

Search information

Received 09/05/2026
Accepted .20/10/2026.

Printed ISSN: 2352-989X
Online ISSN: 2602-6856

Digital Sovereignty in Algeria

An Analysis of Policymakers' Vision within the 2025–2030 Digital Transformation Strategy

Abdelhadi Kherbouche

¹ University of Blida 2(Algeria),

.kherbouche@univ-blida2.dz

ABSTRACT

The shifting geopolitical landscape and escalating threats have profound implications for the security of countries such as Algeria, particularly in cyberspace. The sharp rise in cyberattacks originating in hostile states accentuates the urgent need for carefully targeted strategic measures to detect and prevent state-sponsored cyber operations and mitigate their effects. Contemporary geopolitical conflicts frequently target critical infrastructure, including energy grids, transport networks and communications systems. Algerian policymakers have therefore prioritized stronger digital infrastructure to counter sophisticated, coordinated attacks. These efforts form part of the pursuit of digital sovereignty during 2025–2030, with particular emphasis on safeguarding state security against threats to sensitive databases.

Keywords: digital sovereignty; cyber threats; cybersecurity; information security; data governance; digital transformation.

INTRODUCTION

For Algerian policymakers, digital sovereignty is no longer confined to the digitization of public services. It increasingly concerns who controls data, digital infrastructure, technological capabilities, and the rules governing the digital environment. In this sense, what began largely as a technical project has developed into a broader strategic concern. It now bears directly on state security, autonomy in decision-making, the resilience of the national economy to external shocks, and the capacity to protect critical systems against cyberattacks.

In practical terms, this sovereignty is materialized through high-performance computing infrastructure that stores and secures government databases within national borders. Defined as a state's capacity to exercise authority over its digital infrastructure, data, platforms and technologies, digital sovereignty has become a central concern in academic and policy debate. Revelations of large-scale surveillance and growing dependence on foreign digital services and infrastructure have sharpened that concern.

Against this backdrop, the study raises the following research question: Does the strategic vision of Algerian policymakers represent a substantive step from digital transformation towards digital sovereignty?

1. Definition of Digital Sovereignty

Digital sovereignty refers to a state's capacity to control its digital infrastructure, data and technologies independently of foreign influence or control. In an interconnected world, it is vital to national security, economic stability and individual privacy. Understanding digital sovereignty requires attention to both defensive mechanisms and offensive capabilities, with a view to advancing digital innovation. This understanding underpins the close relationship between digital sovereignty and cybersecurity.¹

Digital sovereignty is no single, settled concept. It is a contested field in which different understandings of control, independence and authority over technology, data and infrastructure compete.² Some scholars distinguish it from related terms, including cyber sovereignty, information sovereignty and data sovereignty.³ Others examine the actors who claim digital sovereignty: governments, private-sector actors and citizen groups.⁴ A third

¹ Gideon Mekonnen and Iris Reychav, "Digital Sovereignty in the Global South: Autonomy in a Connected World," *Procedia Computer Science*, vol. 278 (2026), p. 598.

² Samuele Fratini et al., "Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models," *Digital Society*, 14 November 2024, p. 22.

³ Patrik Hummel, Matthias Braun, Max Tretter and Peter Dabrock, "Data Sovereignty: A Review," *Big Data & Society*, vol. 8, no. 1 (2021). <https://doi.org/10.1177/2053951720982012>

⁴ M. Tretter, "Sovereignty in the Digital and Contact Tracing Apps," *Digital Society* (2023). <https://doi.org/10.1007/s44206-022-00030-2>

approach distinguishes between national and regional models, notably those associated with China, the European Union and the United States.

Glasze and colleagues argue that digital sovereignty has moved beyond a narrowly technical concern to become a geostrategic imperative encompassing autonomy, power relations and control over digital ecosystems.⁵ Pierucci similarly observes that, although no universally accepted definition exists, digital sovereignty generally entails a reinterpretation of traditional state authority in the digital sphere, with significant implications for economic policymaking, security governance and the regulation of information flows.⁶ According to Couture and Toupin,⁷ it also involves the capacity of states, local communities and civil society organizations to drive technological innovation, including the development of domestic industries and open-source infrastructure, while safeguarding the privacy and security of individuals and groups. Initially rooted in concerns over national security and state authority, the concept subsequently expanded to encompass economic autonomy, technological progress and citizens' digital rights. Digital sovereignty has thus become a central, contested force in shaping the future of the digital state.

Pohle and Thiel identify state autonomy, economic self-determination and individual rights as fundamental dimensions of digital sovereignty⁸.

