Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Governed Interdependence as a Framework for Artificial Intelligence Sovereignty in Somalia

Nawiya Farhaan Ali

naawiyocadeyda@gmail.com

Imam Shafi'i University

Mohamed Abdi Ahmed

Imam Shafi'i University

Perspective

Keywords: artificial intelligence sovereignty, algorithmic dependence, governed interdependence, public sector, Somalia, AI procurement, digital governance

Posted Date: November 13th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11255714/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Abstract

Artificial intelligence (AI) sovereignty is often associated with domestically controlled infrastructure, data localisation and nationally developed models. Such measures may be valuable, but they cannot by themselves preserve public authority when consequential functions rely on AI systems that institutions cannot adequately inspect, constrain, challenge, evaluate or replace. This Perspective distinguishes ordinary technological interdependence from algorithmic dependence and proposes governed interdependence as a more practicable sovereignty objective for resource-constrained states. Drawing on scholarship on technological sovereignty and public-sector AI governance, together with documented policy developments in Somalia, we identify five tests of meaningful public control: legibility, enforceability, contestability, reversibility and independent evaluative capability. For Somalia, these tests suggest three priorities: a risk-tiered register of consequential public-sector AI systems, procurement safeguards that secure oversight and exit rights, and independent Somali-language evaluation connected to accessible human redress. These priorities are prospective policy proposals rather than findings from an empirical assessment of existing government AI deployments. The framework reframes AI sovereignty as the demonstrated capacity to govern dependence, providing a basis for comparative policy analysis and future empirical evaluation in low-resource settings.

1. Introduction

The growing use of artificial intelligence complicates established accounts of digital sovereignty. A government may store administrative data on national infrastructure yet depend on an external model to translate public information, classify records or inform an administrative decision. The institution may formally possess the data while remaining unable to inspect the model's behaviour, establish how an update altered its outputs, trace onward processing or provide an effective remedy to someone adversely affected. In such circumstances, the location of servers offers an incomplete measure of control. The central question is whether public institutions retain the authority and practical means to direct and account for functions delegated to AI systems (Roberts, 2024; von Scherenberg et al., 2024).

For states with limited fiscal, computing and specialist resources, technological self-sufficiency is unlikely to provide a credible near-term answer. Advanced computing capacity, cloud infrastructure and AI development remain unevenly distributed, and concentration among suppliers can constrain the options of smaller purchasers (Khan et al., 2024; Korinek & Vipra, 2025). Conversely, attempting to reproduce every layer of the AI value chain domestically can divert scarce resources from essential services and institutional capacity. The relevant policy choice is therefore not between isolation and unqualified reliance on foreign technology. It is between arrangements under which external capabilities remain governable and arrangements in which dependence progressively erodes the ability to oversee, correct or discontinue their use.

Somalia provides a timely setting in which to consider this distinction. The eGovernment Strategy 2025–2029 sets out national digital transformation ambitions. Somalia has enacted the Data Protection Act

No. 005/2023, with implementing regulations approved in January 2026. The National Communications Authority convened the second AI Summit Somalia in June 2026, and Somali National University announced the Somali National Artificial Intelligence Centre in July 2026 (Ministry of Communications and Technology [MoCT], 2025; Somalia Data Protection Authority [SDPA], 2026; National Communications Authority [NCA], 2026; Somali National University [SNU], 2026). These documented developments indicate growing policy and research interest. They do not, by themselves, show that high-stakes AI is extensively deployed in government or that comprehensive AI oversight is already operational.

This Perspective advances a specific proposition: AI sovereignty should be assessed through a public institution's capacity to govern consequential technological dependence, not through the geographic origin of its hardware, software or data alone. We first define algorithmic dependence and distinguish it from ordinary interdependence. We then set out five tests through which governed interdependence can be examined and consider three institutional commitments that could make those tests operational in Somalia. The argument is normative and forward-looking. It draws on existing research and publicly available policy documents rather than original interviews, a systematic review, a procurement audit or a comprehensive survey of deployed government systems.

