The Legal Framework for Digital Sovereignty in Algeria: An Analytical Study of New Legislative Texts

(Law 25-11, Decree 25-320) and other Relevant Legislation

الإطار القانوني للسيادة الرقمية في الجزائر: دراسة تحليلية للنصوص التشريعية الجديدة

(القانون 25-11، والمرسوم 25-320) وبقية التشريعات ذات الصلة

Rachid Attou♦
Faculty of Law, Tissemsilt University /Algeria
Laboratory for the Development of Economic Legislation
attou.rachid@univ-tissemsilt.dz

Date of submission: 20/03/2026 Date of acceptance: 06/06/2026
Date of publication: 30/06/2026

Abstract:

This study examines the legal framework of digital sovereignty in Algeria through an analysis of recent legislative instruments—namely Law No. 25-11 amending Law No. 18-07 and Presidential Decree No. 25-320—alongside relevant prior legislation, with the aim of assessing their role in strengthening digital sovereignty and identifying existing gaps and challenges. The study concludes that Algeria has achieved notable legislative progress in this field, particularly through amendments to laws governing personal data protection, criminal procedure, and the Penal Code, in addition to the establishment of data governance, reflecting a shift toward the effective and practical protection of data. Nevertheless, certain shortcomings and challenges persist and require further attention.

Keywords: Digital sovereignty, data governance, Law No. 25-11, Presidential Decree No. 25-320, digital evidence, cybercrime.

الملخص:

تتناول هذه الدراسة الإطار القانوني للسيادة الرقمية في الجزائر من خلال تحليل التشريعات الجديدة (القانون 25-11المعدل للقانون 18-07، والمرسوم 25- 320)، والتشريعات السابقة ذات الصلة، بهدف تقييم دورها في تعزيز هذه السيادة والكشف عن الثغرات والتحديات القائمة.

♦ Author Sent

وتخلص إلى أن الجزائر حققت تقدماً تشريعياً ملحوظاً في هذا الباب، خاصة عبر تعديل قوانين حماية المعطيات الشخصية، الإجراءات الجزائية، وقانون العقوبات، إلى جانب إقرار حوكمة البيانات، بما يعكس انتقالاً نحو حماية عملية للبيانات. رغم ذلك، لا تزال بعض النقائص والتحديات قائمة، وتحتاج إلى معالجة.

الكلمات المفتاحية: السّيادة الرّقمية، حوكمة البيانات، القانون 25-11، المرسوم 25-320، الإثبات الرّقمي، الجرائم السّيبرانية.

Introduction

In an era of accelerating digital transformation, where boundaries between physical and virtual spaces are increasingly blurred, the concept of "digital sovereignty" has emerged as one of the most prominent challenges facing the nation-state. Digital sovereignty is no longer merely a technical option but has become an expression of the state's ability to control its data, protect its critical infrastructure, ensure its citizens' security in cyberspace, and formulate its own digital model away from external dictates and technological hegemony.

The legal system constitutes the fundamental pillar for achieving this sovereignty. In this context, Algeria witnessed an active legislative movement during the 2025-2026 period, marked by the issuance of a package of new legal and regulatory texts, most notably Law 25-11 amending and supplementing Law 18-07 on the protection of individuals with regard to the processing of personal data, Law 25-14 on Criminal Procedure which brought about a breakthrough in digital evidence, Presidential Decree 25-320 on the national data governance system, in addition to Law 24-06 amending the Penal Code which preceded them slightly, and the proposed law on regulating major digital platforms.

This study stems from **a main problematic**: How do the new legislations for 2025-2026 (Law 25-11 amending and supplementing Law 18-07, and Decree 25-320) integrate with the rest of the relevant legislation to form an integrated legal framework for digital sovereignty in Algeria, and what legal challenges still exist in the face of continuous technological development?

The following sub-questions branch out from this problematic:

1.How has the concept of digital sovereignty evolved in legal thought, and what are the stages of development of digital legislation in Algeria?

2.What are the most prominent amendments introduced by the new legislative texts in the areas of personal data protection, digital evidence, cybercrimes, and regulation of digital platforms?

3.How did Presidential Decree 25-320 establish an integrated national system for data governance?

4.What are the legal gaps that still hinder the achievement of integrated digital sovereignty?

This study gains its **importance** from several considerations, as it coincides with the issuance of very new legal texts (Law 25-11 amending and supplementing Law 18-07, and Decree 25-320) and its comprehensive and comparative analysis with the rest of the relevant legislation issued before that, and the results it reached. In addition to its connection with the Sovereignty of digital autonomy, which has become a top national priority.

The study relies on **the descriptive analytical approach** to analyze legislative and regulatory texts and extract their contents and effects, in addition to the comparative approach to compare some provisions with international models, such as the European General Data Protection Regulation (GDPR), and the European Artificial Intelligence Act (AI Act).

The study is **structured into three main sections**, followed by a conclusion presenting the most prominent findings and recommendations:

- **First topic:** The Conceptual and Referential Framework for Digital Sovereignty
- **Second topic:** New Legislation Framing Digital Sovereignty
- **Third topic:** Legal Gaps in the Digital Sovereignty System
- **Conclusion / Recommendations.**

THE FIRST TOPIC: The Conceptual and Referential Framework for Digital Sovereignty

The conceptual and referential grounding of digital sovereignty constitutes the essential entry point for understanding the nature of this modern concept and its multiple dimensions. The study in this section is divided into three main sub-sections, addressing the evolution of the concept in legal thought (First requirement), the constitutional framework for digital rights in Algeria (Second requirement), and the stages of development of digital and institutional legislation (Third requirement).

