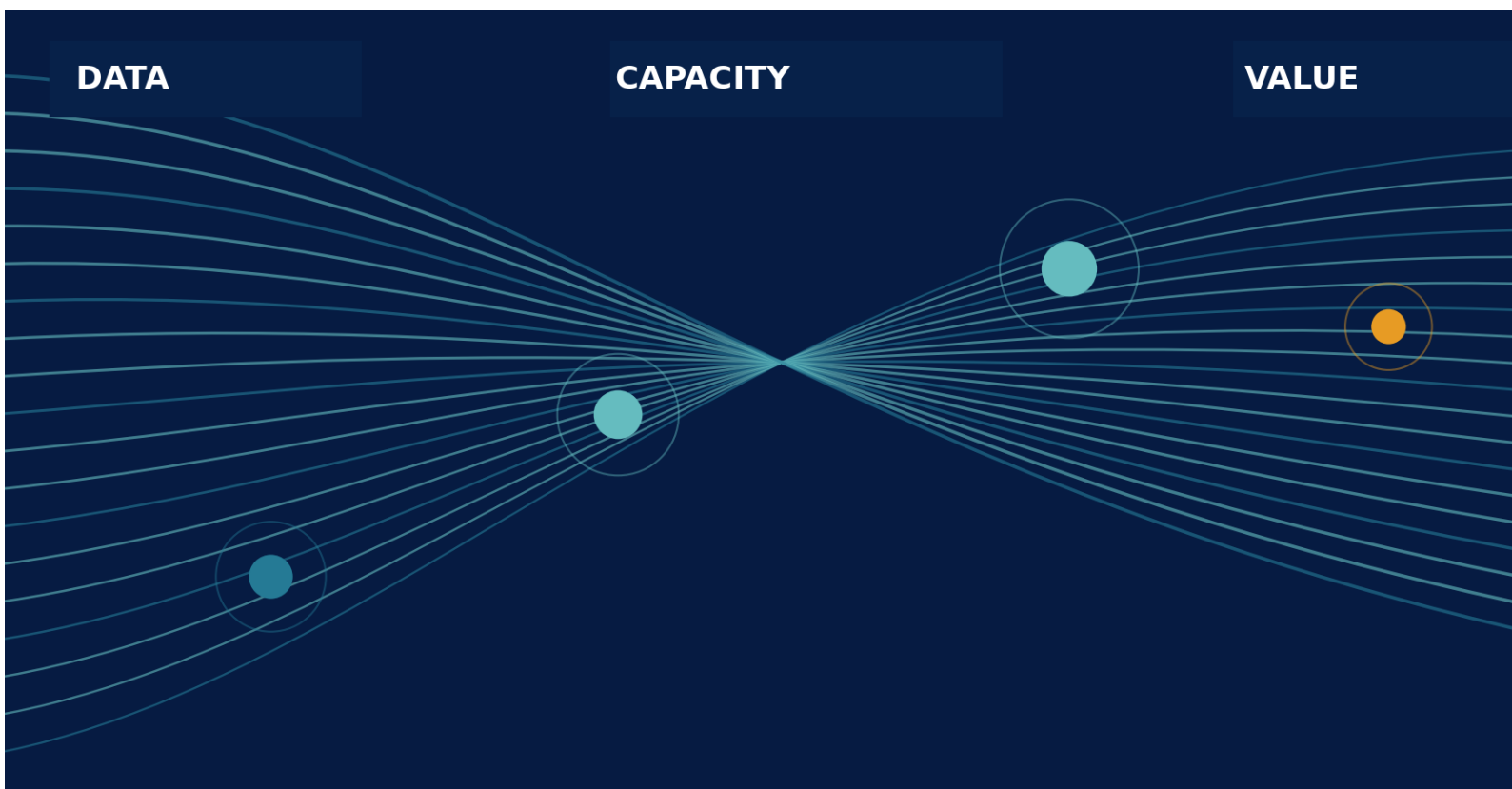


INSIGHT PAPER | JUNE 2026

Digital sovereignty in Angola

Priorities for national capacity and inclusive digital transformation

Angola can strengthen control over its digital assets and turn that control into better services, talent, and economic activity. The path forward combines protection proportional to risk, international cooperation, and local implementation capacity.