2. Algorithmic dependence and the limits of technological ownership

Technology sovereignty has been described as the capacity to act purposefully within complex international innovation networks rather than as complete technological autarky (Edler et al., 2023). Normative work on digital sovereignty similarly distinguishes legitimate public authority from ownership or possession alone (Roberts, 2024). Data sovereignty foregrounds the governance of collection, access, processing and transfer, while scholarship on algorithmic sovereignty draws attention to the models, classifications and computational systems that shape how information is interpreted and used (Brown et al., 2024; von Scherenberg et al., 2024). These perspectives are complementary. However, an additional distinction is needed to identify the point at which reliance on an AI supplier becomes a consequential weakness in public governance.

A recent Somalia-focused analysis treats cloud and data sovereignty as a problem of public authority under structural dependence, recommending incremental governance measures rather than immediate technological self-sufficiency (Abdi et al., 2026). The present argument addresses a related but distinct question. Even if a public institution knows where its data are stored and can enforce a hosting contract, it may still be unable to evaluate a changing model, challenge its recommendations or provide effective redress for an AI-assisted decision. Algorithmic dependence therefore requires additional, decision-facing tests of public control.

We use algorithmic dependence to describe reliance on externally controlled AI models, platforms, computing services, data resources or technical standards for consequential public functions when the responsible institution lacks a feasible legal or practical means to understand, constrain, independently

evaluate, challenge or discontinue that reliance without disproportionate disruption. Three conditions must coincide. First, the system influences a function of public significance. Second, elements relevant to its operation or effects remain outside effective institutional control. Third, adequate mechanisms for oversight, remedy or substitution are absent. A supplier's foreign origin is neither necessary nor sufficient: domestically hosted AI may create equivalent dependence if it cannot be evaluated or challenged, while an externally provided system may remain governable under effective safeguards.

Dependence can arise through several interlocking channels. Infrastructural exposure concerns computing capacity, electricity, connectivity and related services. Contractual exposure concerns supplier terms covering data use, security, subcontracting, liability, model modification and termination. Epistemic exposure arises when models developed and evaluated elsewhere inadequately represent local languages, institutions or knowledge systems. Institutional exposure arises when public bodies lack the authority, expertise or procedures required to scrutinise a system or its supplier. These vulnerabilities can accumulate: low initial procurement costs may conceal expensive migration, opaque model changes or weak Somali-language performance, making the service increasingly difficult to replace (Korinek & Vipra, 2025; Langer & Haag, 2026).

Algorithmic dependence should not be treated as a synonym for every form of international collaboration or as automatic evidence of digital colonialism. Extractive uses of local data, labour or cultural knowledge merit particular scrutiny when consent, fair terms and participation are absent. Yet treating all cross-border provision as intrinsically harmful obscures meaningful differences between exploitative dependence and accountable cooperation. African AI governance scholarship emphasises institutions, public values, capability constraints and locally appropriate rules rather than universal prescriptions for technological separation (Effoduh et al., 2024; Plantinga et al., 2024). On this basis, we propose governed interdependence: continued participation in global AI ecosystems under arrangements that preserve effective public oversight, accountability, remedies and credible alternatives.

3. Governed interdependence as a practical test of sovereignty

Governed interdependence is not a claim that a state controls every component of an AI service. It is a testable condition of the relationship between a public institution and a system on which it relies. We propose five distinct but connected dimensions: legibility, enforceability, contestability, reversibility and independent evaluative capability. Their application should be proportionate to foreseeable harm. A low-risk writing assistant should not face the same scrutiny as an AI system that materially affects identity, healthcare, education, entitlements or public security.

The first test, legibility, requires an identifiable accountable institution and a usable record of the system's purpose, model or version, supplier chain, material data flows and contribution to administrative decisions. Some operational details may require justified confidentiality, but a public authority cannot govern a deployment it has not identified. The second test, enforceability, asks whether requirements for security, data handling, transparency, inspection, liability and service changes are

embedded in applicable administrative procedures and binding contracts. Statements of principle have limited force when the purchaser cannot obtain evidence of compliance or require corrective action.