First requirement: The Evolution of the Concept of Digital Sovereignty in Legal Thought

The concept of digital sovereignty has witnessed remarkable development in recent decades, moving from being merely a technical capacity to protect networks to a comprehensive concept combining technical, legal, economic, and cultural dimensions. Understanding this concept requires tracing its intellectual roots (First section), its evolution (Second section), and analyzing its essential elements and distinctive characteristics (Third section).

First section: Conceptual Foundation of Digital Sovereignty

The concept of digital sovereignty is an extension of the traditional concept of national sovereignty in the digital space. If national sovereignty means the state's ability to exercise its exclusive powers over its territory and population, then digital sovereignty means the state's ability to exercise these powers in cyberspace, through controlling its data, protecting its digital infrastructure, ensuring its citizens' security in the virtual space[1]. Thus, it becomes clear that the concept of sovereignty has shifted from traditional territorial control to control over data and digital infrastructure. Digital identity management, protection of electronic reputation, and regulation of data flows have become essential elements in the exercise of modern sovereignty.

[1] - Belhadj, Khaldia., & Feraoun, Mouhamed. Digital sovereignty. Journal of Research in Law and Political Science, 11(1). 2025. p. 463.

Second section: Development of the Concept at the International Level

The concept of digital sovereignty has witnessed remarkable development over the past two decades, moving during this period from being merely a technical capacity to protect networks to a comprehensive concept combining technical, legal, economic, and cultural dimensions. The concept faces structural challenges represented by the cross-border nature of cyberspace, the difficulty of applying national law to global actors, and the development of cyber threats[1]. This reality has led states to face a new form of hegemony exercised by technology giants (GAFAM), necessitating serious efforts to achieve independence and liberation from their hegemony, investing heavily in developing digital capabilities, and working at the international level to establish common principles to ensure a secure digital future.[2]

Third section: Specificity of the Concept in the Algerian Context

In the Algerian context, the concept of digital sovereignty gradually crystallized through successive legislative stages, starting from the security approach in the founding phase, reaching the comprehensive rights-based approach in the reinforcement and alignment phase. The specificity of the concept in Algeria is evident in its close connection with building a modern state and achieving sustainable development, and in being a fundamental axis in major national strategies such as the "Algeria Digital 2030"[3] vision and the National Strategy for Information Systems Security 2025-2029.[4]

Second requirement: The Constitutional Framework for Digital Rights

The constitution represents the supreme reference upon which all legislation related to digital rights is based, as it enshrines the fundamental principles and general guarantees for protecting private

[1] - Hamil, Moustapha. Digital sovereignty: Challenges and structural solutions. Digitization Journal for Media and Communication Studies, 2(3). 2022. p. 54.
[2] - Egger, Amina. Digital sovereignty in a globalized world: Challenges and stakes. Journal of Legal and Political Studies, 10(2). 2024. p. 75.
[3] - National Strategy for Digital Transformation in Algeria - For a Digital Algeria 2030, Presidency of the Republic, High Commission for Digitalization, 2024.
[4] - National Strategy for Information Security 2025-2029, People's Democratic Republic of Algeria, Commission for Digitization, 2026.

life and personal data. This sub-section deals with the analysis of relevant constitutional texts, foremost among them Article 47 of the 2020 Constitution (First section), explaining their impact on subsequent organic legislation (Second section), and the limits of their protection (Third section).

First section: Article 47 of the Constitution – An Analytical Reading

The constitutional amendment of 2020[1] constituted a major turning point in the path of legal protection of digital rights in Algeria. This amendment laid solid constitutional foundations for the protection of private life and personal data, making them a guaranteed constitutional right.

Article 47 of the Constitution stipulates: "The private life of the citizen, his honor, and the secrecy of his private correspondence and communications, in any form whatsoever, are inviolable. These rights may not be infringed except by a reasoned order from the judicial authority, within the limits prescribed by law. The state guarantees the protection of persons when processing personal data."

This constitutional text represents three basic guarantees:

- Protection of private life, honor, and correspondence in all its forms.

- Restricting the permissibility of infringing upon these rights to a reasoned judicial order.

- Obliging the state to guarantee the protection of persons when processing their personal data.

However, constitutional protection of the right to privacy is not limited to Article 47 but extends to include a set of complementary texts that together form an integrated constitutional system. Article 48 complements the spatial dimension of privacy by protecting the inviolability of the home and requiring a written judicial order for searches. Article 54 guarantees the right of reply to what is published in the media, which constitutes a safeguard for the protection of reputation and privacy. Article 57 exempts court sessions from publicity to preserve public order or morals, which

[1] - Constitutional Amendment of 2020, issued by Presidential Decree No. 442/20 and signed on 15 Jumada al-Ula 1442 corresponding to 30 December 2020 relating to the constitutional amendment, Official Gazette of the People's Democratic Republic of Algeria, No. 82, dated 30 December 2020, p. 13.

includes protecting the privacy of parties in sensitive cases. Article 62 gains special importance in light of the digitization of the health sector, as it imposes the protection of medical privacy. Article 65 can also form a basis for protecting personal data as a form of intangible property. The system is completed by Article 74, which prohibits discrimination, which applies to automated data processing that may lead to algorithmic discrimination against vulnerable groups.[1]

Second section: Impact of the Constitutional Amendment on Organic Legislation

The constitutional debate on the protection of citizens in the digital space paved the way for a series of subsequent organic legislations. Article 47 constituted a supreme constitutional reference upon which the following laws were based:

- Law 18-07 on the protection of individuals with regard to the processing of personal data.
- Law 25-11 amending and supplementing it.
- Law 25-14 on Criminal Procedure concerning digital evidence.
- Law 24-06 amending the Penal Code in criminalizing attacks on private life in the digital space.

