

AI regulation and democratic integrity in West Africa: Policy responses to data, platforms, and misinformation

Habeeb Adisa

Abstract

This paper examines artificial intelligence as a democratic governance problem in West Africa, with Nigeria as the principal case and Ghana, Senegal, Benin, and ECOWAS as regional comparators. Existing AI governance debates often treat data protection, platform regulation, electoral misinformation, digital identity, surveillance, and algorithmic bias as separate issues. This paper identifies separation as the central gap. It argues that, in weakly institutionalised democratic settings, AI operates not only as a tool for innovation or service delivery but also as a technology of classification, visibility, persuasion, exclusion, and public Power. The paper therefore develops a democratic data integrity framework built around five audit questions: whether data are lawful and representative; whether models are locally tested for bias and error; whether public institutions can explain and review automated decisions; whether affected citizens can obtain correction or remedy; and whether electoral and civic spaces remain open under platform Power and synthetic media. Using an analytical policy-review method, the paper compares official AI strategies, data protection laws, electoral reports, fact-checking evidence, regulatory actions, digital identity records, regional instruments, and recent African peer-reviewed research. It finds that the main challenge in West Africa is not the total absence of rules. Nigeria has adopted a national AI strategy, established a statutory data protection commission, used biometric electoral technologies, and created electoral AI capacity. Ghana has an AI strategy and data protection regime, while Senegal, Benin, ECOWAS, and the African Union provide wider regional reference points. The weakness lies in implementation, procurement transparency, audit capacity, surveillance oversight, platform accountability, and accessible remedies for ordinary citizens. The paper concludes that high-risk AI in West Africa should be treated as a form of public Power that must be lawful, contestable, auditable, and democratically accountable.

Keywords: Artificial Intelligence, Algorithmic Bias, Civil Liberties, Data Protection, Elections.

Habeeb Adisa, adisahabeeb11@gmail.com, University of Ibadan, Oyo State, Nigeria

The Nigerian Journal of Business and Social Sciences, Volume 13, 2026 (Special Issue)
A Journal of the Faculty of Social Sciences, University of Lagos, Akoka, Lagos, Nigeria
© 2026

1. Introduction

Artificial intelligence has entered West African governance through public administration, platform politics, financial technology, biometric identity systems, electoral management, security analysis, and synthetic media. Governments now discuss AI in relation to service delivery, fraud detection, public health planning, agriculture, Education, tax administration, and elections. Private firms also use scoring systems, recommendation tools, biometric checks, automated moderation, and synthetic-content tools to classify users and distribute opportunities. These developments are not only technical. They affect how institutions see citizens, how public authority is exercised, and how political claims move through society.

The problem addressed in this paper is that AI governance in West Africa is developing faster than the institutional safeguards needed to control its democratic effects. Much of the global literature on AI governance focuses on fairness, transparency, privacy, accountability, and human oversight. Those ideas are useful, but they are often framed around stronger regulatory systems, larger compliance industries, and better-resourced courts. In West Africa, the same principles operate in a different setting: records are incomplete, procurement is often opaque, regulatory agencies are underfunded, platforms are foreign-owned, and citizens may have weak access to remedies when digital systems make mistakes.

Nigeria is the central case because of its size, digital market, intense electoral politics, and recent policy activity. The country has developed a national AI strategy, expanded the National Identification Number system, used biometric voter registration and accreditation, created a statutory data protection commission, and faced repeated disputes over election-related misinformation. These developments make Nigeria a useful case for examining how AI governance operates in contexts where democratic institutions are active but uneven, where digital ambition is high. Still, public trust is fragile, and where platform politics intersects with older problems of ethnicity, religion, insecurity, and class inequality.

The regional frame is also important. Claims about elections, coups, terrorism, health, migration, religion, and ethnicity can move quickly across borders through WhatsApp, Facebook, TikTok, radio clips, diaspora networks, and translated screenshots. Vendors also sell biometric, surveillance, financial, and analytics systems across neighbouring countries. Cloud storage, data transfers, payment systems, platform moderation, and cybercrime investigations do not stop at national borders. A rumour that begins in Nigeria may circulate in Ghana, while a coup narrative from the Sahel may influence coastal states. This makes AI governance a national and regional problem.

This paper argues that AI governance should be understood as part of democratic governance. The issue is not only whether a model is accurate, efficient, or innovative. The question is whether the data are lawful and representative, whether models are locally tested for bias, whether institutions can explain and review automated decisions, whether citizens can challenge errors, and whether civic space remains open as political communication becomes more automated and synthetic. The paper's contribution is to bring these questions together as a practical democratic audit for West African policy and scholarship.