The third test, contestability, concerns people affected by AI-assisted public decisions. Where a system has a consequential role, individuals should have appropriate notice, an understandable explanation of that role and access to a human reviewer empowered to reconsider or correct the outcome. An appeal process that merely repeats an automated recommendation is not meaningful review. The fourth test, reversibility, concerns the capacity to suspend an unsafe service, export records in usable formats, change providers and sustain essential operations during interruption. An exit clause is credible only when portability and fallback arrangements can be demonstrated. The fifth test, independent evaluative capability, requires technically competent assessment of relevant accuracy, bias, privacy, security and local-language performance rather than exclusive reliance on benchmarks or assurances supplied by the vendor itself (Muis et al., 2025; Langer & Haag, 2026).

Together, the five tests distinguish meaningful public authority from nominal ownership. An externally supplied system that satisfies them may be compatible with public sovereignty, whereas a locally branded system that fails them may present serious governance weaknesses. Single interventions are insufficient: domestic data storage does not guarantee an effective avenue of appeal, and access to open model weights does not establish auditing capacity or service continuity. Figure 1 maps the relationship between dependency exposures, proposed public-control instruments and governance tests. Table 1 identifies illustrative documentary and operational evidence with which each test could be examined. Neither constitutes a measured assessment of AI governance in Somalia.

Table 1
Proposed tests of governed interdependence and illustrative evidence

Test	Minimum governance question	Illustrative evidence
Legibility	Named accountable owner; system purpose; supplier and model record; mapped data flows.	Up-to-date AI register entry and technical file.
Enforceability	Auditable obligations on data use, security, subcontractors, model changes and liability.	Executed contract clauses, inspection rights and documented compliance review.
Contestability	Notice, accessible complaint channel and a human reviewer with authority to change outcomes.	Recorded appeal pathway, resolution decisions and anonymised remedy statistics.
Reversibility	Usable data export, transition assistance and continuity when a model or supplier fails.	Successful exit exercise and documented fallback arrangements.
Evaluative capability	Independent testing of relevant performance, risks and Somali-language suitability.	Local benchmarks, pre-deployment validation and periodic reassessment.

Note. The indicators are proposed for future institutional assessment and empirical testing. They do not report observed levels of AI sovereignty or government performance in Somalia.

4. Priorities for implementing governed interdependence in Somalia

Somalia need not begin with a frontier AI model or a large new regulatory agency. A more feasible initial objective is to establish a limited set of credible controls before externally supplied AI becomes embedded in consequential public functions. Existing digital transformation plans, data protection law and emerging research capacity could provide points of departure, but they should not be mistaken for proof that the required mandates, budgets or operational teams already exist. African policy research supports attention to institutional learning and adaptation rather than assuming that a new central regulator is always the first or best response (Plantinga et al., 2024; Diallo et al., 2025). We propose three mutually reinforcing commitments.

4.1 Establish a risk-tiered register of consequential AI systems

The first commitment is a public-sector AI register designed around the level of risk and supported, where legally possible, by an interim administrative requirement. Ministries and participating public administrations would disclose systems that materially inform decisions or process sensitive information, including AI embedded in purchased software. Each entry should record the use case, deployment stage, responsible official, supplier, significant risks and an accessible contact for complaints. A public version could withhold narrowly justified security-sensitive details while retaining

enough information for scrutiny. Registration should cover proposed as well as deployed systems and be updated when a model, supplier, purpose or risk profile materially changes.

The Ministry of Communications and Technology could coordinate common reporting standards, while the Somalia Data Protection Authority would address matters within its statutory remit and each deploying institution would retain operational responsibility. Any such arrangement would require confirmation of legal mandates, allocation of resources and consultation with Federal Member States and Benadir. Somalia's federal context suggests that interoperable registers and minimum shared reporting fields may be more feasible than presuming that every deployment can be directly administered by one central office. Somaliland should be approached as a distinct administrative and potential comparative setting, rather than being assumed to fall within an implementation chain that the Federal Government does not effectively control.

4.2 Embed oversight and exit rights in AI procurement

The second commitment is a practical AI annex to public procurement and contract management. Before acquiring a consequential service, purchasers should establish the actual model and cloud providers, the location and purposes of relevant processing, the role of subcontractors, and the rules governing retention or reuse of government inputs. Contracts should then make proportionate provision for material change notifications, testing, incident reporting, evidence access or audit, data export, secure deletion, transition support and continuity planning. Such provisions must be assessed in routine contract management rather than treated as formalities. Procurement is a particularly important source of leverage where public institutions lack the resources to develop their own systems but can specify conditions of purchase (de Almeida & dos Santos Júnior, 2025; Sloane & Wüllhorst, 2025).