Moerel and Timmers likewise connect it to strategic autonomy, defining it as “the capacity to decide and act independently on the essential digital aspects of our long-term future in the economy, society and democracy”.⁹ Other scholars question whether traditional sovereignty can apply in cyberspace.¹⁰ They contend that the Internet's technical architecture undermines territorial sovereignty and that cyberspace should be treated as a global commons in which states cooperate.

In the Global South, however, digital sovereignty carries particular weight because of colonial legacies, persistent technological dependence and geopolitical marginalization. This study examines the factors shaping digital sovereignty in Algeria. It also considers the strategies through which policymakers seek national control over critical digital infrastructure, the model used to govern cyberspace, and the promotion of domestic innovation.

⁵ George Glasze et al., “Contested Spatialities of Digital Sovereignty,” *Geopolitics*, vol. 28 (2022), pp. 915–958.

⁶ Federic Pierucci, “Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace,” *Digital Society*, vol. 4 (2025), pp. 1–19.

⁷ Nick Couldry and Ulises A. Mejias, “Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject,” *Television & New Media* (2019), pp. 336–349.

⁸ Julia Pohle and Thorsten Thiel, “Digital Sovereignty,” *Internet Policy Review*, vol. 9 (2020), pp. 1–19.

⁹ Lokke Moerel and Paul Timmers, “Reflections on Digital Sovereignty,” *EU Cyber Direct*, Research in Focus Series (2021), pp. 1–33.

¹⁰ Milton L. Mueller, “Against Sovereignty in Cyberspace,” *International Studies Review*, vol. 22 (2020), pp. 779–801.

2. Definition of Digital Transformation

The roots of digital transformation can be traced to the 1980s and early 1990s, when researchers began examining how the adoption of information technology (IT) affected organizational structures, innovation and performance. As demand for computer technologies grew and Internet use spread, IT-enabled business transformation gained prominence during the 1990s. Global crises, including COVID-19, later renewed its urgency.

The expanding reach and capabilities of IT systems brought digital transformation research into management, economics, entrepreneurship, strategic management, operations management, marketing and organizational studies. Digital transformation (DT) is consequently a multidisciplinary field of research.¹¹ Fitzgerald et al. define it as “the use of new digital technologies (social media, mobile, analytics or embedded devices) to enable major business improvements (such as enhancing customer experience, streamlining operations or new business models”.¹²

Liu et al. describe digital transformation as “an organizational transformation that integrates digital technologies and business processes within a digital economy”.¹³

Singh and Hess favor the term “transformation” over “change”. They emphasize that organizational digital transformation extends beyond functional thinking to encompass the full range of measures required to exploit the opportunities, or avoid the threats, arising from digital technologies.¹⁴ Rogers, for his part, argues that “Digital transformation is not about technology—it is about strategy and new ways of thinking”. Senior leadership teams must therefore find ways to turn new and unforeseen innovations into business models that better address customer needs and experiences.¹⁵

Several related conceptualizations follow from these approaches. Vial defines digital transformation as a process aimed at improving an entity’s operational efficiency, enhancing customer experience and developing new business models to increase competitiveness and create new revenue streams.¹⁶

¹¹ K. S. R. Warner and M. Wäger, “Building Dynamic Capabilities for Digital Transformation: An Ongoing Process of Strategic Renewal,” *Long Range Planning*, vol. 52, no. 3 (2019), p. 327.

¹² M. Fitzgerald, N. Kruschwitz, D. Bonnet and M. Welch, “Embracing Digital Technology: A New Strategic Imperative,” *MIT Sloan Management Review*, vol. 55 (2014), 1–12. P, 1

¹³ D.-Y. Liu, S.-W. Chen and T.-C. Chou, “Resource Fit in Digital Transformation,” *Management Decision*, vol. 49, no. 10 (2011), p. 1730.

¹⁴ A. Singh and T. Hess, “How Chief Digital Officers Promote the Digital Transformation of Their Companies,” *MIS Quarterly Executive* (2017), p. 16.

¹⁵ D. Rogers, *The Digital Transformation Playbook: Rethink Your Business for the Digital Age* (New York: Columbia University Press, 2016), p. 11

¹⁶ G. Vial, “Understanding Digital Transformation: A Review and a Research Agenda,” *Journal of Strategic Information Systems*, vol. 28 (2019). <https://doi.org/10.1016/j.jsis.2019.01.003>. Accessed 7 June 2026.

This definition is among the most frequently cited in the literature. It focuses on three dimensions: efficiency, experience and business models.