DATA**CAPACITY****VALUE**

CONTENTS

Global context	4	
Angolan context	6	
Data and infrastructure	7	
Resilience and procurement	9	
Talent and AI	10	
Public services and inclusion	12	
Digital economy	14	
Implementation and indicators	16	
Priority decisions	28	
A ROADMAP FOR ANGOLA	19	
References	22	

Digital sovereignty means ensuring that Angola has the capacity to decide, protect, operate, regulate, and create value in the digital world.

The country's digital sovereignty should be open, pragmatic, and intelligent: protect what is critical, cooperate where scale matters, develop national capacity where it creates value, and ensure that no one is left out of the digital society.

This insight is intended for public-sector decision-makers, business leaders, and development partners. It contributes to the discussion of the central issues in the digital transformation of the information society and presents an implementation agenda for Angola.

LBC CEO, Carlos Valleré Oliveira, was a guest speaker at ANGOTIC 2026, held in Luanda from June 11 to 13, on the panel “Soberania Digital e Transformação Digital da Sociedade da Informação” (Digital Sovereignty and Digital Transformation of the Information Society). This article, along with another on the digital transformation of the information society in Angola, formed the basis of his contribution. Both are contributions to the discussion.

EXECUTIVE SUMMARY

Digital sovereignty requires decision-making and implementation capacity

Angola should treat digital sovereignty as a development agenda. The objective is to ensure national capacity to make decisions about data, protect essential services, manage suppliers, and create value through technology. This capacity makes it possible to benefit from global solutions with greater security and freedom of choice.

The physical location of a data center does not, by itself, ensure control. Access rights, encryption key management, operating capacity, auditability, and the feasibility of switching suppliers also matter. Digital policy should assess these conditions together.

EXHIBIT 1 Three dimensions to guide decisions**01****CONTROL**

Strategic data
Critical systems
Rules and contracts

02**CAPACITY**

National talent
Operations and auditing
Contextualized AI

03**VALUE**

Inclusive services
Companies and jobs
African cooperation

Analysis model proposed by LBC.

The first priority is to identify strategic digital assets and define requirements proportional to their criticality. The second is to build teams and institutions capable of applying those requirements, operating the systems, and developing solutions suited to the Angolan context. The third is to ensure that investments produce benefits accessible to the population and opportunities for Angolan companies.

Digital transformation should be assessed by usage, service quality, and the capacity to sustain it. Inclusion and resilience need to accompany investment from the outset.

The measure of digital sovereignty is the capacity to choose, operate, and evolve the systems on which the country depends.

01 GLOBAL CONTEXT

The most pressing issues in digital sovereignty

1. Data: who collects it, where it is stored, who accesses it, and who captures value.

Data is now an economic and political infrastructure. The question is no longer simply how to “protect personal data”, but whether the country has the rules, institutions, and technical capacity to manage public, business, personal, strategic, and sectoral data. The African Union places data governance at the center of Africa’s digital economy, advocating harmonized frameworks, shared data spaces, and common standards to increase trust, innovation, and intra-African digital trade.

2. Cloud, data centers, and technology dependence.

Digital sovereignty depends on determining which data and systems should be hosted in the global public cloud, Government cloud, national data centers, or regional African infrastructure. The answer should be neither “everything local” nor “everything abroad”; it should be based on criticality. Security, identity, public finance, health, critical infrastructure, and justice data require enhanced control. Less critical data can benefit from global scale, provided there are appropriate contracts, encryption, reversibility, and auditing.

3. Cybersecurity as national security.

Digital sovereignty fails when critical infrastructure can be paralyzed by attacks, ransomware, sabotage, espionage, or external operational dependence. Angola already recognizes this scenario in its recent framework: Presidential Decree No. 258/25 creates the National Cybersecurity Council and frames cybersecurity as essential to protecting data, networks, information systems, and critical infrastructure, including health, energy, and telecommunications.

4. Artificial intelligence, algorithms, and cognitive sovereignty.

Artificial intelligence (AI) adds a new layer of sovereignty: which models we use, what data they were trained on, which languages and cultures they represent, which decisions they automate, and which biases they reproduce. For Africa, the question is: will we be merely consumers of global models, or producers of solutions adapted to our realities, languages, public services, and economies?

5. Digital identity, payments, and public-sector interoperability.

Whoever controls identity, authentication, digital signature, payment, and secure data exchange systems controls the backbone of the digital society. The World Bank highlights digital public infrastructure – digital identity, payments, and secure data sharing – as the foundation for digital public services, inclusion, and innovation.