Third section: Limits of Constitutional Protection in the Face of Digital Challenges

Despite the importance of the constitutional text, some issues regarding the constitutional protection of personal data remain, most notably:

- **The general nature of the texts:** The constitutional text lacks details that keep pace with the complexities of the digital space.
- **The balance between security and freedoms:** The perennial issue of defining the limits of intervention to protect national security without infringing on rights and freedoms.

[1] - Berkani, Fadhila. Protection of the right to privacy in Algerian legislation. Algerian Journal of Law and Political Science, 1(10). 2022. p. 988.

•**Protection from non-traditional threats:** such as algorithmic discrimination and deepfakes, threats that were not present when the constitutional text was drafted.

Third requirement: Stages of Development of Digital Legislation in Algeria

Digital legislation in Algeria has passed through successive stages that reflected the evolution of the legal perspective on cyberspace, from a narrow security approach to a comprehensive rights-based vision. These stages are divided into three main eras: the founding phase (2009-2020) which established the initial rules for dealing with cybercrime (First section), the construction phase (2018-2024) which witnessed the issuance of the Personal Data Protection Law (Second section), and the reinforcement and alignment phase (2025-2026) which is the focus of this study (Third section).

First section: The Founding Phase (2009-2020)

This phase was characterized by the issuance of the first foundational texts that established the basic rules for dealing with the digital space, most notably:

•Law 09-04 on the prevention and combating of crimes related to information and communication technologies.[1]

•Presidential Decree 20-05 on the national information systems security system.[2]

The perspective during this phase was primarily security/technical, focusing on protecting systems from intrusions and cybercrimes, with an emphasis on the punitive aspect over the preventive rights-based aspect.

Second section: The Construction Phase (2018-2024)

This phase witnessed a qualitative shift with the issuance of **Law No. 18-07 of June 10, 2018**, on the protection of individuals with regard to the processing of personal data.[3] This law enshrined a

[1] - Law No. 09-04 of August 5, 2009, containing the special rules for the prevention and combating of crimes related to information and communication technologies. Official Gazette of the People's Democratic Republic of Algeria, No. 47, dated August 16, 2009. P. 5.

[2] - Presidential Decree No. 20-05 dated January 20, 2020, relating to the establishment of a national system for the security of information systems, Official Gazette, No. 04, dated January 26, 2020, p. 5.

[3] - Law 18-07 of June 10, 2018, relating to the protection of natural persons in the field of processing of personal data, Official Gazette of the People's Democratic Republic of Algeria, No. 34, dated June 10, 2018, p. 11.

set of basic principles inspired by international standards: the principle of lawfulness and transparency, purpose specification, data minimization, explicit consent, accuracy, security and confidentiality of processing, and accountability.[1]

However, the most prominent feature of this phase was the transition from theoretical protection to institutional protection, through the establishment of the **National Authority for the Protection of Personal Data** as an independent regulatory body.[2] The law entrusted this authority with broad powers including monitoring the lawfulness of data processing, conducting investigations and inspections, imposing administrative sanctions, and providing opinions on draft related texts.

This phase was also marked by the beginning of awareness of the importance of institutional integration, as the implementation of Law 18-07 coincided with strengthening the role of existing bodies (such as the National Council for Information Systems Security and the Information Systems Security Agency established by Decree 20-05), and paving the way for the creation of new structures such as the High Commission for Digitization (2023) and the National Higher School of Artificial Intelligence (2021). This emerging integration formed the nucleus of the integrated digital sovereignty system that later crystallized in the reinforcement and alignment phase (2025-2026).

Thus, it can be said that this law represented a legislative break with the previous phase, as it moved the Algerian legislator from a security/repressive approach to a comprehensive rights-based approach placing the individual and their right to digital privacy at the heart of concern.

Third section: The Reinforcement and Alignment Phase (2025-2026)

This phase represents the focus of the study and is characterized by the issuance of an integrated package of new legislative texts:

[1] - Boufelagha, Wahiba. (2018). Protection of personal data in Algeria in light of Law No. 18-07. Journal of Legal and Political Studies, 2(3). p. 119.
[2] - Berkani, 2022, p. 996.

- Law 25-11 amending and supplementing Law 18-07.[1]
- Law 25-14 on Criminal Procedure.[2]
- Law 24-06 amending the Penal Code.[3]
- Presidential Decree 25-320 on the national data governance system.[4]
- Proposed law on regulating major digital platforms.[5]

These texts reflect a qualitative shift towards comprehensive and integrated protection of data and personal information, while strengthening implementation, monitoring, and sanction mechanisms.