2. Method, Evidence Base, and Contribution

This article is an analytical policy review. It does not present new interviews, a new survey, a technical model audit, a procurement-contract database, or an experiment on misinformation exposure. That limitation is deliberate and should be stated clearly. The article uses available policy, legal, regulatory, electoral, and scholarly evidence to build a framework for assessing when the use of AI becomes a democratic governance problem. It therefore contributes to conceptual and policy analysis rather than claiming primary empirical measurement.

Documents were selected according to four criteria. First, they had to address AI, data protection, digital identity, electoral integrity, platform governance, misinformation, surveillance, or automated decision-making in Africa or in a directly relevant global regulatory

setting. Second, they had to come from credible sources such as official state institutions, ECOWAS, the African Union, electoral bodies, data protection authorities, reputable civil society organisations, peer-reviewed journals, or recognised international organisations. Third, they had to be current enough to reflect the recent AI policy environment, with priority given to materials from 2021 onward, while retaining older legal instruments where they remained in force. Fourth, they had to provide evidence that could be compared across Nigeria, Ghana, Senegal, Benin, ECOWAS, and wider African governance debates.

The analysis proceeded through thematic comparison. The materials were read for recurring governance mechanisms, including data quality, bias, procurement, institutional accountability, citizen remedy, platform influence, misinformation, and surveillance oversight. Country evidence was then compared to identify common patterns and local differences. Nigeria received greater attention due to its population size, digital market, electoral experience, and recent AI policy activity. At the same time, Ghana, Senegal, Benin, ECOWAS, and the African Union served as regional comparators. This method cannot replace fieldwork, but it improves transparency by showing how the evidence was selected, grouped, and interpreted.

The paper's originality lies in the democratic data integrity framework. Existing AI ethics language often invokes fairness, transparency, accountability, privacy, and human oversight. Those terms remain useful, but they can be too general for public institutions that must decide whether to deploy a specific high-risk system. This paper translates those broad principles into five practical audit questions about data, models, institutions, remedies, and civic space. The framework is meant to help scholars, regulators, electoral bodies, civil society groups, and public agencies assess AI as a form of public Power rather than as a neutral technical instrument.

3. Conceptual Framework: Democratic Data Integrity

AI is used here in a broad governance sense. It includes machine-learning models, recommender systems, large language models, facial recognition, biometric matching, predictive analytics, automated scoring, synthetic media tools, and algorithmic systems used to rank, classify, identify, recommend, verify, or exclude. This broad definition is necessary because the most consequential AI-related systems in West Africa may not be frontier models. They may be ordinary classification systems used in welfare access, credit scoring, digital identity, policing, border control, tax enforcement, platform visibility, or election communication.

The democratic data integrity framework draws from three bodies of thought. The first is democratic accountability, which requires public Power to be justified, reviewable, and open to challenge. The second is data ethics, which asks whether data are collected lawfully, used fairly, protected securely, and interpreted in ways that respect human dignity. The third is political economy, which asks who owns systems, who controls data, who benefits from opacity, and who bears the cost of error. Bringing these traditions together helps explain why AI risk in West Africa is not only technical. It is also institutional and political.

Data integrity is the first dimension. If data are incomplete, biased, outdated, unlawfully collected, or poorly documented, the system will carry those problems forward. This can happen even when the software appears advanced. Birth registration may be incomplete. Address systems may be weak. Informal work may not be properly recorded. Rural people, displaced citizens, and people without stable documentation may also be less visible in digital records. An automated system may then treat ordinary social conditions as risk, fraud, ineligibility, or non-compliance.

Model integrity is the second dimension. A tool that performs well in One context may fail in another because local data, language, infrastructure, and institutional use differ. Facial recognition trained mainly outside African contexts may misread some faces more than others,

and content moderation trained on standard English may fail when harmful messages are coded through Pidgin, Hausa, Yoruba, Igbo, Wolof, Twi, or mixed-language posts. The issue is not only technical bias. It is the conversion of social inequality into automated judgment.

Institutional integrity and remedy form the third and fourth dimensions. AI systems do not govern on their own. Ministries, electoral bodies, banks, police units, immigration agencies, regulators, and platform companies choose data sources, define risk categories, buy systems from vendors, set thresholds, and decide what happens when a person is flagged. A person wrongly denied a SIM registration, bank account, public benefit, school placement, loan, travel document, or voter accreditation therefore needs a route for correction. That route must be practical, affordable, and timely. Without remedy, automated error becomes administrative fate.

Civic openness is the fifth dimension. AI affects democracy through information, not only through individual decisions. Generative AI makes fake audio, misleading images, forged documents, false endorsements, and local propaganda easier to produce, while recommendation systems can spread outrage because outrage attracts engagement. Surveillance technology may discourage protest, journalism, and opposition activity. The five dimensions interact as a chain: weak data weaken models, weak models shape institutional decisions, weak institutions block remedy, and blocked remedy reduces civic trust. This is why the framework treats AI governance as democratic data integrity rather than as software ethics alone.

