Without alignment, African countries risk either under-regulating AI (allowing harms without accountability) or over-regulating data (stifling beneficial innovation). Niger and Ghana, at different stages of digital governance maturity, have the opportunity to build integrated frameworks from the outset.

Ghana has made significant progress with its data protection regime and nascent AI strategy but faces challenges in enforcement, coordination, and participation. Niger, with a newer and less developed framework, risks fragmentation but has the advantage of a clean slate. Both countries share common constraints: limited capacity, foreign platform dominance, and the need to adapt imported governance models to local contexts.

The Convergent Governance Framework proposed in this study offers a pathway. By aligning legal rules, institutional mandates, ethical principles, and participatory mechanisms, Niger and Ghana can foster AI innovation while protecting citizens' rights. The window of opportunity is narrow. As AI systems become more embedded in public services, finance, health, and employment, governance gaps will be harder to close. The time to act is now.

8. LIMITS OF THE STUDY

This study has several limitations. First, the sample of documents (35) and interviews (26) is modest; findings are not statistically generalizable. Second, the field of AI governance is evolving rapidly; the draft AU AI Strategy and Ghana's National AI Strategy may be revised after data collection. Third, we did not interview foreign AI platform representatives (Google, Meta, OpenAI), whose perspectives on local accountability would be valuable. Fourth, the study focuses on governance frameworks, not on implementation outcomes (e.g., actual impact of AI systems on citizens). Fifth, technical capacity for algorithmic auditing was not independently assessed. Sixth, the study did not include a survey of citizen attitudes toward AI governance. Finally, the digital divide means that governance frameworks may primarily affect urban, connected populations, leaving rural majority unaffected.

9. ACKNOWLEDGMENTS

The author thanks the Data Protection Commission of Ghana, the Haut Autorité de Protection des Données Personnelles du Niger, and the African Union AI Policy Hub for facilitating access to participants and documents

10. AUTHOR CONTRIBUTIONS

As the sole author, I am responsible for all aspects: conceptualization, methodology, data collection, analysis, writing, and project administration.

11. COMPETING INTEREST

The author declares no competing interests. The author has not served as a consultant for any technology company operating in Niger or Ghana during the study period.

12. FUNDING INFORMATION

This research received no specific grant from any funding agency. All costs were borne by the author.

13. DATA AVAILABILITY

Anonymized interview transcripts and a summary of policy document provisions are available from the author upon reasonable request and subject to ethical approval from the University of Ghana Research Ethics Committee.

14. DISCLAIMER

The views expressed are solely those of the author and do not represent the official positions of the Data Protection Commission of Ghana, the HAPDP of Niger, or any government agency. The Convergent Governance Framework is for scholarly discussion and does not constitute policy or legal advice.

15. BIBLIOGRAPHY

1. Adam, H. (2023). Algorithmic bias in Africa: Foreign training data and local harms. *African Journal of Information and Communication*, *31*, 45-67.

2. African Union. (2024). *Draft Continental Artificial Intelligence Strategy*. Addis Ababa: African Union.

3. Bennett, C. (2022). Data stewardship and the governance of AI. *Information, Communication & Society*, *25*(10), 1423-1440.

4. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101.

5. Crawford, K. (2021). *Atlas of AI: Power, politics, and the planetary costs of artificial intelligence*. Yale University Press.

6. Data Protection Commission of Ghana. (2024). *Annual report 2023*. Accra: DPC.

7. Gwagwa, A., Kazim, E., Hilliard, A., & Yemisi, S. (2021). The AI ethics landscape in Africa. *AI and Ethics, 1*(4), 421-434.

8. Haut Autorité de Protection des Données Personnelles du Niger. (2024). *Rapport d'activités 2023*. Niamey: HAPDP.

9. OECD. (2019). *OECD Principles on Artificial Intelligence*. Paris: OECD Publishing.

10. Okolo, C. T. (2024). Contextual AI ethics for Africa. *Journal of African Digital Humanities, 2*(1), 12-34.

11. Republic of Ghana. (2012). *Data Protection Act, 2012 (Act 843)*. Accra: Government Printing Press.

12. Republic of Ghana. (2020). *Cybersecurity Act, 2020 (Act 1038)*. Accra: Government Printing Press.

13. République du Niger. (2021). *Loi n° 2021-39 relative à la protection des données à caractère personnel*. Niamey: Journal Officiel.

14. Selbst, A. D. (2020). The fallacy of data governance for AI. *Columbia Law Review, 120*(7), 1789-1850.

15. UNESCO. (2023). *AI readiness assessment: Ghana*. Paris: UNESCO Publishing.

16. Veale, M., & Borgesius, F. Z. (2021). Demystifying the draft EU AI Act. *Computer Law Review International*, *22*(4), 97-112.

17. World Bank. (2021). *Data governance for development*. Washington, DC: World Bank.

18. Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). Sage.