THE SECOND TOPIC: Key Developments in New Legislation Framing Digital Sovereignty

The period 2025-2026 witnessed an active legislative movement in Algeria represented by the issuance of a package of laws and decrees that enhance digital sovereignty and keep pace with accelerating technological developments. This section analyzes these key texts, focusing on the qualitative additions they introduced in the areas of personal data protection (First requirement), digital evidence (Second requirement), cybercrimes (Third requirement), platform regulation (Fourth Sub-section), and data governance (Fifth requirement).

First requirement: Enhancing Personal Data Protection – Law 25-11

Law 25-11 (July 24, 2025), amending and supplementing Law 18-07, represents a qualitative shift in the personal data protection system in Algeria, as it came to keep pace with technological developments and fill the gaps revealed by the practical application

---

[1] - Law No. 25-11 of July 24, 2025, amending and supplementing Law No. 18-07 of 10 June 2018 relating to the protection of natural persons in the field of processing of personal data, Official Gazette, No. 48, dated July 24, 2025, p. 14.

[2] - Law No. 25-14 of August 3, 2025, containing the Code of Criminal Procedure. Official Gazette of the People's Democratic Republic of Algeria, No. 54, dated August 13, 2025, p. 7.

[3] - Law No. 24-06 of April 28, 2024, amending and supplementing Ordinance No. 66-156 of June 8, 1966, containing the Penal Code. Official Gazette of the People's Democratic Republic of Algeria, dated April 30, 2024. P. 4.

[4] - Presidential Decree No. 25-320 of December 30, 2025, establishing a national data governance system. Official Gazette of the People's Democratic Republic of Algeria, No. 87, dated December 30, 2025. p. 4.

[5] - National People's Assembly. (Parliamentary Session 2024-2025). Proposed law on regulating major digital platforms. Parliamentary document.

of the original law. This amendment enshrines a transition from theoretical to practical protection (First section), through stricter regulatory and punitive mechanisms responding to new digital challenges (Second section), followed by its evaluation (Third section).

First section: Fundamental Principles of Law 18-07

This phase witnessed a qualitative shift with the issuance of **Law No. 18-07 of June 10, 2018** on the protection of individuals with regard to the processing of personal data.[1] This law represented a legislative break with the previous phase, moving the Algerian legislator from a security/repressive approach to a comprehensive rights-based approach placing the individual and their right to digital privacy at the core of concern. The law included several fundamental principles: the principle of lawfulness and transparency, the principle of purpose specification, the principle of data minimization, the principle of explicit consent, the principle of security and confidentiality of processing, and the principle of responsibility and accountability.

This phase was also marked by the beginning of awareness of the importance of institutional integration, as the implementation of Law 18-07 coincided with strengthening the role of existing bodies (such as the National Council for Information Systems Security and the Information Systems Security Agency established by Decree 20-05), and paving the way for the creation of new structures such as the High Commission for Digitization (2023) and the National Higher School of Artificial Intelligence (2021). This emerging integration formed the nucleus of the integrated digital sovereignty system that later crystallized in the reinforcement and alignment phase (2025-2026).

Second section: Substantive Amendments in Law 25-11

Law 25-11 of July 24, 2025[2], amending and supplementing Law 18-07, reflects the Algerian legislator's keenness to keep pace with accelerating technological developments and fill the gaps

[1] - Law No. 18-07**,** Official Gazette, Issue 34. (June 10, 2018).
[2] - Law No**.** 25-11, Official Gazette, Issue 48. (July 24, 2025).

revealed by the practical application of the original law. The substantive amendments can be classified into four main axes:

First : Creation of the position of "Data Protection Delegate (DPO)"(Article 41 bis): Mandating public and private institutions and administrations to appoint a specialized data protection delegate, who is notified to the national authority.

Second : Mandatory Data Protection Impact Assessment (DPIA) (Article 35 bis): Requiring a prior study to assess risks before processing high-risk data (biometric, health, video surveillance, data of children and employees).

Third : Precise organization of records: Introducing two mandatory registers (Article 41 bis\ 2, Article 41 bis\ 3):: a "register of processing activities" and an "automated register for processing personal data," in addition to a register of violations, placed at the disposal of the national authority.

Fourth: Strengthening controls on data transfers abroad: Transfers outside Algeria are now subject to prior authorization from the National Data Protection Authority, along with an assessment of the level of protection in the receiving country.

Fifth: Enhancing the powers of the National Data Protection Authority: (Article 27 bis) stipulates the establishment of regional hubs within the National Data Protection Authority to oversee and audit public and private entities that process personal data.

Third section: Evaluating the Effectiveness of the Legal Framework for Data Protection

The new amendment reflects a transition from theoretical protection to practical protection, as compliance has become a strict legal obligation covering all stages of data processing, from planning (impact assessment) to implementation (protection delegate and records) to monitoring (strengthening the authority's powers) and punishment (toughening sanctions).

However, actual effectiveness remains contingent on the extent of the national authority's readiness to exercise its regulatory functions,

and the availability of qualified human resources to follow up on the implementation of these new obligations.[1]

Second requirement: Criminal Procedure Law and Digital Evidence (Law 25-14)

Law 25-14 (August 3, 2025), containing the new Criminal Procedure Law, represented a break with the previous law issued in 1966 and a response to the accelerating technological developments that necessitated a reconsideration of evidence and investigation mechanisms in the digital age. This sub-section focuses on the most prominent developments introduced by the law in the area of recognizing digital evidence (First section), expanding digital investigation powers (Second section), while strengthening defendants' guarantees in the digital environment (Third section).