Table 1: Democratic Data Integrity Framework

Audit question	Governance concern	Practical safeguard
Are the data lawful and representative?	Incomplete or biased records can turn inequality into automated exclusion.	Purpose limitation, data-quality review, correction rights, and inclusion testing.
Has the model been tested locally?	Imported or poorly trained systems may fail across language, gender, region, class, or disability.	Bias testing, local validation, explainability review, and independent audit.
Is the institution accountable?	Vague mandates and vendor-led procurement can make public Power opaque.	Clear legal basis, procurement disclosure, audit access, and public registers.
Can citizens obtain a remedy?	Automated errors can deny services without a realistic appeal route.	Human review, assisted complaint channels, time-bound correction, and judicial oversight.
Does civic space remain open?	AI can be used for citizen monitoring, political pressure, the spread of false information, and unfair platform influence.	Clear election rules, surveillance controls, disclosure duties, and civil society oversight.

4. West Africa and Global AI Governance Models

The European Union now has a strong influence on global AI governance. The GDPR made rights-based data protection more important internationally, while the EU AI Act introduced a risk-based system for high-risk AI. These instruments matter for West Africa because they affect multinational companies, donor programmes, technical assistance, and legal thinking. They also show that voluntary ethics are not enough. When automated systems affect public life, there must be risk classification, enforcement powers, documentation, transparency, and rights for affected persons.

The EU model cannot be copied directly. It works in a setting with stronger courts, better-funded regulators, larger compliance industries, bigger public budgets, and a longer history of official documentation. West African regulators face different conditions. Budgets are smaller. There are fewer technical staff. Courts may move slowly. Public records may be incomplete or scattered. Governments may also depend more heavily on foreign vendors and donor-backed digital projects. The question is therefore not whether West Africa should accept or reject global models. The real question is how global principles can be adjusted to local institutional capacity and political economy. International technology firms and external partners shape this policy space. Platform companies control much of the infrastructure through which political information circulates. Cloud providers, biometric vendors, cybersecurity firms, and analytics companies also influence what governments can buy and inspect. Donor agencies and international organisations can help build regulatory capacity, but they may also promote templates that do not fully match local enforcement conditions. Regional AI governance must therefore address Power asymmetries between states, vendors, platforms, and citizens. Otherwise, formal rules may exist while the most important decisions remain inside contracts, technical standards, and private platform systems.

Nigeria shows why adaptation matters. A high-risk AI regime would be weak if it classified systems carefully but did not control procurement contracts. A transparency rule would also have limited value if citizens cannot read official notices or reach a complaints office. Data protection rights would be weaker if public agencies are exempt in practice or if citizens fear retaliation when challenging security agencies. Ghana is a useful comparison because it has adopted a national AI strategy and already has a data protection framework. Senegal and Benin also show that Francophone West Africa has data protection traditions that can be connected to AI governance, although enforcement capacity remains uneven. ECOWAS is central to this connection. The 2010 Supplementary Act on personal data protection was early by regional standards. Still, it was written before generative AI, platform campaigning, biometric identity expansion, and public-sector analytics became major governance issues. ECOWAS therefore needs AI-specific guidance on public procurement, high-risk systems, election misinformation, surveillance safeguards, regional complaint referral, and platform cooperation. Data protection is necessary, but it cannot manage algorithmic bias, synthetic media, surveillance procurement, and cross-border platform accountability on its own.

Table 2: Adapting Global AI Governance to West Africa

Global regulatory idea	West African adaptation
Risk-based classification	Prioritize the use of AI in identity systems, elections, policing, welfare, credit, Education, borders, and surveillance.
Transparency	Use public registers, procurement disclosure, plain-language notices, local-language communication, and civil society access.
Human oversight	Require review by named public officials and appeal routes that citizens can actually use, not only internal technical review.
Data protection	Consent, lawful basis, data minimisation, and correction rights should be clearly connected to public-sector AI and digital identity systems.
Cross-border enforcement	ECOWAS should be used to develop shared standards, support referrals between regulators, improve platform cooperation, and coordinate responses to election misinformation.

5. AI in Public Decision-making and Administration

Public decision-making is One of the main areas where West African governments may want to use AI. Many states have limited money, weak records, and strong demand for services. AI tools may seem useful because they promise faster verification, better targeting, fraud detection, higher revenue, and better planning. They can help find duplicate records, predict disease outbreaks, target agricultural support, detect tax problems, process complaints, translate public information, and manage large datasets. These benefits matter. A state that does not know its population well will find it harder to plan roads, schools, hospitals, welfare, and emergency response.