6. Supplier dependence and public procurement.

Digital sovereignty also means avoiding excessive dependence on a single supplier, technology, or country. This requires interoperability, open standards, data portability, exit clauses, knowledge transfer, and the development of local capacity.

7. Talent and productive capacity.

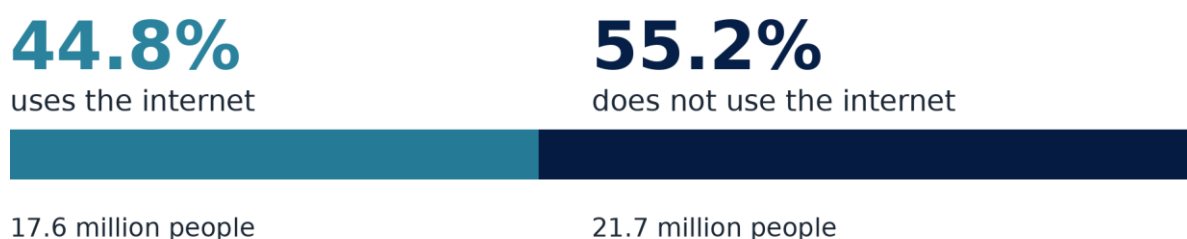
A country is not digitally sovereign simply because it buys technology. It is sovereign when it has engineers, digital legal experts, data managers, cybersecurity specialists, cloud architects, capable regulators, start-ups, and Angolan companies able to create, maintain, and audit solutions.

02 ANGOLAN CONTEXT

Inclusion defines the scale of Angola's challenge

Effective internet access should guide digital transformation choices. Estimates in the "Digital 2026: Angola" report, referring to October 2025, indicate that more than half of the population still does not use the internet. The existence of mobile connections does not eliminate this gap: a connection may be used only for voice or messaging, and one person may have multiple connections. [1]

EXHIBIT 2 Most of the population still did not use the internet in 2025



30.6 million mobile connections

Mobile connections do not correspond to unique internet users.

Source: DataReportal, "Digital 2026: Angola", October 2025 data. Percentages of the total population; figures rounded.

The response should combine coverage, affordable devices, data costs, energy, digital skills, and useful services. For citizens, these conditions work together. An available network does not solve a lack of equipment; equipment does not solve the difficulty of understanding or completing a service.

A strategic foundation is already in place

The "Livro Branco das Tecnologias de Informação e Comunicação 2023-2027" (White Paper on Information and Communication Technologies 2023-2027) frames digital transformation within Angola's development instruments, including the Plano de Desenvolvimento Nacional 2023-2027 (National Development Plan 2023-2027) and Angola 2050. It organizes action around six pillars: broadband, connectivity, and digital

inclusion; capacity building; technological modernization of Public Administration; technological innovation; regulation; and cybersecurity. [2]

Sovereignty should bring coherence to the implementation of this agenda. Each investment needs to specify the service it improves, the dependence it reduces, the capacity it develops, and the resources required to operate over time.

African scale strengthens national capacity

The Digital Transformation Strategy for Africa (2020–2030) advocates an inclusive digital economy and the development of a digital single market. Harmonized rules and interoperability can expand the scale available to African companies and institutions. For Angola, cooperation on data, payments, cybersecurity, and skills can increase bargaining power and access to markets. [3, 4]

03 DATA AND INFRASTRUCTURE

Data control should reflect its criticality

The first decision is to identify the digital assets on which the State and the economy depend. The inventory should cover civil identity, public finance, health, justice, security, energy, telecommunications, banking, transportation, natural resources, and geospatial information. For each asset, it is important to identify the owner, authorized users, dependencies, and the consequences of loss, alteration, or unavailability.

A data policy should translate this inventory into rules for collection, use, retention, sharing, and transfer. The African Union Data Policy Framework provides a reference for harmonizing governance, building trust, and developing data spaces that support innovation and digital trade. [4]

EXHIBIT 3 Criteria for deciding where data is hosted and how it is controlled

Asset type	Option to assess	Control conditions
Strategic or critical	National or government infrastructure, or a solution with enhanced control	Authority over access and keys; tested continuity; auditing; operating capacity
Sensitive or regulated	National, regional, or hybrid architecture, according to risk and the applicable framework	Restricted access; encryption; operation logs; transfer and retention rules
Non-sensitive or public	Infrastructure offering the best combination of scale, cost, and service	Integrity; availability; open formats; data portability and recovery

Decision matrix proposed by LBC. Options depend on the specific classification of the asset and the applicable regulatory framework; they do not constitute a general data localization rule.