The required level of assurance should reflect the function and its risks. An approved assistant used only to draft non-sensitive text may need basic use rules and records of information handling. In contrast, AI systems affecting identification, healthcare prioritisation, examinations, public benefits or security decisions require stronger pre-deployment evaluation, meaningful human oversight and tested continuity arrangements. Procurement should also begin with a more elementary question: does the service require AI at all? Automating inconsistent records or poorly specified administrative rules can reproduce errors more quickly rather than solve them. Budgeting must include recurrent evaluation, contract monitoring and the practical cost of exit, not simply licence fees.

4.3 Build independent Somali-language assurance and accessible redress

The third commitment is a modest, distributed assurance capability that combines independent technical evaluation with public accountability. Somali National University's newly announced AI centre could help convene researchers and build shared resources in collaboration with other universities, regulators, professional associations and independent specialists. A useful early output would be a Somali-language public-service benchmark addressing translation, speech, question answering, factual

reliability, safety and performance under constrained connectivity. Evaluation should attend to relevant dialects and use conditions, record dataset provenance and disclose conflicts of interest. A distributed consortium may reduce the burden on any one institution, but a system developer should not be its sole auditor. Strong results on global benchmarks cannot be assumed to establish suitability for Somali public services (Brown et al., 2024; Effoduh et al., 2024).

Technical evaluation alone is insufficient if affected people lack a practical remedy. When AI materially shapes a consequential public decision, the responsible institution should communicate that role in accessible Somali and make human reconsideration available through channels people can actually use. Telephone, assisted and in-person routes may be necessary alongside digital forms. Privacy concerns should be directed to an appropriate data-protection process, while decisions about a particular service should remain reviewable through the responsible sectoral body, subject to applicable law and any available independent mechanisms. These are proposed safeguards, not claims that every AI-specific right of appeal already exists in Somalia. Research on rights and algorithmic impact assessments supports integrating such protections during system design and procurement rather than waiting for harms to become visible (Muis et al., 2025).

A first phase could consist of a costed 12-month pilot across a small number of willing public institutions. The pilot should produce verifiable outputs: an initial register; model procurement provisions; named accountable officers; an independently designed Somali-language assessment protocol; and documented exercises of complaint handling and provider exit for any selected high-impact application. Further expansion should depend on evidence about legal authority, staffing, cost, implementation burden and service outcomes. Regional collaboration through the East African Community, which Somalia joined in March 2024, may help share training resources, contract templates and assessment methods, but regional cooperation cannot replace domestic accountability (East African Community, 2024; African Union, 2024).

5. Policy trade-offs and implementation risks

Three trade-offs warrant explicit consideration. First, sovereign capability should not be confused with domestic ownership. A national data centre or locally branded model may be justified for specific continuity, security or research purposes, but ownership creates little public value if the asset cannot be maintained, independently tested or financed over time. It can also substitute one form of dependence with reliance on a narrow group of suppliers or specialists. In Somalia, shared computing arrangements, smaller adaptable models and more than one viable provider may sometimes improve resilience more affordably than an attempt to reproduce frontier-model capacity (Khan et al., 2024; Langer & Haag, 2026).

Second, openness is not automatically safe, and restriction is not automatically sovereign. Somali-language datasets and models supported by public resources could advance local research and inclusion, but unrestricted disclosure of voice, health, identity or culturally sensitive materials can expose

individuals and communities to harms that are difficult to reverse. A public-interest stewardship model should distinguish genuinely open material from data requiring controlled access, establish provenance and permitted uses, and address attribution and equitable benefit sharing. These decisions should involve the people and communities contributing the material, not only technology suppliers and research institutions (Effoduh et al., 2024; Brown et al., 2024).

Third, proportionate oversight should neither obstruct beneficial low-risk experimentation nor become symbolic compliance. Elaborate approval pathways may impose excessive costs where risks are limited, whereas uncosted principles and checklists provide weak protection in consequential applications. A differentiated approach is therefore essential: documentation, independent assessment, explanation and external scrutiny should intensify with foreseeable harm. The African Union's Continental AI Strategy articulates an inclusive, locally responsive development agenda, but its aspirations require clear mandates, realistic institutional budgets and verifiable obligations if they are to influence actual public-sector practice (African Union, 2024; Plantinga et al., 2024).