The democratic risk begins when administrative visibility becomes administrative exclusion. Nigeria's digital identity expansion shows the tension. National Identification Number enrollment had passed 100 million records by 2025. This made it One of the largest identity projects in Africa. The system can help with financial inclusion, SIM registration, welfare targeting, security, and service delivery. But large enrollment is not the same as universal or error-free coverage. People without stable documentation, displaced persons, elderly citizens, rural dwellers, informal workers, and those whose demographic information is incorrectly recorded may have difficulty correcting errors. If AI systems are later layered onto these identity records, the consequences of error can spread across multiple services.

Welfare targeting provides a realistic example of how a government may use an automated risk model to identify households eligible for cash transfers after floods, insecurity, or food-price shocks. The model may draw on identity records, bank verification, mobile money use, geolocation, household size, previous benefit records, and community data. Such a tool may reduce fraud and speed up payment. It may also exclude widows whose phone numbers are registered in a relative's name, displaced persons whose addresses are unstable, rural families with poor network histories, or households whose bank records do not reflect real deprivation. The harm would appear as a technical ranking problem, but its source would be social inequality and weak records.

Public-sector AI should be governed before deployment, not only after a problem occurs. Ministries and agencies should record the purpose of each high-risk system, the legal basis for using personal data, the data sources, the vendor's role, the testing process, the appeal route, and the likely consequences of error. This may look like ordinary bureaucracy, but it is the kind of bureaucracy that protects citizens. If a public institution cannot explain why, it needs a system, what data it uses, how the system was tested, and how errors will be corrected; it should not use that system for decisions that affect people's rights.

6. Misinformation, Surveillance, and Electoral Processes

Elections are among the clearest areas where AI and governance intersect. West African elections already take place within ethnic and religious mobilization, partisan distrust, monetized campaigning, security concerns, and heavy social media use. AI adds speed and scale to these pressures. AI can create false claims, imitate voices, make fake images, translate propaganda into local languages, and automate replies. It can also help campaign teams test which messages affect people emotionally. The result is a more unstable boundary between authentic speech, satire, manipulation, and deception.

Nigeria's 2023 elections provide important evidence. Fact-checking groups found false claims about candidates, endorsements, health, ethnic identity, election procedures, violence, and the transmission of results. CDD West Africa reported more than 200 fact checks and explainers from its election war room. The Nigeria Fact-Checkers' Coalition reviewed 127 election-related claims across the presidential, National Assembly, governorship, and state assembly elections. The EU Election Observation Mission also monitored online campaign activity and analysed thousands of posts by governorship candidates. These figures do not show the full scale of

misinformation. But they show that false and misleading content became a regular part of electoral competition.

Evidence from Nigeria's 2023 election can also be read alongside newer peer-reviewed African work on election disinformation. One South African study of the 2024 election analysed 22,384 WhatsApp messages from 47 politically active groups and 6,283 users. Its findings are useful for West Africa because they show that AI-linked disinformation does not spread only. After all, it appears technically convincing. It also spreads through fear, identity, partisan loyalty, and trust within closed groups. The lesson is careful but important. Deepfakes and synthetic media matter, but the social and political character of the channel still shapes whether falsehood spreads.

AI changes this environment in three ways. First, it reduces production cost. A small campaign unit can produce many versions of a message, image, or audio clip without the need for expensive studios. Second, it improves localization. False claims can be translated into local languages, adjusted to religious or ethnic languages, and shared through trusted group networks. Third, it makes verification harder. People may not know whether a video, voice note, or screenshot is real. Electoral bodies may also respond too slowly, after the claim has already spread. The damage to democracy comes from cumulative uncertainty. When citizens cannot tell what is real, distrust becomes politically useful.

Surveillance is the other side of the electoral problem. Governments may defend digital monitoring as a way to track hate speech, violence, terrorism, cybercrime, and foreign interference. These are real concerns even though surveillance tools can also be used against journalists, protesters, opposition actors, civic groups, and whistleblowers. Predictive systems can turn political dissent into a security issue. Facial recognition in public spaces can discourage public assembly. Social media monitoring can also shift from public safety to partisan intelligence. When oversight is weak, technology that claims to protect order can reduce civic freedom.

Electoral information integrity should protect the vote without criminalizing ordinary political disagreement. Electoral bodies should publish clear procedural information in local languages. They should also respond quickly to false claims and create rules for synthetic campaign media. At the same time, citizens must retain the right to criticize election management.

INEC's Creation of AI capacity is therefore both significant and delicate. Electoral AI can help with election logistics, voter Education, translation, misinformation monitoring, and operational analysis. But it should not be used as a black box to Judge political speech or to make decisions that affect voters' rights. Any use that affects voters should be explained publicly because the 2023 elections showed that technology does not automatically create trust. People judged the tools by the institution's broader credibility. Technology can support elections. But it cannot replace transparency, timely communication, and accountable administration.