Asma Ezzat Othman Ahmed defines it as a process based on the extensive use of information and communication technologies in educational settings, with effects across all components of the education system.¹⁷

3. Digital Sovereignty and Cybersecurity

Digital sovereignty is closely tied to cybersecurity. The latter is essential to national security because it protects government systems, military infrastructure and critical sectors against cyberattacks and espionage by foreign actors. Effective cybersecurity also ensures that citizens' personal data and sensitive national data remain within national borders, reducing the risk of external surveillance or exploitation. It is therefore a practical prerequisite for digital sovereignty: a state cannot exercise effective sovereignty over its data or public services if its networks, data centers and applications remain vulnerable to intrusion or disruption from abroad.¹⁸ Conversely, digital sovereignty strengthens cybersecurity by giving the state greater visibility over data location, infrastructure operators, communication routes, access privileges and incident-response mechanisms.

Against this backdrop, security agencies in Western countries, particularly EU member states, have strengthened their capacity to monitor domestic developments through surveillance. Their aim is to counter security threats,¹⁹ whether from terrorist organizations or foreign espionage. This concern intensified after the US Federal Bureau of Investigation and Central Intelligence Agency directly accused Russian President Vladimir Putin of ordering his agencies to influence the 2016 US presidential election through false information on social media and strategically released leaks, favoring the current US president, Donald Trump, over Democratic candidate Hillary Clinton.²⁰ Concerns about foreign electoral interference spread well beyond the United States, notably to France, the United Kingdom and other European countries. These states consequently expanded their development of information, surveillance and monitoring technologies to protect cybersecurity.²¹

¹⁷ Asmaa Ezzat Othman Ahmed, "Digital Transformation in Pre-University Education in Light of the Concept of the New Republic: An Analytical Study," Ahmed El-Minshawi Centre for Scientific Publishing and Research Excellence, Faculty of Education, Assiut University, vol. 41, no. 4, April 2024. https://mfes.journals.ekb.eg/article_431140.html. Accessed 21 June 2026.

¹⁸ Abdelhalim Al-Hourani, "Artificial Intelligence and Sovereign Cybersecurity," *Al-Wa'i*, no. 482 (2026). <https://www.alwaie.org/archives/article/20482>. Accessed 27 July 2026.

¹⁹ Edoardo Celeste, "Digital Sovereignty in the EU: Challenges and Future Perspectives," in *Data Protection Beyond Borders*, edited by Federico Fabbrini, Edoardo Celeste and John Quinn (2021). Accessed 13 April 2026.

²⁰ Michael N. Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law," Exeter Centre for International Law Working Paper Series, no. 3 (2018). <https://bit.ly/2NU691A>

²¹ Shadi Abdelwahab Mansour, *Fifth-Generation Warfare: Methods of Destabilisation from Within in the International Arena*, 1st ed. (Cairo: Al-Arabi Publishing and Distribution, 2019), p. 157.

Cybersecurity thus builds confidence in national infrastructure among government bodies and citizens alike, strengthening resilience to threats that could erode sovereignty. A central difficulty lies in dependence on foreign software and hardware within global technology supply chains. Such dependence can create vulnerabilities that may be exploited for espionage. State-sponsored cyberattacks and cyber espionage by foreign actors pose a further, growing concern, making sovereignty harder to protect. The widespread adoption of emerging, disruptive technologies compounds these problems by introducing new vulnerabilities and enlarging the attack surface.

Cybersecurity research can help address these challenges. Investment in domestic research allows states to develop their own tools and solutions for protecting critical infrastructure, reducing reliance on foreign providers. Building local expertise also supports more effective detection of, and responses to, emerging threats, as well as the deployment of offensive cyberwarfare capabilities. Research in cryptography, distributed ledger technology and secure data storage can further strengthen the protection of, and control over, national data.

Digital sovereignty has accordingly become a prominent geopolitical watchword in a world marked by political uncertainty, shifting alliances and emerging technologies. States pursue it through socioeconomic, political and security strategies, even as digital integration and interdependence deepen.²² These efforts reflect anxiety over a loss of control alongside a desire for autonomy in the digital world, particularly in the aftermath of the COVID-19 pandemic.