Deciding beyond physical location

The global public cloud can provide scale and access to technology. National or regional infrastructure can address specific control and continuity needs. Selection should consider risk, jurisdiction, technical capacity, total cost, and effective operations. Keeping everything local without maintenance capacity can also create vulnerabilities.

Key management, privileged access, backups, and audit mechanisms should be designed before procurement. The same applies to reversibility: it is necessary to know how to recover data, configurations, and documentation, how much migration will cost, and who can carry it out.

Infrastructure choices should result from an assessment of risk and operational capacity, with reviews whenever systems, services, or supply conditions change.

04 RESILIENCE AND PROCUREMENT

Protecting critical systems requires testing continuity

An outage in a health system, energy, telecommunications, finance, ports, airports, or tax administration can affect essential services and economic confidence. Digital sovereignty requires the capacity to prevent incidents, detect anomalies, respond, and restore operations. Protection should include information systems and, where applicable, operational technology.

Presidential Decree No. 258/25 of December 3 created the National Cybersecurity Council and approved its rules of procedure. This framework strengthens the institutional dimension of cybersecurity. Implementation requires clear responsibilities among national coordination bodies, sector entities, and service operators. [5]

From compliance to response capacity

Organizations responsible for critical assets should understand dependencies between systems, define recovery times, and test failure scenarios. Backups provide effective protection only when they can be restored. A continuity plan is credible only when those responsible know who makes decisions, who communicates, and how service is maintained during an interruption.

Joint exercises make it possible to assess failures that cross multiple entities. They also help distinguish technical unavailability, data loss, and compromised credentials – situations that require different responses. Test findings should lead to corrective actions with assigned owners and deadlines.

Public procurement should preserve options

Excessive dependence on a supplier, technology, or country reduces freedom of choice. Contracts should provide for open standards, documented interfaces, portability, service levels, audit rights, and exit conditions. Economic evaluation should include operations, updates, training, and transition to another provider.

Contractual reversibility has value only when the technical capacity to execute it exists.

Knowledge transfer should produce verifiable evidence: teams trained on real tasks, up-to-date documentation, access to relevant configurations, and exercises in independent operation. Where appropriate, there should be provisions for code audits. These requirements make international partnerships more sustainable and strengthen accountability for service delivery.

Supplier diversity should be proportional to risk. Multiplying solutions without a common architecture increases complexity. The objective is to maintain viable alternatives and internal expertise to assess, integrate, and manage them.

05 TALENT AND ARTIFICIAL INTELLIGENCE

National capacity should grow with every project

Technology acquisition should be accompanied by the capacity to use, maintain, and improve it. Angola needs professionals in data, software development, cloud architecture, cybersecurity, product management, and digital regulation. It also needs public-sector leaders capable of linking technology decisions to service outcomes.

Training gains value when it is connected to the work. Mixed teams, supervised maintenance, architecture reviews, and joint incident resolution enable knowledge transfer that a stand-alone course can rarely provide. Universities, training centers, companies, and public institutions can organize pathways tied to concrete operational needs.

Applying AI to well-defined problems

AI adds a dimension of sovereignty related to data, languages, and the decisions influenced by models. Angola can use global models while developing local capacity to adapt, integrate, and evaluate them. This includes testing the Portuguese used in the country, national languages, and the suitability of responses to institutional and cultural contexts.

Domain	Possible initial application	Condition for moving forward
Public administration	Support for service delivery, search, and document analysis	Verified sources; data protection; human review and exception handling
Education and health	Support for teachers and professionals; content and information	Expert validation; clear limits; error assessment and accessibility
Agriculture, small and medium-sized enterprises (SMEs)	Technical information, management support, and access to services	Local adaptation; accessible channels; user testing
Customs and inspection	Document screening and anomaly detection	Traceability; bias testing; human decision-making and accountability

Examples of applications proposed for analysis. Suitability depends on available data, risk, and supervisory capacity.

Initial investment should prioritize use cases with demonstrable utility and measurable quality. Before scaling a solution, it is important to verify accuracy, cost per task, time saved, incidents, and effects on access to the service. Decisions that affect rights or benefits require enhanced oversight and mechanisms for appeal.