7. Algorithmic Bias, Data Governance, and Civil Liberties

Algorithmic bias in West Africa should not be understood only as hostile design. Many biased outcomes arise from ordinary institutional choices. A dataset may reflect old patterns of exclusion. A model may use proxy variables that appear neutral but correlate with class, gender, region, ethnicity, disability, or language. A vendor may test a system on a population different from the One that will use it. A public agency may deploy a tool without a correction route. Discrimination can therefore occur without explicit discriminatory intent.

Digital credit provides a realistic local example. Fintech and lending platforms may use data such as transaction data, phone usage, repayment history, device type, location stability, contact networks, and platform activity. This can help lenders reach people without collateral or formal credit records. But it can also hurt people whose lives are informal, seasonal, cash-based, or shared through family networks. Women traders who borrow phones may be scored badly.

Rural users with weak internet access may also be affected. Young people with cheap devices and small businesses with irregular digital records may look risky even when they repay loans. The bias does not need to mention gender or poverty. It can enter through digital traces that serve as substitutes for social knowledge.

Biometric identity offers a second example. Biometric matching can reduce duplicate registrations and strengthen public records. But errors are not distributed equally. Manual labourers may have worn fingerprints. Older people may face capture difficulty. People in rural areas may be enrolled through lower-quality equipment. Names may be misspelled or reordered across identity systems. Women who change names after marriage may have mismatched records. Displaced persons may lack supporting documents. If AI-enabled verification is then connected to SIM registration, banking, welfare, pensions, or travel, a small data error can become a broad civil-liberties problem. The right affected is not only privacy. It is access to ordinary citizenship.

Policing and security analytics raise a third example. Insecurity in parts of Nigeria and the Sahel creates pressure for stronger intelligence systems. Data analytics may help identify crime patterns, allocate patrols, or connect case information. Yet historical security data can reflect patterns of over-policing, profiling, extortion, or underreporting. If a predictive tool is trained on such data, it may send more attention to already-policed communities while ignoring crimes that are less reported or less visible. Youth in poor urban neighbourhoods, border communities, migrants, motorcyclists, and politically active groups may become suspicious because the system sees previous police attention as evidence of risk. Bias here is institutional memory converted into mathematical probability.

Language and content moderation provide a fourth example. West Africa's digital public sphere is multilingual and often code-switching, as a single post may combine English with Pidgin, Hausa, Yoruba, Igbo, Twi, Ewe, Wolof, French, and Arabic, as well as emojis, coded insults, satire, and local political references. A moderation system that works fairly well in standard English or French may miss harmful rumours in local speech. It may also remove harmless cultural expressions because it does not understand the context. This creates a double harm. Dangerous misinformation may remain online, while legitimate speech from less-represented language communities may be suppressed. Platform governance is therefore also language governance.

Civil liberties are involved in all these examples. Privacy is the most obvious right, but equality, expression, association, due process, access to services, and political participation also matter. A citizen should not lose access to a service because a database contains an error. A journalist should also not be treated as a threat because a monitoring tool mistakes public scrutiny for subversion.

Data governance must therefore go beyond a privacy notice by including data minimisation, lawful basis, purpose limitation, retention rules, security safeguards, independent oversight, public-sector transparency, and citizens' right to correct errors. Recent African AI scholarship makes a similar point about trust and inclusion. Bias is not only a model error. It can also come from data, language, participation, and institutional design. In West Africa, the urgent need is for an enforceable routine. Institutions should document the data, test the model, disclose public use, allow independent review, and provide a remedy when the system is wrong.

8. Regulatory Gaps and Policy Responses

West Africa's regulatory problem is often described as the absence of AI law. That description is only partly accurate. The region already has relevant legal and policy instruments. Nigeria has the Data Protection Act and the Nigeria Data Protection Commission. It also has a national AI strategy and active digital-economy institutions. Ghana has a national AI strategy and a data protection framework. Senegal and Benin have data protection institutions shaped by Francophone legal traditions. ECOWAS has a regional data protection instrument. The African

Union has adopted a continental AI strategy. The problem is that these instruments remain weakly connected to the specific sites where AI produces public consequences.

One gap is public procurement. Many high-risk systems enter government through contracts rather than through AI policy. A Ministry may buy a biometric tool, analytics system, case-management platform, surveillance service, or data-integration product without public discussion of algorithmic risk. If the contract does not require audits, clear data rules, independent testing, documentation, deletion rules, breach notification, and limits on vendor reuse, later accountability becomes hard. Procurement is therefore important, but often hidden. A second gap is automated decision-making. Data protection laws may protect personal data, but they may not explain how algorithmic decisions should work in welfare, credit, Education, policing, migration, tax, or elections. Citizens need more than consent forms. They need to know when a system is involved. They also need to know what data is used, how to correct errors, who is responsible, and whether a human officer can reverse the decision, since without these rules, agencies may call decisions data-driven while avoiding responsibility for the harm they cause.