6. Limitations, future research and conclusion

This article proposes a normative framework based on published scholarship and publicly documented Somali and regional policy developments. It is neither a systematic review nor an empirical assessment of government AI use, procurement contracts, and institutional capability or citizen outcomes. The fact that the documents considered here do not provide a comprehensive publicly accessible register should not be interpreted as proof that no government AI deployments or internal safeguards exist. Similarly, the institutional roles suggested in this Perspective remain proposals: their legal feasibility and operational practicality require confirmation before implementation. These limitations also define the framework's appropriate use as a guide for inquiry and policy design rather than an established measure of Somali AI governance performance.

The next task for research is to examine whether the proposed tests discriminate between better and worse governance arrangements. Empirical work could inventory consequential AI systems, assess real procurement clauses and provider portability, test Somali-language performance and differential error, evaluate human review procedures and compare federal and state-level institutional arrangements. Observable measures might include the completeness of registration records, the enforceability of supplier obligations, accessibility and outcomes of appeal pathways, results of tested provider transitions and the independence and coverage of performance assessments. Such work could refine the framework and establish which controls are feasible, effective and affordable in low-resource environments.

The central choice for Somalia is not whether to accept or reject foreign AI. It is whether global capabilities can be used without surrendering the practical authority to understand, regulate, contest and replace them. Where a public body cannot identify a model used in an essential service, examine its performance in Somali, enforce supplier obligations or correct a harmful AI-assisted decision, its

dependence becomes politically consequential regardless of where the servers are situated. Governed interdependence therefore shifts the meaning of AI sovereignty from an unattainable ideal of complete technological self-sufficiency to a demonstrable commitment to accountable public power.

Declarations

Competing interests

The authors declare that they have no financial or non-financial competing interests that could have influenced the preparation, interpretation, or presentation of this manuscript.

Ethical approval

Not applicable (NA). This article is a conceptual Perspective based on previously published scholarly literature and publicly available policy documents. The work did not involve human participants, animal subjects, or the collection of identifiable personal information. Therefore, institutional ethical approval was not required.

Consent to participate

Not applicable (NA). This manuscript does not report primary research involving human participants. No individuals were recruited, interviewed, surveyed, or otherwise enrolled in a research study. Consequently, informed consent to participate was not required.

Consent to publish

Not applicable (NA). This manuscript does not contain identifiable personal information, individual participant data, or images requiring consent for publication. All authors have reviewed and approved the final manuscript and consent to its submission for publication.

Funding

This work was funded by Imam Shafi'i University, Mogadishu, Somalia.

Author Contribution

N.F.A. conceptualized the Perspective, developed the conceptual framework, conducted the literature review, and drafted the original manuscript. M.A.A. contributed to the literature review, policy analysis, and critical revision of the manuscript. Both authors reviewed and approved the final manuscript and agreed to be accountable for its content.

Data availability statement

Not applicable (NA). This Perspective article presents a conceptual and policy-oriented analysis informed by existing scholarly literature and publicly available policy documents. No new empirical datasets were generated or analyzed during the preparation of this manuscript. All supporting published sources are acknowledged in the reference list.