First section: Explicit Recognition of Digital Evidence

Law No. 25-14 of August 3, 2025[2], containing the new Criminal Procedure Law, was issued, constituting a break with the previous law issued in 1966. Article 349 stipulates that crimes can be proven by any means of proof, including electronic means, unless the law provides otherwise, leaving discretionary power to the judge according to his personal conviction. This text represents the cornerstone for the flexibility of proof in the digital age.

Second section: Expanding Digital Investigation Powers

The new law granted the investigating judge expanded powers in the field of digital investigation:

- Seizure of digital assets throughout the investigation period (Article 198).

- Requesting assistance from all employees and officers working in public administrations and services.

- The possibility of notification and information via electronic address or telephone number, with the explicit consent of the accused (Article 175).

[1] - Ben Berghout, Lila. Cybersecurity and protection of digital data privacy in Algeria in the era of digital transformation and artificial intelligence. International Journal of Social Communication, 10(1), 2023. 443-457. p. 449.

[2] - Law No. 25-14, Official Gazette. Issue 54, (August 3, 2025).

Third section: Guarantees for the Accused in the Digital Environment

The granting of expanded investigation powers in the new law (25-14) was accompanied by the establishment of strong procedural guarantees to protect the rights of the defense, namely:

- Warning the accused of his right not to make any statement.
- Informing the accused of his right to choose a lawyer.
- The right of the accused's lawyer to submit observations while his client is being heard.

This law represents an important step towards modernizing the judicial system; however, the biggest challenge remains the speed of legislative updating compared to technological innovation, and the need to issue complementary regulatory texts to activate the provisions of digital evidence.

Third requirement: Penal Code and Cybercrimes (Law 24-06)

Law 24-06, amending and supplementing the Penal Code[1], strengthened the legal framework for combating cybercrime by toughening penalties and expanding the scope of criminalization to include new acts. This sub-section addresses the most important amendments introduced by the law, foremost among them the protection of the right to image in the digital space (First section), toughening penalties for cyberattacks targeting critical infrastructure (Second section), and introducing alternative penalties to imprisonment (Third section).

First section: Protection of the Right to Image in the Digital Space

Article 333 bis 4 of Law 24-06 criminalizes capturing or obtaining photos, videos, electronic messages, or any private information of any person by any means, and broadcasting, publishing, or threatening to do so without the permission or consent of the owner, with aggravated penalties of imprisonment from one to five years and a fine of 100,000 to 500,000 Algerian dinars.

This text represents a qualitative expansion of criminal protection, as the legislator moved from limiting it to private places (home,

[1] - Law No. 24-06, Official Gazette. Issue 30. (April 28, 2024).

bedrooms) to anywhere, when it comes to capturing or publishing information and images that are private in nature. The article also includes photos and videos that may be taken in public spaces but are circulated with the intent to harm the person or defame them. This expansion embodies a legislative response to the reality of the digital age, where privacy violations are no longer confined to physical space but have become linked to the nature of the content (private) regardless of where it was captured.

Second section: Toughening Penalties for Cyberattacks

Law 24-06, amending and supplementing the Penal Code, significantly toughened penalties for acts related to cyberattacks targeting national defense systems or the state's critical infrastructure, primarily the energy, communications, and finance sectors.

This approach reflects a legislative response to the growing cyber threats targeting national sovereignty, as electronic attacks are now classified among the most serious threats facing states in the twenty-first century, especially those targeting critical infrastructure such as electricity grids, nuclear plants, electronic payment systems, and strategic communications networks.

This tightening integrates with the role of the National Council for Information Systems Security and the Information Systems Security Agency (ANSSI) in protecting critical infrastructure, and within the framework of the National Strategy for Information Systems Security 2025-2029, which places the protection of these sectors among its top priorities.

Third section: Introducing Alternative Penalties in Cybercrimes

Law 24-06 introduced alternative penalties to imprisonment, such as community service and electronic monitoring (electronic bracelet), within the framework of modernizing penal policy and focusing on rehabilitation rather than punishment. This introduction represents a qualitative shift in the philosophy of criminalization and punishment in Algeria, moving the legislator from the logic of custodial sentences as the sole option to a more flexible and humane logic, allowing the judge broad discretionary power to choose the penalty most appropriate to the defendant's personality and the circumstances of the crime.

These amendments reflect a shift from the general preventive framework to a more comprehensive and specialized criminal protection. They respond to new digital challenges and enhance legal deterrence against cybercrimes. The balance between toughening penalties for serious crimes (such as those targeting critical infrastructure) and introducing alternatives for less serious offenses (such as community service in cases of unintentional electronic publication) represents an integrated approach combining deterrence and rehabilitation. This approach is likely to alleviate pressure on prison institutions and rehabilitate digital offenders who are not high-risk to become productive members of society, especially since many cybercrimes are committed by young people who can be reformed without depriving them of their liberty.