4. Models of Digital Sovereignty

Four models of digital sovereignty can be distinguished according to their defining characteristics, underlying values and intended objectives.²³

A. The Rights-Based Model

The rights-based model treats digital regulation as a means of advancing fundamental rights and democracy. It seeks a workable balance between rights and the benefits of markets, while taking an assertive regulatory approach towards private companies. Its ultimate purpose is to extend and strengthen citizens' rights in the digital sphere. Although it includes measures that assert state sovereignty over digital companies, state control serves a further objective:

²² See generally Anupam Chander and Haochen Sun, *Data Sovereignty: From the Digital Silk Road to the Return of the State*, 1st ed. (Oxford University Press, 2023), Introduction; Farid Gueham, "Digital Sovereignty: Steps towards a New System of Internet Governance" (Fondapol, February 2017), accessed 20 October 2023; Edoardo Celeste, "Digital Sovereignty in the EU: Challenges and Future Perspectives," in *Data Protection Beyond Borders*, edited by Federico Fabbrini, Edoardo Celeste and John Quinn (Hart, 2021), accessed 13 April 2026.

²³ S. Fratini, E. Hine, C. Novelli, H. Roberts and L. Floridi, "Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models," *Digital Society*, vol. 3 (2024), art. 59, p. 10.

enabling citizens to act freely online. This objective is commonly expressed through the language of autonomy, empowerment and user sovereignty.

B. The Market Oriented Model

The free-market model privileges economic freedom, market benefits and competition-driven innovation over state regulation. This suggests that states adopting the model avoid regulation altogether. The United States is often presented as the quintessential neoliberal state, responsible for the emergence of technology corporations that now appear beyond effective control. Yet their development is difficult to imagine without substantial federal intervention. As Chander argues, Silicon Valley companies cultivated a neoliberal discourse even as “American judges and legislators at the turn of the millennium adapted the law to support the development of Internet companies”, much as nineteenth-century judges had supported industrial development.²⁴

Even the most neoliberal states, then, did not leave technology companies wholly unregulated. They actively supported their growth by allocating substantial public funding to research and development. As political tensions with China have increased, the United States has relied more heavily on industrial policy to preserve its advantage in emerging technologies.²⁵

C. The State-Based Model

The state-based model is characterized by a blurred boundary between the public and private sectors, a view of digital media as instruments of nation-building and socioeconomic development, near-total reliance on domestic digital resources, substantial investment in emerging technologies, and an ambition to export governance norms and digital standards. Unlike in the other models, the close relationship between digital companies and state authorities makes it difficult to speak of an attempt to reassert state sovereignty over companies.

D. The Centralized Model

This model reconfigures digital governance around centralized regulation, understood here as the exclusion of non-state actors from decision-making. Centralization is an ongoing process and varies in degree. Countries associated with this model have often previously followed more flexible regulatory approaches resembling those of Western countries, but began changing course in the early 2010s. This distinct transition towards centralized governance separates the model from the state-based approach. Rather than delegating

²⁴ A. Chander, “How Law Made Silicon Valley,” *Emory Law Journal*, vol. 63, no. 3 (2013), pp. 639–694.

²⁵ H. Roberts, Hine and L. Floridi, “Digital Sovereignty, Digital Expansionism, and the Prospects for Global AI Governance,” in *Quo Vadis, Sovereignty?*, edited by M. Timoteo, B. Verri and R. Nanni, *Philosophical Studies Series*, vol. 154 (Springer Nature Switzerland, 2023), pp. 51–75. https://doi.org/10.1007/978-3-031-41566-1_4

governance and drawing on the infrastructural features of the digital sphere to enforce content rules and economic and legal provisions, these states commonly establish powerful new regulatory bodies.²⁶

5. The Legal and Institutional Framework for Digital Sovereignty in Algeria

Presidential Decree No. 25-320 of 30 December 2025²⁷ constitutes a foundational instrument in Algeria's construction of sovereign digital infrastructure. Its significance extends beyond the technical management of data: it redefines the relationship between the state and data by treating the latter as a strategic sovereign resource, comparable in importance to natural and financial resources.²⁸

This legal instrument formally establishes what may be termed a “data-driven state”. Public administration moves from paper-based procedures or fragmented digital systems towards comprehensive data governance. A defining feature of the decree is the shift from treating data as mere outputs of information systems to recognizing them as strategic assets requiring clear rules for their production, use, protection and exchange.

This shift is evident in the precise legal definition of key concepts. A “data source” is no longer simply a technical producer: it bears legal responsibility for data quality, reliability, updating, classification and indexing, thereby establishing institutional accountability for data. The concept of a “data user” similarly restricts use to a specified functional purpose, affirming the principle of lawful, purpose-bound use of public data.

“Data exploitation” encompasses the entire data lifecycle, from recording to retention and encryption. This broader definition reflects legislative recognition that control over data concerns their added value as much as their storage. Such conceptual precision acknowledges that digital sovereignty depends on the rules governing the production and circulation of information within the state, alongside its infrastructure.

