



# Governing Telecom Data for Ethical AI Adoption in North Africa:

## Policy Pathways from Algeria's Experience

**Author:** Zeyneb Zerouali

**Date:** November 2025

# Executive Summary

**Telecommunications** have become one of Algeria's most data-intensive and strategically important sectors. The country's 51 million-plus mobile broadband subscribers generate vast volumes of high-frequency information every day: from location traces and call metadata to service usage and digital payments. These datasets underpin a new wave of artificial intelligence (AI) applications that promise to transform public service delivery, network management, and business innovation. However, without robust data governance, Algerian citizens are at serious risk of surveillance, misuse, and algorithmic bias.

This policy brief argues that the telecommunications sector offers Algeria its most practical entry point for building an ethical, sovereign, and innovation-friendly AI governance model. Reforming how telecom data is classified, managed, and safeguarded can transform it from a fragmented technical resource into a foundation for national competitiveness, public trust, and digital sovereignty.

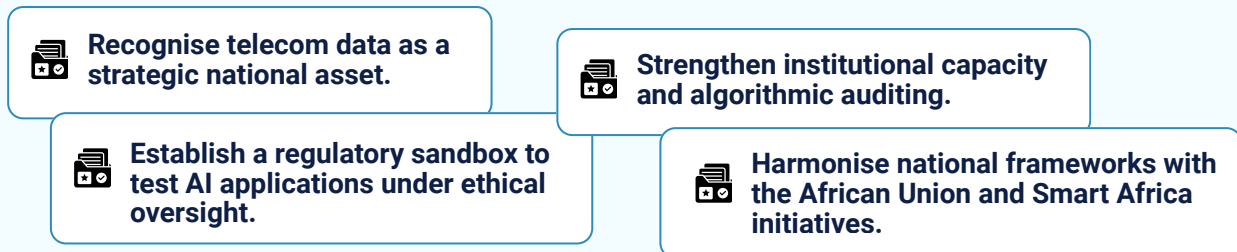
The brief finds that Algeria's current data policy framework, anchored in the 2018 Law No. 18-07<sup>[1]</sup> on personal data protection, remains too narrow to govern AI-driven systems.

[1] Republic of Algeria (2018) Law No. 18-07 on the Protection of Individuals in the Processing of Personal Data. Algiers.



The National Authority for the Protection of Personal Data (ANPDP) and the Regulatory Authority for Post and Electronic Communications (ARPCE) face resource and technical constraints, while cross-border data flows to foreign vendors threaten sovereignty. Public trust in digital systems is fragile, and regional cooperation remains underdeveloped.

To address these challenges, the brief proposes a phased policy agenda:



By acting decisively, Algeria can position itself as a regional leader in ethical and sovereign AI adoption, balancing innovation with accountability, efficiency, and public trust.

1.

## Telecommunications at the Heart of Algeria's Digital Transformation

Telecommunications plays a pivotal role in Algeria's digital transformation, shaping how people connect, how services are delivered, and how data flows across the economy. Mobile connectivity is now deeply embedded in everyday life, with Algeria's mobile-penetration rate reported at over 100% in recent years, a reflection of widespread multi-SIM use and strong reliance on mobile networks. The market, led by Mobilis, Djezzy (Optimum Telecom Algérie), and Ooredoo (Wataniya Telecom Algérie), provides nationwide coverage and continues to expand data services as demand grows. The data-traffic volumes are also significant: ARPCE's Q1-2025 report shows total mobile data traffic of 1.3 billion GB.

Strategically, Algeria expects the telecoms sector to contribute around US\$30 billion to its GDP by 2029, underscoring its significant role in the economy beyond connectivity. As connectivity and data generation expand, the sector becomes a clear entry point for AI innovation: the rich volume and variety of telecom data provide the raw material for machine learning, network optimisation, personalised services, and smarter public systems.

Strategically, Algeria expects the telecoms sector to contribute approximately US\$30 billion to its GDP by 2029, underscoring its significant role in the economy that extends beyond mere connectivity.