Building domestic AI capacity does not require starting by developing large foundation models. It can begin with data quality, independent evaluations, and sector-specific applications that national teams can operate and evolve.

06 PUBLIC SERVICES AND INCLUSION

Common infrastructure can simplify interactions with the State

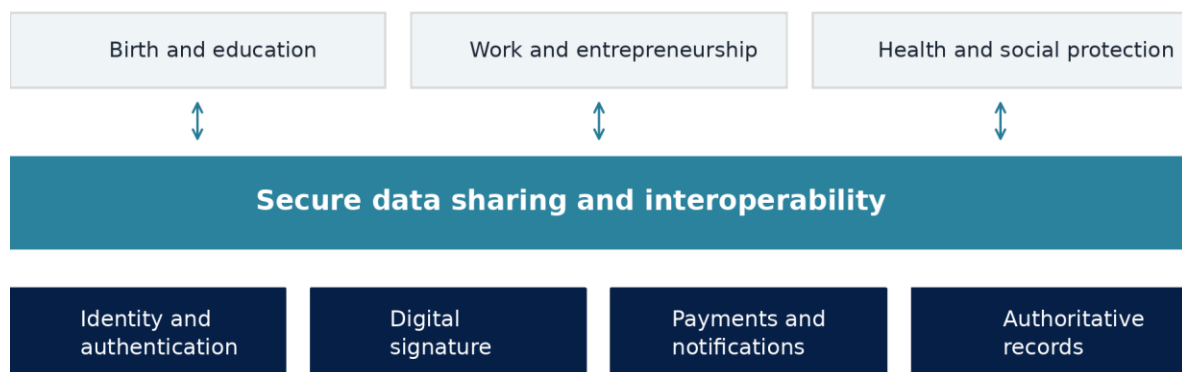
Digitizing Public Administration requires redesigning services around concrete needs: registering a birth, studying, starting a business, paying taxes, receiving benefits, or accessing health care. Publishing forms without reviewing processes preserves many of the difficulties citizens already face.

Common digital public infrastructure makes it possible to reuse identity, authentication, signatures, payments, and data sharing. The World Bank identifies digital public infrastructure as a foundation for improving service delivery across sectors. [6]

For Angola, the architecture should define common components, responsibilities for authoritative records, and secure access conditions.

EXHIBIT 4 Shared components for integrated public services

SERVICES ORGANIZED AROUND PEOPLE'S LIVES



Cross-cutting foundation Security • Data protection • Accessibility • Oversight

Conceptual architecture proposed by LBC, informed by the World Bank's digital public infrastructure approach. [6]

The once-only principle for providing information should guide simplification. Its application requires reliable records, an appropriate legal basis, and access controls. Consent should be used when it is the applicable legal basis; it does not replace other requirements for legitimacy, security, and transparency.

Design for those who face the greatest barriers

Services should work on affordable devices, with low data consumption and understandable instructions. Support channels and assisted service are necessary for people with lower digital literacy, limited access, or disabilities. Geographic expansion should consider schools, public employees, SMEs, farmers, and young people, including outside Luanda.

Trust depends on predictable service: knowing what data is requested, why, who uses it, and how to correct an error. Evaluation should track request completion, resolution time, and satisfaction, with analysis of differences across regions and user groups.

07 DIGITAL ECONOMY

Public demand can develop national productive capacity

Digital sovereignty has an economic dimension. Public projects and major business investments can create demand for Angolan suppliers of software, data, cybersecurity, training, and operational services. For this to happen, contracts need to turn local participation into lasting skills and delivery capacity.

Creating opportunities while maintaining quality requirements

Procurement can facilitate the participation of Angolan companies through proportional requirements, open interfaces, consortia, and clear knowledge-transfer conditions. Selection should continue to require quality, security, and economic sustainability. Local participation adds value when companies can maintain solutions, assume technical responsibilities, and win new clients.

The business agenda should cover e-commerce, payments, digital financial services, technology for agriculture, education, and health, as well as the digitization of SMEs. Exportable digital services can contribute to economic diversification where skills, quality, and market access are available.

Building a regional position on concrete foundations

Angola can aspire to become a regional digital platform. This possibility should be assessed based on connectivity, energy availability and cost, infrastructure quality, regulatory predictability, talent, and demand. The ambition should translate into a competitive proposition for companies and users.