Fourth requirement: Proposed Law on Regulating Major Digital Platforms

A proposed law to regulate major digital platforms was introduced during the 2024-2025 parliamentary session, aiming to impose national sovereignty over the digital space and obligate foreign platforms to respect national legislation. This sub-section analyzes the justifications and objectives of the proposal (First Branch), the obligations imposed on platforms (Second section), implementation mechanisms and sanctions (Third section), in light of successful international experiences (Fourth section).

First section: Justifications and Objectives of the Proposal

The proposed law, submitted to the Algerian Parliament to regulate major digital platforms during the 2024-2025 parliamentary session, is based on three main justifications.[1]

- Safeguarding religious and social values in light of the spread of obscene content and hate speech.

- Protecting children and adolescents, as UNESCO studies indicate that over 40% of children in the region are exposed to harmful content online.

- Enhancing digital sovereignty to counter unregulated data collection and the risk of sensitive information leakage.

[1] - National People's Assembly, 2025.

Second section: Obligations Imposed on Foreign Platforms

The proposal imposes several obligations on major foreign platforms (Facebook, TikTok, YouTube, Instagram):

- Opening a local office in Algeria and appointing a legal representative.
- Removing violative content within 24 hours of official notification.
- Storing Algerian users' data within the national territory.
- Submitting semi-annual reports to the National Authority for the Digital Space.

Third section: Sanctions and Implementation Mechanisms

Sanctions range from escalating financial fines, restrictive measures, or service blocking, with the possibility of criminal prosecution when appropriate. To ensure implementation, the proposal establishes the **National Authority for Regulating the Digital Space** as an independent body attached to the Presidency of the Republic, tasked with monitoring implementation, issuing regulations, imposing escalating financial fines, and potentially blocking services or initiating criminal prosecution in serious cases.[1]

These obligations are based on successful international experiences. Turkey (2020) obligated platforms to appoint a local representative and imposed fines of up to 10 million lira. India (2021) forced platforms to appoint local employees to handle complaints. Germany (2018) applied the "NetzDG" law requiring the removal of criminal content within 24 hours[2].

Thus, it can be said that this proposal represents an advanced legislative trend towards achieving digital sovereignty and aligns with international trends in this field.

[1] - National People's Assembly, 2025.

[2] - Al-Quds Al-Arabi Newspaper. (2025). A proposed law in the Algerian parliament to restrict content on social media platforms such as Facebook, TikTok, and YouTube quickly sparked concerns. https://www.alquds.co.uk/%D8%B3%D8%B1%D8%B9%D8%A7%D9%86
Viewed on: 27/10/2025.

Fifth requirement: Presidential Decree 25-320 and the National Data Governance System

Presidential Decree No. 25-320 (December 30, 2025)[1] represents a qualitative shift in the concept of data governance in Algeria, as it establishes an integrated national system aimed at organizing, managing, and exchanging data between public institutions. This sub-section presents the most important components of this system, starting from considering data as a "strategic asset" (First Branch), moving through the basic components such as the data classification reference and the national interoperability system (Second section), and reaching the distribution of competencies among national bodies (Third section), and finally addressing integration with Law 25-11 regarding data transfer (Fourth section).

First section: Considering Data as a "Strategic Asset"

Presidential Decree No. 25-320 of December 30, 2025[2] represents a qualitative shift in the concept of data governance in Algeria. The preamble of the decree states that data has become "a strategic resource no less important than infrastructure and human capital," and that the goal is to transition from "traditional governance based on paper and fragmented digitization to comprehensive digital governance centered on data". The system aims to "consolidate state sovereignty over data of national interest" and "ensure organized, secure, transparent, and effective management of public data." This approach redefines the relationship between the state and data, placing it among strategic national assets.

Second section: Basic Components of the System

The decree, consisting of 20 articles spread over 4 chapters, includes three basic components: the **data classification reference** (Article 6) which defines the standards and procedures for determining data sensitivity levels and the types of protection to be applied to each category; the **data source indexing reference** (Article 7) which defines the standards for compiling and defining data sources through a unified model to reduce data multiplicity and

[1] - Presidential Decree No. 25-320 relating to the national data governance system. Official Gazette of The Algerian Republic, Issue 87. (2025, December 30).
[2] - Presidential Decree No. 25-320. Official Gazette. Issue 87, (2025, December 30).

duplication of sources; and the **national interoperability system** (Article 9) which enables the secure, organized, and effective exchange of digital data between public institutions. This system is considered the exclusive framework for data exchange via the secure national network (Article 10).

Third section: Distribution of Competencies Among National Bodies

The decree assigned specific tasks to national bodies: the **High Commission for Digitization** (Articles 8, 11, 17) manages the national system, prepares the references, and establishes the secure infrastructure; the **National Council for Information Systems Security** (Article 14) is responsible for deciding on functional matters of the system and ensuring functional safety; the **Information Systems Security Agency** (Article 16) decides on the classification of data security levels; and the **National Authority for the Protection of Personal Data** (Article 15) monitors the conformity of personal data with applicable legislation and regulations. The system was officially put into service on February 9, 2026, under the supervision of the Prime Minister.