2.

## The Governance Gap: When Data Outpaces Regulation

Under the Digital Algeria 2025 strategy, telecom data is recognised as a catalyst for economic diversification and smarter public administration, ranging from predictive maintenance of network assets to e-governance, fraud detection, and personalised customer services. However, AI adoption in Algeria is advancing faster than the institutional and legal systems designed to govern it.

Law No. 18-07 introduced important data protection principles for consent minimisation and legal processing, but it did not address algorithmic accountability, data portability, automated decision-making, or the ethical auditing of AI systems. The ANPDP, tasked with enforcement, is widely understood to operate with a relatively modest state-allocated budget and limited staffing resources (often estimated in commentary at under 500 million DZD and around 50 professionals).<sup>[2]</sup> The authority's limited financial and technical capacity hinders its ability to effectively monitor AI-driven telecom operations or cross-border data flows.

The ARPCE faces similar limitations. While it regulates operators and service quality, it lacks mechanisms for algorithmic oversight, transparency auditing, or ethical review. As telecom operators increasingly rely on foreign vendors for AI analytics and cloud infrastructure, significant volumes of Algerian data are processed abroad, raising concerns over sovereignty, cybersecurity, and compliance with national law.

The ARPCE faces similar limitations. While it regulates operators and service quality, it lacks mechanisms for algorithmic oversight, transparency auditing, or ethical review. As telecom operators increasingly rely on foreign vendors for AI analytics and cloud infrastructure, significant volumes of Algerian data are processed abroad, raising concerns over sovereignty, cybersecurity, and compliance with national law.

At the same time, citizens' trust in digital systems remains low. Existing studies and regional analyses suggest widespread concerns about government surveillance and opaque corporate data practices across Algeria and the North African subregion.<sup>[3]</sup> The absence of transparent mechanisms, such as public reports or independent audits, has deepened this scepticism and slowed the adoption of AI-enabled services.

<sup>[2]</sup> Budget and staffing estimates are drawn from secondary commentary; publicly disclosed official figures are not available.

<sup>[3]</sup> Arab Barometer (2022)

However, systematic, up-to-date surveys of public trust in digital systems in Algeria are limited, highlighting a gap in evidence about citizens' perceptions and experiences with AI and data governance.

3.

## **Telecom Data as a Strategic National Asset**

Telecom data is not a by-product of connectivity; it is a national resource. Properly governed, it can drive evidence-based policymaking, enhance resilience, and unlock new economic opportunities. Yet Algeria lacks a formal data classification or stewardship framework that distinguishes between public, sensitive, and critical datasets.

A national data classification framework would enable a clearer hierarchy of access and protection. Data about critical infrastructure, network integrity, cybersecurity incidents, or emergency response systems needs to be protected at the state level and with restricted access. Robust privacy and consent mechanisms must govern sensitive personal data, including geolocation and communication metadata. Researchers, urban planners, and innovators could then access aggregated or anonymised datasets through defined ethical protocols.

The absence of such a framework has practical consequences. The 2023 nationwide network outage illustrated how fragmented data-sharing arrangements between telecom operators and public agencies delayed emergency coordination. A classification system coupled with inter-agency data protocols would strengthen resilience and reinforce the perception of telecom data as a public asset, not merely a corporate commodity.

4.

## **Structural and Institutional Barriers**

Behind Algeria's governance gap lie deeper systemic challenges. Institutional fragmentation has produced overlapping mandates across ministries of Telecommunications, Digital Economy, Interior, and Security, with no central coordination mechanism for AI or data governance. Data is often treated as a security-sensitive resource rather than a developmental one, discouraging collaboration with academia or industry.

Infrastructure limitations further compound the problem. National data centres remain underdeveloped, and interoperability standards are weak, hindering secure data sharing between governments and private operators. Regulatory decision-making is often reactive, informed by compliance rather than empirical evidence or impact assessments.