African cooperation can expand the market and reduce fragmentation. Compatible rules for data, interoperability, and cross-border payments facilitate the development of regional services. Angola's participation in the African digital agenda should seek concrete operational and commercial benefits while preserving control over strategic assets. [3, 4]

Integrating sustainability into investment

Digital growth increases the use of energy, water, equipment, and materials. UNCTAD (United Nations Trade and Development) highlights the environmental footprint across the digitalization life cycle and the unequal distribution of its costs. [7] Data centers, networks, and devices should be assessed in terms of efficiency, maintenance, durability, reuse, and e-waste management.

Local productive capacity should be assessed by the knowledge and operational capability that remain in the country.

08 IMPLEMENTATION AND INDICATORS

Sequencing priorities makes the agenda executable

An indicative 18-month sequence is proposed from the start of a program, centered on critical assets and high-public-value services. The proposal should be adjusted to available resources and institutional decisions; it does not represent a government commitment.

EXHIBIT 5 Indicative sequence for building capacity and demonstrating results



LBC proposal. Time horizons refer to months after the start of the program; workstreams may overlap.

Preparation should define assets, dependencies, and owners. Pilots should test user experience, control, continuity, and local operations. Expansion should depend on demonstrated results, with an assessment of costs and support capacity.

Coordination should integrate services, data, technology, cybersecurity, procurement, and capacity building. Each initiative needs an owner accountable for results, an operating budget, acceptance criteria, and monitoring of risks and cross-entity decisions.

EXHIBIT 6 Indicators for measuring capacity and public value

Dimension	Suggested indicator	Evidence to collect
Control and resilience	Critical assets classified; recovery within the defined time	Validated inventory and test results
Operational autonomy	Systems operable by local teams; supplier exits tested	Operational and portability exercises
Service and inclusion	Requests completed; resolution time; usage by region	Service records and user research
Talent and economy	Skills applied; contracts with demonstrated knowledge transfer	Practical assessment and accepted deliverables
Sustainability	Energy consumption and equipment disposition	Operational measurement and records of reuse or recycling

Proposed indicators. Establish a baseline and targets for each service before assessing performance; avoid using expenditure or the number of platforms as measures of success.

09 PRIORITY DECISIONS

Ten decisions to guide Angola's digital sovereignty

The digital sovereignty agenda should translate into verifiable decisions. The following priorities combine protection, national capacity, and value creation while remaining open to international partners and markets.

01 Identify strategic assets. Inventory essential data and systems, assign owners, and classify criticality, sensitivity, and dependencies.

02 Define the data policy. Clarify conditions for access, hosting, use, retention, sharing, and transfer, with control proportional to risk.

03 Strengthen national cybersecurity. Connect institutional coordination to prevention, detection, response, and recovery, with exercises in critical sectors.

04 Reduce excessive dependencies. Require interoperability, portability, documentation, audit rights, and executable exit conditions.

05 Develop national talent. Link training to real projects and verify teams' capacity to manage, maintain, audit, and improve systems.

06 Build AI capacity. Select useful applications, improve data quality, and evaluate models in the Angolan context, with oversight proportional to impact.

07 Consolidate digital public infrastructure. Reuse identity, authentication, signatures, payments, and secure data sharing to simplify services.

08 Turn demand into economic activity. Create opportunities for national companies, exportable services, and skilled employment, while maintaining quality requirements.

09 Remain open under clear rules. Mobilize international investment and technology while protecting strategic assets and ensuring knowledge transfer.

10 Participate in the African digital agenda. Promote cooperation on data, cloud, cybersecurity, AI, and payments, seeking regional scale and interoperability.

10 A ROADMAP FOR ANGOLA

Proposed roadmap for Angola

1st: Clearly define which digital assets are strategic.

Not all data and systems have the same level of sensitivity. Angola should identify the critical data of the State and the economy: civil identity, tax data, health, security, justice, energy, telecommunications, banking, critical infrastructure, natural resources, and geospatial data. Digital sovereignty begins with knowing what is strategic and what requires enhanced protection.

2nd: Define a clear policy for national data.

The country should decide which data may be hosted in international clouds, which data should be hosted on national or regional infrastructure, and what rules should apply to access, storage, processing, and international data transfers. The central question is not only “where is the data?” but also: who has access, with what authorization, with what security, and for what purpose?