Surveillance oversight is a third gap in a context where security agencies face real threats such as terrorism, banditry, kidnapping, cybercrime, and violent conflict. But they can also be used to expand monitoring without enough control. Surveillance tools should not be used without legal approval, clear limits, time limits, independent review, proper records, and accountability after use. If these safeguards are weak, AI-enabled surveillance can become a tool for political monitoring and can reduce civic freedom.

A fourth gap is platform accountability. Major platforms are central to election communication and political advertising. They also shape influencer campaigns and the circulation of misinformation. Yet many enforcement systems remain weak for local languages, smaller markets, and fast-moving political claims. Nigeria's regulatory actions involving large platforms show that domestic authorities can challenge global companies, but platform accountability must not depend only on spectacular penalties after harm has occurred. Regulators need routine access to transparency reports, political ad libraries, content moderation language capacity, and election risk assessments. They also need fast channels for correcting false claims about voting procedures.

A fifth gap is regional coordination. No ECOWAS member state can adequately address cross-border misinformation, cloud data transfers, platform opacity, and vendor dependence on its own. ECOWAS can provide shared procurement clauses for high-risk AI systems. It can also set common standards for biometric systems, create regional channels for data protection complaints, and support cooperation among regulators, electoral bodies, and fact-checking networks during election periods. This would not remove national responsibility. It would only reduce vendors' and platforms' ability to take advantage of uneven rules across neighbouring states.

9. Implementation Challenges and Political Economy

The difficulty is not only in writing better rules. It is implementing them in political economies where regulators may be underfunded, public agencies may prefer rapid technological adoption, and political actors may benefit from opacity. A data protection authority may publish strong guidance while still needing engineers, investigators, lawyers, secure laboratories, complaint systems, and enforcement independence. An electoral body may promise digital transparency while still requiring operational credibility, clear communication, and the ability to correct misinformation quickly. A Ministry may require an impact assessment, but officials must understand the technology well enough to question vendors.

Vendor dependence is One of the most serious constraints. Many West African states rely on foreign suppliers for biometric registration, cloud infrastructure, analytics systems, cybersecurity products, surveillance tools, and digital public infrastructure. Dependence is not

automatically harmful. Foreign vendors may provide capacity that the state does not yet possess. The problem arises when contracts limit audit, obscure data flows, prevent local knowledge transfer, or lock government into proprietary systems. In such cases, technological modernization can weaken sovereignty because the public authority using the system cannot fully inspect or control it.

Political incentives also matter. AI tools are attractive because they allow governments to present an image of modernization. Announcing a new system can be easier than reforming the institution that will use it. Digital identity can be presented as an act of inclusion even when correction systems remain weak. Electoral technology can be presented as transparent even when communication is poor. Surveillance can be presented as security even when oversight is thin. Ghana's strategy-oriented approach, Nigeria's expanding digital identity system, Senegal's and Benin's data protection institutions, and ECOWAS regional instruments all show that formal policy activity is growing. However, implementation still depends on budgets, staff, courts, political will, and public trust.

Civil society and universities have an important role in this environment. They can monitor misinformation, test local-language systems, support affected citizens, examine procurement practices, and produce independent evidence of bias. The lack of original empirical research in many policy papers is itself a sign of the wider problem. Researchers often lack access to data, contracts, model documentation, and regulator files. A stronger next wave of research should include technical audits of biometric and scoring systems, interviews with affected citizens, content analysis of synthetic election material, and comparative studies of AI procurement across ECOWAS states.

Public trust is the final implementation issue. In low-trust settings, citizens may interpret AI systems through existing experiences of bureaucracy, policing, fraud, exclusion, and political manipulation. Trust cannot be built by describing a system as innovative. It is built when people can see the rules, correct errors, complain without fear, receive explanations, and face sanctions when powerful actors abuse data. Accountability is therefore not an obstacle to AI adoption. It is a condition for adoption that citizens will accept and institutions can defend.

10. Policy Recommendations

Immediate priority, within six to twelve months: First, Nigeria and ECOWAS should use a risk-based approach to AI governance. The approach should fit West African conditions. Low-risk tools used for drafting memos or routine administrative work should not be treated like high-risk systems. High-risk systems such as biometric identity systems, election technologies, predictive policing, welfare eligibility tools, credit scoring, border control, and public surveillance need stricter rules. Before such systems are used, there should be legal authority, a clear purpose, data protection compliance, bias testing, cybersecurity review, human oversight, public documentation, and complaint channels that citizens can use.