These structural deficits also have regional implications. While North African countries share similar data governance challenges, there is no coordinated Maghreb framework for cross-border data exchange. This fragmentation limits Algeria's leverage in continental digital policy and restricts innovation ecosystems that rely on transnational datasets.

5.

## Public Trust and the Social Contract of Data

Public trust is fundamental to digital economy growth. Without it, even the most advanced AI infrastructure cannot achieve social legitimacy. In Algeria, the fragility of digital trust persists due to limited transparency and inadequate public communication regarding the use, storage, or anonymisation of data.

Telecom operators rarely disclose data-handling practices or algorithmic processes that shape pricing, service allocation, or targeted marketing. This opacity fosters public suspicion, particularly in a context where citizens already express concerns over surveillance. Comparative experiences demonstrate that transparency can rebuild trust: Morocco's 2023 Digital Charter requires operators to publish annual transparency reports, while Tunisia's World Bank-supported Digital Governance Unit pilots algorithmic audits for public services. These examples show that clear, consistent communication about AI and data use can simultaneously enhance accountability and stimulate innovation.

6.

## Risks of Inaction

If Algeria fails to reform its data governance framework, several risks may crystallise:

- 🔵 **Erosion of public confidence:** Citizens reluctant to share or consent to data use will constrain both public-sector digital services and private-sector innovation.
- 🔵 **National security exposure:** Unregulated data flows increase vulnerability to cyberattacks and foreign exploitation of strategic datasets.

- **Entrenched inequalities:** AI systems trained on unrepresentative or biased data risk reinforcing existing social and regional disparities in service access.
- **Economic stagnation:** A lack of trusted governance frameworks could deter investment and stifle AI-based business models in telecommunications and beyond.
- **Regional isolation:** Without harmonisation, Algeria may fall behind peers who engage actively in the African Union or Smart Africa data initiatives.

Conversely, proactive reform could yield substantial benefits: a trusted environment for innovation, improved regulatory legitimacy, enhanced cybersecurity, and stronger regional competitiveness aligned with global frameworks such as the OECD AI Principles.<sup>[4]</sup>

## 7. Policy Pathways for Reform

To transform telecom data into a foundation for ethical AI and responsible innovation, Algeria should pursue a sequenced and pragmatic reform agenda anchored in five key priorities.

### **Recognise Telecom Data as a Strategic Public Asset**

Adopt a National Data Classification and Stewardship Framework that differentiates between critical, sensitive, and non-personal data. This will clarify ownership, access rights, and reuse conditions while enabling the safe release of anonymised datasets for research and innovation. Lessons can be drawn from Tunisia's 2022 open-data governance reforms and Morocco's Charte du Numérique, both of which improved inter-agency data coordination and private-sector innovation.

### **Launch a Telecom Data Governance Sandbox**

A controlled regulatory sandbox jointly managed by the Ministry of Post and Telecommunications, ANPDP, and ARPCE should allow operators, startups, and AI researchers to test data-driven applications under supervision. Inspired by the OECD's AI Sandbox Guidelines (2024) and the UAE's AI Lab experience, such a mechanism would promote privacy-by-design innovation, iterative learning between regulators and developers, and early identification of ethical and security risks before large-scale deployment.

### **Strengthen Institutional Capacity and Technical Oversight**

Algeria must expand the technical, analytical, and human resource base of its regulators.

[4] Organisation for Economic Co-operation and Development (OECD) (2024) *AI and Data Policy in Telecommunications*. Paris.

Establishing a Digital Governance and AI Unit within the ANPDP would enable algorithmic audits, AI impact assessments, and coordination with research institutions. Partnerships with the ITU's AI for Good programme and local universities could facilitate training in data science, privacy engineering, and ethics. An AI and Data Governance Fund could finance capacity building, infrastructure, and joint public-private innovation projects.