Fourth section: Integration with Law 25-11 on Data Transfer

Decree 25-320 integrates with Law 25-11 in regulating data transfer. The latter (Article 44) requires prior authorization from the National Authority for the Protection of Personal Data to transfer personal data abroad, permitting it only if the destination country provides an adequate level of protection. In contrast, Decree 25-320 establishes the national interoperability system as the exclusive framework for data exchange between public institutions, limiting dependence on foreign infrastructure. This integration forms a dual framework for data protection: legal through prior authorization, and technical through the secure national infrastructure. However, the fundamental issue remains the absence of clear implementing mechanisms, such as an official list of countries with adequate protection, which will be analyzed in Section Three.

THE THIRD TOPIC: Legal Gaps in the Digital Sovereignty System

Despite the significant legislative progress Algeria has witnessed in recent years, represented by the issuance of Law 18-07 and its amendment by Law 25-11, Law 25-14 on Criminal Procedure, Presidential Decree 25-320 on data governance, and Executive Decree 26-97 on equipment certification, legal and regulatory gaps still hinder the construction of integrated digital sovereignty. From this standpoint, this section analyzes the most prominent of these gaps, distributed across three main levels: gaps at the level of legislative content (First requirement), gaps at the level of implementation and oversight mechanisms (Second requirement), and gaps at the level of supplementary regulatory texts (Third requirement), providing a critical reading that contributes to identifying priorities for future legislative reform.

First requirement: Legal Gaps at the Level of Legislative Content

Gaps at the level of legislative content relate to areas that the Algerian legislator has not yet addressed, or has addressed insufficiently, despite their critical importance in achieving integrated digital sovereignty. This sub-section focuses on analyzing three main gaps: the gap in keeping legislation pace with accelerating technological developments (First section), the gap in digital ethics and human rights (Second section), and the gap in legal protection for vulnerable groups (Third section).

First section: The Gap in Keeping Legislation Pace with Accelerating Technological Developments

Generative AI and the Internet of Things (IoT) raise unprecedented legal issues not addressed by current texts, even after the amendment of Law 18-07 by Law 25-11. The most prominent of these issues include determining legal liability for content generated by AI systems, protecting intellectual property rights for creative outputs, and confronting the phenomenon of deepfakes.

Many researchers attribute this to the absence of mechanisms for periodic evaluation and review of legislation, especially since the Algerian legislator adopts a "reactive approach" rather than a "proactive legislative approach," intervening after the emergence of criminal phenomena instead of anticipating digital risks before they

evolve into widespread criminal activities. Additionally, there are no legal or regulatory texts requiring systematic periodic evaluation of the effectiveness of digital legislation and its updating, compared to the clear trend observed in European legislation towards incorporating evaluation and periodic review mechanisms every 3-5 years. Article 97 of the General Data Protection Regulation (GDPR) requires the European Commission to submit an evaluation report every four years[1]. Chapter Thirteen of the European Artificial Intelligence Act (AI Act) also provides for periodic reviews.[2]

In light of this gap, it is possible to propose the creation of a national mechanism for the periodic evaluation of digital legislation every two or three years, and the establishment of a permanent advisory body to monitor technological developments and propose amendments.

Second section: The Gap in Digital Ethics and Human Rights

With the increasing reliance on artificial intelligence in making critical decisions such as hiring, granting loans, and medical diagnosis, there is an urgent need for legal texts prohibiting algorithmic discrimination and guaranteeing the citizen's right to an explanation of automated decisions affecting them. Algerian legislation lacks any text enshrining the principle of algorithmic transparency. Although Article 74 of the Constitution prohibits discrimination based on gender, origin, or opinion, and although Algerian legislation has provided for the principle of transparency in specific areas, such as public procurement (Law No. 23-12 established mechanisms to enhance transparency via electronic portals), these texts do not extend to cover "algorithmic transparency" or the right to an explanation of automated decisions, nor do they cover discrimination resulting from automated systems.

Third section: The Gap in Legal Protection for Vulnerable Groups

Despite the significant development witnessed in 2025 with the issance of Executive Decree No. 25-309 of November 16, 2025,

[1] - European Union Agency for Fundamental Rights, 2024. the General Data Protection Regulation (GDPR).
[2] - Hannes Snellman Digital Horizon. (2024). Chapter XIII of the AI Act: Final Provisions. https://digitalhorizon.hannessnellman.com/ai-strategy/ai-regulation-air/ Viewed on: 13/12/2025

which establishes a "national cyber vigilance cell" attached to the National Authority for the Protection and Promotion of Childhood (ONPPE), this mechanism – given the increasing risks of the digital space – remains recent and limited to children without explicitly extending to people with special needs or other marginalized groups.[1] UNICEF has affirmed that the COVID-19 pandemic increased children's reliance on the internet, exposing them to multiple risks such as sexual exploitation and cyberbullying.[2]

This situation calls for expanding the scope of protection to include all vulnerable groups and developing more comprehensive oversight mechanisms that respond to the diversity of risks these groups face in the digital space.

Second requirement: Gaps at the Level of Implementation and Oversight Mechanisms

The actual application of legal texts is the true test of their effectiveness, as laws remain dead letter unless coupled with effective implementation and oversight mechanisms that ensure compliance and achieve deterrence. In this context, three main gaps hinder the implementation of digital legislation in Algeria: the gap in the effectiveness of oversight (First section), the gap in institutional coordination (Second section), and the gap in the capacities of competent bodies (Third section).