The National Interoperability System²⁹ is the decree's principal technical and legal pillar. It addresses a persistent weakness of public administration: fragmented data and isolated information systems. The system establishes an exclusive, unified framework for digital data exchange among public institutions and administrations, intended to replace ad hoc and bilateral practices.

²⁶ Samuele Fratini et al., “Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models,” p. 16.

²⁷ See Official Gazette, no. 87: Presidential Decree No. 25-320 of 10 Rajab 1447 AH, corresponding to 30 December 2025, establishing a national data governance framework.

²⁸ Khemissi Ghanem, “Data Governance in Algeria: Laying the Foundations for Digital Sovereignty and Modern Administration,” Al-Sarih, 17 January 2026. <https://sarih.dz/66958/>. Accessed 12 May 2026.

²⁹ See High Commission for Digitalisation, “National Interoperability System.” <https://www.hcn.dz/projets/FondementTechnologique/Datashiring>

Secure, orderly data flows should reduce duplication, improve public services and accelerate decision-making. Reliance on a secure, closed national network separated from the Internet is itself a sovereign choice, reflecting an awareness of the risks associated with open infrastructure when handling sensitive data. Algeria's digital transition thus moves from the digitization of individual procedures towards the digitization of the state as an integrated whole, in which data are shared under common controls.³⁰

The decree embeds security within digital governance as a structural requirement for successful transformation. Mandatory classification and indexing under a national framework that specifies levels of sensitivity enable protection proportionate to risk. Responsibilities are also clearly allocated. The High Commission for Digitalization provides technical and regulatory leadership; the National Council for Information Systems Security³¹ seeks to ensure the system's functional integrity; and the National Authority for the Protection of Personal Data³² oversees respect for individual rights and freedoms.

Law No. 25-11 of 24 July 2025, amending and supplementing Law No. 18-07 of 10 June 2018 on the protection of natural persons with regard to the processing of personal data, introduces further definitions and obligations. These include requirements concerning data protection officers (DPOs), processing records, registration, data protection impact assessments, prior consultation for high-risk processing and breach notification.

This allocation reflects an approach that separates production, regulation and oversight, preventing digital authority from being concentrated in a single body. Sovereign exceptions relating to defense, national security and justice also affirm that digital openness remains subject to clear limits and does not entail relinquishing the core of sovereignty.³³

6. Algeria's Strategy for Building Digital Sovereignty in 2025–2030

Across Africa, digital sovereignty has moved from academic debate into the realm of national security priorities. Kenya, Ghana, Nigeria and Algeria now require certain categories of data to be stored and processed within their borders. Algeria's approach is distinctive: rather than relying on a single law, it has sought to construct a multilayered regulatory framework that progressively tightens control over where data reside and who may access them.

³⁰ Khemissi Ghanem, "Data Governance in Algeria: Laying the Foundations for Digital Sovereignty and Modern Administration."

³¹ Fatiha Hezam, "Protecting Digital Systems through Technical Mechanisms and Protection Bodies: A Reading of Presidential Decree No. 20-05," *Journal of Law and Human Sciences*, no. 3, October 2020, p. 181.

³² See the official website of the National Authority for the Protection of Personal Data. <https://anpdp.dz/ar/>

³³ Khemissi Ghanem, "Data Governance in Algeria: Laying the Foundations for Digital Sovereignty and Modern Administration."

To protect state institutions and national bodies against threats in cyberspace, the Ministry of National Defense's Information Systems Security Agency published the first edition of the National Information Systems Security Strategy for 2025–2029 on 3 March 2026, following its approval by President Abdelmadjid Tebboune. The strategy provides a comprehensive framework for national cyber resilience, the protection of state digital infrastructure and data, and citizens' security in cyberspace. It accompanies the national leadership's efforts to accelerate digital transformation across state institutions.

As a roadmap, it seeks to preserve national digital sovereignty, ensure essential public services and strengthen citizens' trust in their digital environment.

Its preparation involved relevant state institutions and public and private bodies, an assessment of the national digital landscape, and the identification of difficulties and potential obstacles. Developments in digital technologies and the classification of cyber threats were also taken into account. The strategy's pillars reflect a policymaking vision whose main features can be outlined as follows.