### **Mandate Transparency and Algorithmic Accountability**

Amend Law No. 18-07 to require mandatory AI Impact Assessments for telecom systems processing personal or behavioural data. Telecom operators should publish annual Data Ethics and Transparency Reports, detailing how datasets are anonymised, shared, and audited. Independent external reviews should evaluate algorithmic fairness, accuracy, and potential discrimination. These reforms would strengthen user confidence in AI-driven services.

### **Promote Regional Harmonisation and Cooperation**

Algeria should take a leadership role in establishing a Maghreb Data Governance Charter under the African Union's Data Policy Framework (2022), collaborating with Morocco, Tunisia, and Mauritania. Shared principles on privacy, data mobility, and ethical AI would enable cross-border innovation, digital trade, and joint capacity-building while enhancing the region's collective voice in global digital governance forums.

## **8. Implementation Roadmap**

Reform must proceed in phases, each building the institutional, legal, and social foundations for sustained ethical AI governance.

### **Phase 1 (2025–2026): Foundation and Capacity Building**

National consultations should define the roles of the ANPDP, ARPCE, and key ministries. Training programmes for data protection officers, regulators, and telecom engineers should be launched in collaboration with universities and international partners. A pilot telecom sandbox engaging at least two major operators will serve as a proof of concept.

### **Phase 2 (2026–2028): Legal Reform and Institutional Integration**

Law No. 18-07 should be amended to integrate AI governance, algorithmic transparency, and cross-border data-sharing provisions.

A National Inter-Ministerial Committee on AI and Data Governance, chaired by the Prime Minister's Office, should coordinate national policy. Fiscal incentives and recognition schemes could encourage compliance and ethical innovation by telecom operators.

### **Phase 3 (2028–2030): Consolidation and Evaluation**

Best practices developed during earlier phases should be institutionalised in regulatory codes and national legislation. Annual Telecom Data Governance Reports should assess implementation outcomes, while public awareness campaigns build digital literacy and trust. The process should remain adaptive, incorporating new insights as AI technologies evolve.

9.

## **Anticipated Barriers and Mitigation Strategies**

Reform will inevitably face political, financial, and institutional resistance. Several mitigation measures can ensure continuity and buy-in:

**Limited financial and human capacity** can be mitigated through partnerships with the ITU, OECD, and AU initiatives, alongside capacity-building grants and technical assistance.

**Resistance from telecom operators**, concerned about compliance costs, can be eased through phased implementation, tax relief for compliant firms, and public recognition for ethical innovation.

**Jurisdictional overlaps** between ministries and regulators should be resolved through clear mandates under the Inter-Ministerial Committee and shared data-exchange protocols.

**Public scepticism** can be addressed by engaging civil society, consumer associations, and privacy advocates in consultative councils and public communication strategies.

## Conclusion: From Data Fragility to Digital Sovereignty

The governance of telecom data sits at the intersection of Algeria's technological ambition, national security, and social contract. Data governance is no longer a technical issue; it is a question of public legitimacy and sovereignty. By treating telecom data as a strategic asset and embedding ethics, transparency, and accountability in its management, Algeria can move from reactive regulation to proactive leadership.

Reforming data governance will safeguard citizens and enable innovation to flourish within trusted boundaries. With coordinated institutions, modernised laws, and regional cooperation, Algeria can demonstrate that ethical AI is compatible with economic dynamism and national sovereignty. In doing so, it can set a precedent for North Africa, proving that digital transformation, when grounded in integrity and inclusion, becomes a pathway not just to growth, but to collective empowerment.

**Acknowledgements:** This paper was developed through the Africa's Data Future Fellowship, a CSEA initiative that builds expert capacity for evidence-based data policy in Africa. The Fellowship is part of CSEA's wider data governance programme, supported by the William and Flora Hewlett Foundation. The author gratefully acknowledges the project team's guidance and collaboration.

**Disclaimer:** The views expressed here are the author's own and do not necessarily reflect the positions of CSEA, the Fellowship, or the Hewlett Foundation. This work contributes to policy dialogue on data governance and ethical digital transformation in Africa.