References

1. Abdi AS, Abdulle AA, Hambali MM. Building public authority for cloud governance and data sovereignty in Somalia under structural dependence. Discover Global Soc. 2026;4., Article 118. https://doi.org/10.1007/s44282-026-00471-x.
2. African Union. (2024). Continental artificial intelligence strategy. https://au.int/en/documents/20240809/continental-artificial-intelligence-strategy
3. Brown PT, Wilson D, West K, Escott K-R, Basabas K, Ritchie B, Lucas D, Taia I, Kusabs N, Keegan TT. Māori algorithmic sovereignty: Idea, principles, and use. Data Sci J. 2024;23., Article 15. https://doi.org/10.5334/dsj-2024-015.
4. de Almeida PGR, dos Júnior S, C. D. Artificial intelligence governance: Understanding how public organizations implement it. Government Inform Q. 2025;42(1). https://doi.org/10.1016/j.giq.2024.102003. Article 102003.
5. Diallo K, Smith J, Okolo CT, Nyamwaya D, Kgomo J, Ngamita R. Case studies of AI policy development in Africa. Data Policy. 2025;7:e15. https://doi.org/10.1017/dap.2024.71.
6. East African Community. (2024, March 4). Somalia finally joins EAC as the bloc's 8th partner state. https://www.eac.int/eac-press-releases/3049-somalia-finally-joins-eac-as-the-bloc-s-8th-partner-state
7. Edler J, Blind K, Kroll H, Schubert T. Technology sovereignty as an emerging frame for innovation policy: Defining rationales, ends and means. Res Policy. 2023;52(6). https://doi.org/10.1016/j.respol.2023.104765. Article 104765.
8. Effoduh JO, Akpudo UE, Kong JD. Data Policy. 2024;6:e34. https://doi.org/10.1017/dap.2024.26. Toward a trustworthy and inclusive data governance policy for the use of artificial intelligence in Africa.
9. Khan MS, Umer H, Faruqe F. Artificial intelligence for low income countries. Humanit Social Sci Commun. 2024;11., Article 1422. https://doi.org/10.1057/s41599-024-03947-w.
10. Korinek A, Vipra J. Concentrating intelligence: Scaling and market structure in artificial intelligence. Economic Policy. 2025;40(121):225–56. https://doi.org/10.1093/epolic/eiae057.
11. Langer PF, Haag S. AI sovereignty: Redundant use of large language models for public sector resilience. Public Organ Rev Adv online publication. 2026. https://doi.org/10.1007/s11115-026-01021-4.

12. Ministry of Communications and Technology. (2025). eGovernment strategy 2025–2029. https://moct.gov.so/en/wp-content/uploads/2025/08/eGovernment-Strategy-2025-2029.pdf
13. Muis IM, Straatman J, Kamphorst BA. Responsible AI innovation in the public sector: Lessons from and recommendations for facilitating fundamental rights and algorithms impact assessments. J Responsible Technol. 2025;22:100118. https://doi.org/10.1016/j.jrt.2025.100118.
14. National Communications Authority. (2026, June 14). National Communications Authority holds the second AI Summit Somalia 2026. https://nca.gov.so/news/national-communications-authority-holds-the-second-ai-summit-somalia-2026
15. Plantinga P, Shilongo K, Mudongo O, Umubyeyi A, Gastrow M, Razzano G. Responsible artificial intelligence in Africa: Towards policy learning. Data Policy. 2024;6:e72. https://doi.org/10.1017/dap.2024.60.
16. Roberts H. Digital sovereignty and artificial intelligence: A normative approach. Ethics Inf Technol. 2024;26. https://doi.org/10.1007/s10676-024-09810-5. Article 70.
17. Sloane M, Wüllhorst E. A systematic review of regulatory strategies and transparency mandates in AI regulation in Europe, the United States, and Canada. Data Policy. 2025;7:e11. https://doi.org/10.1017/dap.2024.54.
18. Somalia Data Protection Authority. (2026, January 5). Council of Ministers approves Data Protection Act regulations. https://dpa.gov.so/news/council-of-ministries-approves-data-protection-act-regulations/
19. Somali National University. (2026, July 15). Jaamacadda Ummadda oo daahfurtay Xarunta Garaadka Gacmeedka (Somali National Artificial Intelligence Center). https://snu.edu.so/jaamacadda-ummadda-oo-daahfurtay-xarunta-garaadka-gacmeedka-somali-national-artificial-intelligence-center/
20. von Scherenberg F, Hellmeier M, Otto B. Data sovereignty in information systems. Electron Markets. 2024;34., Article 15. https://doi.org/10.1007/s12525-024-00693-4.

Figures



Governed interdependence means externally supplied AI remains subject to demonstrable public control.

Figure 1

From algorithmic dependence exposures to governed interdependence. The conceptual model links infrastructural, contractual, epistemic and institutional exposures to proposed public-control instruments and five tests of public authority. The arrows represent a proposed governance relationship, not an empirically estimated causal effect. Source: authors' conceptualisation.