A. Data Governance

Algeria has implemented legislation protecting individuals in the processing of personal data and imposes data-localization requirements on e-commerce, cloud services and media content.³⁴

The law on the protection of individuals in the processing of personal data entered into force in August 2023. It grants individuals rights of access, rectification and objection to processing. Data controllers and processors must ensure lawful, fair and transparent processing and implement appropriate security measures against unauthorized access, alteration or destruction. Controllers must also notify the National Authority for the Protection of Personal Data (ANPDP) before processing personal data. Prior authorization is required where processing is likely to pose a clear risk to individuals' fundamental rights and freedoms.

Algeria's cybersecurity framework comprises several sectoral arrangements. In January 2021, Decree No. 20-05 required the appointment of a dedicated information systems security officer. It also established the National Council for Information Systems Security to formulate strategies and approve policies, and the National Information Systems Security Agency to implement them.

³⁴ Maria Buza and Sherif Taha, "DPA Digital Digest: Algeria [2025 Edition]: A Close-Up of Algeria's Regulatory Approach to Data Governance, Content Moderation, Competition, Artificial Intelligence, and More," 16 April 2025. <https://digitalpolicyalert.org/digest/dpa-digital-digest-algeria>. Accessed 16 June 2026.

Law No. 18-04 of 2018 requires electronic communications providers to secure networks, protect data confidentiality and prevent unauthorized interception of communications.³⁵

Law No. 09-04 of 2009 requires information and communication technology providers to adopt technical measures that protect stored data.

Algeria also participates in international data-governance initiatives. In October 2024, the ANPDP signed a memorandum of understanding with Mauritius's Data Protection Office to strengthen cooperation on data protection rules.

In December 2024, the law governing audiovisual activities entered into force, requiring online audiovisual services to be hosted exclusively on servers physically located in Algeria and to use the national “.dz” domain.

In June 2024, the law on print and electronic media required electronic press providers to use websites hosted exclusively on physical infrastructure in Algeria, under the “.dz” domain.

In November 2018, the e-commerce law introduced an obligation for e-commerce businesses to host their websites under a domestic “.dz” domain and register in the national commercial register.

In November 2017, the Regulatory Authority for Post and Electronic Communications issued rules requiring public cloud service operators to locate their infrastructure in Algeria and to host and store their data domestically.³⁶

B. Content Oversight and Moderation

Algeria has implemented laws regulating audiovisual and online content and has introduced domestic-content quotas. Its content-moderation framework comprises several laws.

In December 2024, Algeria implemented the law on audiovisual activities. It prohibits audiovisual and online communications services from disseminating content that promotes violence, terrorism, racial discrimination or false information. The law also extends the audiovisual regulator's remit to content published on digital platforms and sets a domestic-content quota of 60%.

In June 2024, Algeria implemented the law on print and electronic media, empowering the print and electronic press regulator to suspend publications or websites for up to 30 days where statutory obligations are breached. Violations include publishing material that

³⁵ Maria Buza and Sherif Taha, *ibid.*

³⁶ Maria Buza and Sherif Taha, *ibid.*

undermines national defense and security, territorial integrity, public order, Islam or public morals. Online media must notify the competent authorities and remove such material or block access to it immediately upon detection.

The 2009 law on preventing and combating offences related to information and communication technologies requires Internet service providers to remove illegal content, or block access to it, as soon as it is detected, particularly where it violates public order or public morals. Providers must introduce technical measures to restrict access to prohibited content and inform subscribers of those restrictions. The law also includes copyright protection to prevent the unauthorized use of protected digital content.

In November 2021, Decree No. 21-439 reorganized the National Body for the Prevention and Combating of Offences Related to Information and Communication Technologies. Subject to judicial authorization, the body may conduct preventive monitoring of electronic communications to detect terrorist acts, subversive activities or threats to state security.³⁷

In June 2012, Law No. 12-05 established the audiovisual regulatory authority, responsible for monitoring compliance with content standards in the audiovisual sector. The law also established the print and electronic press regulator, which oversees content standards in print and online media.

Internationally, Algeria participates in several initiatives concerning digital content. In February 2024, Algeria joined other African governments in adopting the Association of African Electoral Authorities' "Guidelines for the Use of Digital and Social Media", which set standards for the responsible use of digital platforms during electoral processes.

In June 2023, Algeria was among 71 governments that signed the "International Statement on the Removal of Online Child Sexual Abuse Material", committing to proactive measures against online child exploitation.

In May 2024, Algeria, as an African Union member, adopted the "Child Online Safety and Empowerment Policy", which provides a framework for protecting children online while strengthening digital literacy and skills.

C. Competition Policy

Algeria applies its Competition Ordinance to digital markets and authorizes the Regulatory Authority for Post and Electronic Communications to identify and regulate operators with significant market power in telecommunications markets.