High-feasibility institutional priority, within twelve months: Second, public-sector AI procurement should be treated as a democratic accountability issue. Contracts should state the data sources, storage location, audit rights, model-testing requirements, subcontracting rules, cybersecurity standards, deletion rules, and limits on vendor reuse. Public agencies should not buy high-risk systems through vague technology contracts that make later inspection difficult. ECOWAS could develop model clauses to help smaller states negotiate with vendors and reduce uneven standards across the region.

Third, algorithmic impact assessment should be treated as a medium-term regulatory requirement. Data protection authorities, communications ministries, public procurement agencies, electoral bodies, and sector regulators should jointly develop assessment templates within One to two years. The assessments should identify who may be affected, likely errors, appeal options, data-quality issues, language limitations, and the practical implications of false

positives or false negatives. Monitoring should include published summaries of assessments, independent review of selected systems, and annual reporting on complaints and corrections. Fourth, electoral information integrity should be handled before elections, not only during election season. Electoral bodies, communications regulators, platforms, fact-checking organisations, political parties, and civil society groups should agree on protocols at least One year before major polls. The most urgent tasks are public communication in major local languages, rapid correction of false procedural claims, rules on AI-generated political content, and transparent platform cooperation. Evaluation should examine response time, reach of corrective information, number of synthetic-media incidents, and whether enforcement protects voters without suppressing lawful criticism.

Fifth, data protection authorities should issue AI-specific guidance and cooperate regionally. The guidance should cover automated decisions, biometric systems, children's data, public-sector data sharing, model training, cross-border transfers, and privacy by design. This is a medium-feasibility task because it requires technical expertise and regional coordination, but it can begin through guidance notes before full AI legislation is enacted. Regulators should also publish simple summaries of enforcement actions so citizens and institutions can understand what the rules mean in practice.

Sixth, West African governments should support independent research and civic monitoring through controlled access to non-sensitive public data, procurement information, and platform transparency materials. Universities, professional associations, election observers, digital rights groups, and fact-checking organisations should be treated as part of the accountability ecosystem. The framework points to four empirical priorities: audits of error rates in biometric and scoring systems, multilingual datasets on election misinformation, comparative studies of AI procurement contracts across ECOWAS states, and documentation of citizen experiences of correction, appeal, and exclusion.

11. Conclusion

Artificial intelligence is entering West African governance at a difficult time. The region needs better services, stronger planning, more credible elections, better security coordination, and wider economic opportunity. AI may help address some of these needs, especially where governments manage large populations, limited budgets, and scattered records. But it can also deepen exclusion, automate bias, expand surveillance, and spread misinformation when safeguards are weak.

The evidence reviewed in this paper shows that the problem is not that law or policy is completely absent. Nigeria, Ghana, Senegal, Benin, ECOWAS, and the African Union already have some parts of a governance system. The weakness is the limited connection between strategy, procurement, data protection, electoral integrity, surveillance oversight, citizen remedy, and regional enforcement. AI governance will fail if it stays confined to policy documents, innovation hubs, or general statements about ethics.

The democratic data integrity framework offers the paper's main theoretical contribution. It links democratic accountability, data ethics, and political economy through five audit questions about data, models, institutions, remedies, and civic space. These questions make clear that AI governance is not only a technical matter. It is a question of how public Power is organised, justified, contested, and corrected. In West Africa, that question must be answered under conditions of unequal data visibility, platform dependence, cross-border misinformation, security pressure, and uneven regulatory capacity.

This paper remains a critical synthesis rather than original empirical fieldwork. That limits its theoretical ceiling but does not remove its policy value. Its purpose is to clarify the governance problem and define the empirical path forward: procurement analysis, technical audits, and interviews with affected citizens, election misinformation datasets, platform language studies, and comparative regulatory studies across ECOWAS.

Future empirical research should test the framework through procurement analysis, technical audits, citizen interviews, election misinformation datasets, platform language studies, and comparative regulatory studies across ECOWAS. Such studies would show where democratic data integrity succeeds or fails in practice. Until that evidence grows, the safest policy position is clear: high-risk AI should be treated as a form of public Power that must be lawful, auditable, contestable, and open to remedy.

Acknowledgements

I would like to first express my profound appreciation to my colleague, Victor Abiolu, for painstakingly reading and editing the drafts of this work and for his availability to brainstorm and shape the intellectual direction of the paper. His thoughtful insights and constructive engagements greatly contributed to the refinement of this article.

I also sincerely thank my younger brother, Ahmed Adisa Aderemilekun, Mr. Habeeb Tajudeen, and Chief Solomon Adewole for their kind feedback and valuable observations after reviewing the final drafts of the manuscript. Their encouragement and comments are deeply appreciated. Furthermore, I acknowledge the scholars and stakeholders whose academic and policy debates shaped the development of this paper, particularly ongoing discussions on artificial intelligence, misinformation, electoral integrity, data governance, and democratic accountability in West Africa.