3rd: Strengthen national cybersecurity capacity.

Digital sovereignty depends on the capacity to prevent, detect, respond to, and recover from cyberattacks. This is especially important for sectors such as energy, telecommunications, banking, public administration, health, transportation, ports, airports, and oil and gas. Cybersecurity should be treated as a matter of national security, continuity of the State, and economic confidence.

4th: Avoid excessive technology dependencies.

Dependence on a single supplier, platform, technology, or country can create strategic vulnerabilities. Angola should promote interoperability, open standards, data portability, exit clauses in public contracts, and internal capacity to manage solutions. Digital sovereignty does not mean rejecting international partners; it means negotiating better, exercising better control, and preserving freedom of choice.

5th: Develop national digital talent.

There is no digital sovereignty without qualified people. The country needs to train software developers, data specialists, cloud architects, cybersecurity professionals, digital product managers, digital legal experts, technology regulators, and public-sector leaders capable of understanding technology. Buying technology is relatively easy; building national capacity to manage, audit, and evolve it is the real challenge.

6th: Build domestic AI capacity.

AI adds a new dimension to sovereignty: models can influence decisions, language, culture, public policy, credit, recruitment, education, and access to services. Angola should use global AI where it makes sense, while also developing solutions adapted to the Angolan context, the Portuguese language, national languages, public services, and priority sectors of the economy. Otherwise, it risks becoming merely a consumer of algorithms designed outside its reality.

7th: Build robust digital public infrastructure.

Digital identity, digital signatures, digital payments, secure authentication, interoperability among public databases, and secure information exchange are fundamental components of digital sovereignty. Without this infrastructure, digital transformation remains fragmented, costly, and unreliable. With it, Angola can accelerate public services, financial inclusion, economic formalization, and State efficiency.

8th: Turn digital sovereignty into economic opportunity.

Digital sovereignty should not be viewed only as defense or protection. It should also be an opportunity to develop national technology companies, start-ups, data centers, exportable digital services, and govtech, fintech, agritech, edtech, and healthtech solutions. Angola can use public demand and major digital projects as a lever to build a national digital industry.

9th: Balance sovereignty with international openness.

It would be a mistake to confuse digital sovereignty with isolation. Angola needs global partners, foreign investment, international technology, and regional cooperation. But it should engage under clear rules, with protection of national interests and knowledge transfer. The strongest position is open sovereignty: cooperating with the world while preserving control over what is strategic.

10th: Participate actively in the African digital agenda.

Many digital challenges require regional or continental scale: cybersecurity, cloud, AI, cross-border payments, data protection, digital trade, and platform regulation. Angola should position itself not merely as a user, but as a leading participant in building the African digital market. Angola's digital sovereignty will be stronger when it is aligned with African digital sovereignty.

For Angola, digital sovereignty means having the national capacity to protect data, operate critical systems, develop talent, negotiate with international partners, and turn technology into economic and social development.

The ultimate criterion should be economic and social development: citizens with better access to services, institutions capable of protecting and operating their systems, and companies able to create value.

Inclusion and sustainability should accompany the implementation of all these decisions.

REFERENCES

Sources and context

The following references support the data and frameworks cited in the text. The matrices, illustrative applications, implementation sequence, and indicators are analytical proposals by LBC.

1 DataReportal

"Digital 2026: Angola". Estimates of internet use and mobile connections, referring to October 2025.

[View the report](#)

2 Republic of Angola

Presidential Decree No. 272/24 of December 5. Approves the "Livro Branco das Tecnologias de Informação e Comunicação 2023-2027".

[View the decree](#)

3 African Union

The Digital Transformation Strategy for Africa (2020–2030). Continental strategy for an inclusive digital society and economy.

[View the strategy](#)

4 African Union

"AU Data Policy Framework". Data policy framework adopted in 2022.

[View the policy framework](#)

5 Republic of Angola

Presidential Decree No. 258/25 of December 3. Creates the National Cybersecurity Council and approves its rules of procedure.

[View the decree](#)

6 World Bank

"Digital Progress and Trends Report 2023". Chapter 4, on digital public infrastructure and cross-sector service delivery.

[View the report](#)

7 UNCTAD

"Digital Economy Report 2024. Shaping an Environmentally Sustainable and Inclusive Digital Future."

[View the publication](#)

LBC

Intelligent Transformation
Digital governance and organizational transformation.