³⁷ Maria Buza and Sherif Taha, *ibid.*

Algeria has not adopted competition rules specifically for digital markets; the Competition Ordinance of 2003 applies instead. It prohibits abuse of a dominant position, including predatory pricing, territorial restrictions and discriminatory treatment of trading partners. It also prohibits anticompetitive agreements that restrict market access, limit output or fix prices.³⁸

Two amending laws expanded the obligations under the Competition Ordinance. In August 2010, Law No. 10-05 introduced measures to regulate prices during market disruption, requiring transparent pricing structures and non-discrimination to prevent unfair treatment of trading partners.

In July 2008, Law No. 08-12 broadened the provisions on anticompetitive agreements and merger control. Entities must notify the Competition Council and obtain its approval for mergers “likely to affect competition”.

In May 2018, Algeria also implemented the law establishing the general rules governing postal services and electronic communications. It prohibits anticompetitive practices, including abuse of a dominant position, refusal to share essential facilities and discriminatory conduct by operators. The law further empowers the Regulatory Authority for Post and Electronic Communications to designate “operators with significant market power” and impose corrective measures to address anticompetitive conduct.

D. Artificial Intelligence

Algeria has not yet adopted laws or regulations specifically governing the development and use of artificial intelligence. In June 2023, however, the Ministry of Higher Education and Scientific Research and the Ministry of the Knowledge Economy jointly established an “Artificial Intelligence Council”. The council advises on AI development and governance and is tasked with aligning innovation with national priorities and ethical standards.

In December 2024, the Artificial Intelligence Council announced an AI strategy intended to advance technological growth and global competitiveness through research, innovation and infrastructure. It envisages a national AI fund, stronger data systems, and domestic and international investment. The strategy also proposes expanding the data protection authority’s role in overseeing data protection and enforcing AI regulations, alongside the development of a legal framework for AI and the extension of existing data-privacy rules to address AI-specific concerns.³⁹

Internationally, Algeria has endorsed several AI-governance initiatives. The African Union, of which Algeria is a member, has adopted a “Continental Artificial Intelligence

³⁸ Maria Buza and Sherif Taha, *ibid.*

³⁹ Maria Buza and Sherif Taha, *ibid.*

Strategy” for digital transformation and an “AI Governance Framework”, alongside a cooperation agreement with China on AI research and development. Moreover, the African Continental Free Trade Area’s “Protocol on Digital Trade” was adopted in February 2024. It provides that parties should facilitate the adoption and regulation of emerging and advanced technologies in line with public-policy and security interests, and develop governance frameworks that ensure their ethical, trustworthy, safe and responsible use.

Conclusion

The study demonstrated that considering digital sovereignty in Algeria has developed alongside the digital transformation strategy, the construction of a knowledge economy, and efforts to improve the country’s standing in indicators of innovation, artificial intelligence, infrastructure and the legislative environment. Algeria has considerable latent capacity. Its success, however, depends on increased research and development expenditure, stronger telecommunications and better regulatory and legislative conditions.

The trajectory of e-government also shows that Algeria adopted an early program to expand IT use, develop broadband infrastructure, train human resources and adapt the legal framework. Practical initiatives include the artificial intelligence school and the Sidi Abdellah smart-city project. Policies supporting e-learning have accompanied administrative modernization, the creation of information platforms and a government data center to support monitoring and decision-making.

Digital sovereignty therefore appears to be an increasingly central structural priority in Algerian policymakers’ strategic thinking. Its effectiveness depends on translating digital transformation into integrated sovereign policy objectives that connect digital infrastructure with security, innovation, legislation, the economy and political decision-making.

References

Translated Arabic-Language Sources

1. Mansour, Shadi Abdelwahab. *Fifth-Generation Warfare: Methods of Destabilization from Within in the International Arena*. 1st ed. Cairo: Al-Arabi Publishing and Distribution, 2019.
2. Hezam, Fatiha. "Protecting Digital Systems through Technical Mechanisms and Protection Bodies: A Reading of Presidential Decree No. 20-05." *Journal of Law and Human Sciences*, no. 3, October 2020, p. 181.
3. Ahmed, Asmaa Ezzat Othman. "Digital Transformation in Pre-University Education in Light of the Concept of the New Republic: An Analytical Study." Ahmed El-Minshawi Centre for Scientific Publishing and Research Excellence, Faculty of Education, Assiut University, vol. 41, no. 4, April 2024.
4. Ghanem, Khemissi. "Data Governance in Algeria: Laying the Foundations for Digital Sovereignty and Modern Administration." *Al-Sarih*, 17 January 2026.
5. Al-Hourani, Abdelhalim. "Artificial Intelligence and Sovereign Cybersecurity." *Al-Wa'i*, no. 482, 2026.
6. Official Gazette, no. 87. Presidential Decree No. 25-320 of 10 Rajab 1447 AH, corresponding to 30 December 2025, establishing a national data governance framework.
7. High Commission for Digitalisation. "National Interoperability System." <https://www.hcn.dz/projets/FondementTechnologique/Datashiring>
8. National Authority for the Protection of Personal Data. Official website. <https://anpdp.dz/ar/>