No external funding was received for the preparation of this article, and all views expressed herein remain solely those of the author.

References

- African Union. (2024). *Continental artificial intelligence strategy*. African Union Commission. <https://au.int/en/documents/20240809/continental-artificial-intelligence-strategy>.
- Bala-Gbogbo, E., & Dzirutwe, M. (2024, July 19). *Nigeria fines Meta \$220 million for violating consumer and data protection laws*. Reuters. <https://www.reuters.com/technology/nigerias-consumer-watchdog-fines-meta-220-million-violating-local-consumer-data-2024-07-19/>.
- Centre for Democracy and Development. (2023). *Information wins elections: Lessons from the Centre's 2023 election war room*. Centre for Democracy and Development West Africa.
- Centre for Democracy and Development. (2023). *Nigeria 2023 decides: Disinformation brief*—Centre for Democracy and Development West Africa.
- Data Protection Commission. (2023). *Annual report 2023*. Data Protection Commission.
- Eboh, C. (2024, August 22). *Nigerian data agency fines Fidelity Bank for breaches*. Reuters. <https://www.reuters.com/business/finance/nigerian-data-agency-fines-fidelity-bank-breaches-2024-08-22/>.
- Economic Community of West African States. (2010). *Supplementary Act A/SA.1/01/10 on personal data protection within ECOWAS*. ECOWAS Commission.
- Effoduh, J. O., Akpudo, U. E., & Kong, J. D. (2024). Toward a trustworthy and inclusive data governance policy for the use of artificial intelligence in Africa. *Data & Policy*, 6, Article e34. <https://doi.org/10.1017/dap.2024.26>.
- European Commission. (2025). *AI Act: Regulatory framework for artificial intelligence*. <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>.
- European Union Election Observation Mission. (2023). *Nigeria 2023: Final report—General elections of 25 February and 18 March 2023*. European External Action Service.
- Federal Competition and Consumer Protection Commission. (2025, April 25). *Tribunal upholds FCCPC's \$220 million fine against Meta/WhatsApp*.

- <https://fccpc.gov.ng/violations-tribunal-upholds-fccpcs-220-million-fine-against-meta-whatsapp/>.
- Freedom House. (2023). *Freedom on the net 2023: The repressive Power of artificial intelligence*. <https://freedomhouse.org/report/freedom-net/2023/repressive-power-artificial-intelligence>.
- Ghana Ministry of Communications and Digitalisation. (2023). *Ghana's national artificial intelligence strategy (2023–2033)*. Government of Ghana. https://moc.gov.gh/wp-content/uploads/2023/03/GHANA-AI-STRATEGY_BROCHURE.pdf.
- Gondwe, G. (2025). AI-driven disinformation and political influence on WhatsApp in South Africa's 2024 elections. *The International Journal of Press/Politics*. Advance online publication. <https://doi.org/10.1177/19401612251395434>.
- Independent National Electoral Commission. (2024). *Report of the 2023 general election*. Independent National Electoral Commission.
- Independent National Electoral Commission. (2025). *Creation of a division of artificial intelligence by the Commission*. Independent National Electoral Commission.
- Jonathan, S. (2023). *Typological analysis of fact-checking by the Nigeria Fact-Checkers' Coalition during the 2023 elections*. Dubawa. <https://dubawa.org/typological-analysis-of-fact-checking-by-the-nigeria-fact-checkers-coalition-during-the-2023-elections/>.
- National Centre for Artificial Intelligence and Robotics & National Information Technology Development Agency. (2025). *National artificial intelligence strategy*. Federal Ministry of Communications, Innovation and Digital Economy.
- National Identity Management Commission. (2025). *National identification number enrolment dashboard*. <https://nimc.gov.ng>.
- Nigeria Data Protection Act, 2023 (Act No. 33 of 2023).
- Nigeria Data Protection Commission. (2024). *Nigeria data protection annual report 2024*. Nigeria Data Protection Commission.
- Omilusi, M. (2025). Fake news, election-related disinformation laws, and citizens' rights in African political ecology. *Journal of African Elections*, 24(1), 1–25. <https://doi.org/10.20940/JAE/2025/v24i1a>.
- Pasipamire, N., & Muroyiwa, A. M. (2024). Navigating algorithmic bias in AI: Ensuring fairness and trust in Africa. *Frontiers in Research Metrics and Analytics*, 9, Article 1486600. <https://doi.org/10.3389/frma.2024.1486600>.
- World Bank. (2021). *Barriers to the inclusion of women and marginalized groups in Nigeria's ID system: Findings and solutions from an in-depth qualitative study*. World Bank.
- World Bank. (2021). *World development report 2021: Data for better lives*. World Bank. <https://www.worldbank.org/en/publication/wdr2021>.