Foreign-Language Sources

1. Mekonnen, Gideon, and Iris Reyhav. "Digital Sovereignty in the Global South: Autonomy in a Connected World." *Procedia Computer Science*, 2026.
2. S. Fratini, E. Hine, C. Novelli, H. Roberts and L. Floridi, "Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models," *Digital Society*, vol. 3 (2024).
3. Hummel, Patrik, Matthias Braun, Max Tretter and Peter Dabrock. "Data Sovereignty: A Review." *Big Data & Society*, 2021.
4. Tretter, M. "Sovereignty in the Digital and Contact Tracing Apps." *Digital Society*, 2023.
5. Glasze, George, et al. "Contested Spatialities of Digital Sovereignty." *Geopolitics*, vol. 28, 2022.
6. Pierucci, Federic. "Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace." *Digital Society*, vol. 4, 2025.
7. Couldry, Nick, and Ulises A. Mejias. "Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject." *Television & New Media*, 2019.
8. Pohle, Julia, and Thorsten Thiel. "Digital Sovereignty." *Internet Policy Review*, vol. 9, 2020.
9. Gravett, Willem. "Digital Neo-Colonialism: The Chinese Model of Internet Sovereignty in Africa." *African Human Rights Law Journal*, vol. 20, 2020.

10. Moerel, Lokke, and Paul Timmers. "Reflections on Digital Sovereignty." EU Cyber Direct, Research in Focus Series, 2021.
11. Mueller, Milton L. "Against Sovereignty in Cyberspace." *International Studies Review*, vol. 22, 2020.
12. Chander, Anupam, and Haochen Sun. *Data Sovereignty: From the Digital Silk Road to the Return of the State*. 1st ed. Oxford University Press, 2023, Introduction
13. Gueham, Farid. "Digital Sovereignty: Steps towards a New System of Internet Governance." Fondapol, February 2017.
14. Celeste, Edoardo. "Digital Sovereignty in the EU: Challenges and Future Perspectives." In *Data Protection Beyond Borders*, edited by Federico Fabbrini, Edoardo Celeste and John Quinn. Hart, 2021.
15. Chander, A. "How Law Made Silicon Valley." *Emory Law Journal*, vol. 63, 2013.
16. Roberts, H., Hine, and Floridi, L. "Digital Sovereignty, Digital Expansionism, and the Prospects for Global AI Governance." In *Quo Vadis, Sovereignty?* edited by M. Timoteo, B. Verri and R. Nanni. *Philosophical Studies Series*, vol. 154. Springer Nature Switzerland, 2023.
17. Buza, Maria, and Sherif Taha. "DPA Digital Digest: Algeria [2025 Edition]: A Close-Up of Algeria's Regulatory Approach to Data Governance, Content Moderation, Competition, Artificial Intelligence, and More." 16 April 2025.
18. Schmitt, Michael N. "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." *Exeter Centre for International Law Working Paper Series*, no. 3, 2018.
19. M. Fitzgerald, N. Kruschwitz, D. Bonnet and M. Welch, "Embracing Digital Technology: A New Strategic Imperative," *MIT Sloan Management Review*, vol. 55 (2014), pp. 1–12.
20. D.-Y. Liu, S.-W. Chen and T.-C. Chou, "Resource Fit in Digital Transformation," *Management Decision*, vol. 49, no. 10 (2011),
21. Singh and Hess, T. "How Chief Digital Officers Promote the Digital Transformation of Their Companies." *MIS Quarterly Executive*, 2017.
22. Rogers, D. *The Digital Transformation Playbook: Rethink Your Business for the Digital Age*. New York: Columbia University Press, 2016.
23. Warner, K. S. R., and Wäger, M. "Building Dynamic Capabilities for Digital Transformation: An Ongoing Process of Strategic Renewal." *Long Range Planning*, vol. 52, no. 3, 2019.
24. Vial, G. "Understanding Digital Transformation: A Review and a Research Agenda." *Journal of Strategic Information Systems*, vol. 28, 2019.