First section: The Gap in the Effectiveness of Implementation and Oversight Mechanisms of Competent Bodies

Despite Law 25-11 strengthening the powers of the National Authority for the Protection of Personal Data and expanding its regulatory tasks and powers, the published activities of the authority until early 2026 focused on awareness-raising and training aspects, such as organizing study days for data protection delegates and issuing awareness statements for e-commerce traders. Despite the issuance of some decisions published in the Official Gazette, there is no evidence of undertaking concrete regulatory actions (field investigations, sanctions). This absence of actual regulatory action prevents the achievement of the desired legal deterrence, undermines citizens' and institutions' confidence in the viability of legal protection, and weakens the principle of deterrence upon which any

[1] - UNICEF. (2021). Child Online Protection in Algeria: Assessment Report, p. 15.
[2] - UNICEF, 2021, p. 18.

effective punitive system is based.[1] It also raises serious questions about the authority's readiness to exercise its regulatory functions in terms of human and material resources, and the political will to activate actual oversight.

Second section: The Gap in Institutional Coordination Among National Bodies

Numerous bodies are involved in the digital field in Algeria: the High Commission for Digitization established by Presidential Decree 23-314[2], the Information Systems Security Agency (ANSSI) established by Presidential Decree 20-05, the National Authority for the Protection of Personal Data established by Law 18-07, in addition to the National Council for Information Systems Security and the Cyber Surveillance, Monitoring, and Response Center (DZ-CERT). Although some texts contain phrases ordering coordination (such as Article 4 of Decree 25-320), they remain general and non-detailed, merely using vague expressions like "in coordination with the competent authorities," without defining permanent mechanisms for consultation, information exchange, and resolution of potential disputes[3]. This ambiguity creates an overlap in competencies (especially in areas of joint auditing) and leads to duplication of efforts or the assignment of shared responsibilities without a clear definition of roles, necessitating legislative intervention to create a permanent coordination body or binding protocols for cooperation between these bodies.

Third section: The Gap in the Capacities of Regulatory Bodies and Weak Allocated Resources

The competent bodies (the National Authority for the Protection of Personal Data, the Information Systems Security Agency, the High Commission for Digitization) suffer from weak qualified human and material resources necessary to carry out their regulatory functions efficiently. Keeping pace with digital transformation requires specialized competencies in overlapping

[1] - Decisions and opinions of the National Authority for the Protection of Personal Data,2026. https://anpdp.dz/ar/?page_id=1859 . on the date: 05/03/2026.
[2] - Presidential Decree No. 23-314, Establishing a High Commission for Digitalization and defining its missions, organization and operation. Official Gazette of The Algerian Republic, Issue 59. (2023, September 6).
[3] - State of Algerian Software Engineering. Analyse du Référentiel National de Sécurité de l'Information (NISR). 2020.

fields (legal, technical, security), and sufficient financial resources to develop oversight systems and keep up with international developments. The absence of these resources prevents these bodies from effectively fulfilling their oversight and evaluation roles, rendering them incapable of achieving the objectives for which they were established. Moreover, the scarcity of specialized cadres in the digital field at the national level negatively reflects on these bodies' ability to attract the necessary competencies, creating a vicious circle that weakens the entire regulatory system.[1]

Third requirement: Gaps at the Level of Supplementary Regulatory Texts

If framework laws set general principles and basic rules, supplementary regulatory texts (executive decrees, ministerial decisions, implementing circulars) are the main mechanism for activating these laws and transforming their general principles into clear practical procedures. However, the digital legal system in Algeria suffers from gaps at this level, especially in two vital areas: cross-border data transfer (First section) and government cloud services (Second section), which hinders the effective implementation of existing legislation (Third section).

First section: The Gap in Cross-Border Data Transfer

Law 25-11 establishes a strict framework for transferring personal data across borders, requiring prior authorization from the national authority and permitting transfer only if the destination country provides an adequate level of protection. However, this legal mechanism lacks the supplementary regulatory texts specifying its practical implementation, most notably the absence of an officially published list of countries providing an "adequate level of protection" according to Algerian standards, the lack of clear and specific procedures for assessing this level, and the shortage of approved models for binding contractual guarantees between the concerned parties. This ambiguity creates a state of legal uncertainty for companies and institutions dealing with foreign partners, hindering the necessary data flow for economic activity despite efforts made within the framework of the national digital transformation strategy.

[1] - Ben Berghout, 2023, p. 449.

Second section: The Gap in Government Cloud Services

With the launch of the national data governance system under Presidential Decree 25-320, and the creation of the national interoperability system as the exclusive framework for data exchange between public institutions, there is an urgent need for regulatory texts precisely defining the standards and conditions for using cloud services in the government sector. The most prominent gaps include the absence of unified security standards required for data centers and cloud service providers, the lack of clear conditions for contracting with foreign service providers ensuring that national data remains under Algerian legal sovereignty, and agreed-upon mechanisms for periodic auditing and monitoring of compliance with these standards. This regulatory vacuum poses a risk to the security and privacy of government data and hinders the optimal utilization of advanced cloud infrastructures.

Third section: The Gap of Absence of Mechanisms for Periodic Evaluation and Updating of Regulatory Texts

The foresight gap is not limited to the absence of legal texts requiring periodic evaluation of digital legislation but extends to the delay in issuing supplementary regulatory texts (executive decrees, ministerial decisions) essential for activating laws and transforming their general principles into clear practical procedures. The Algerian legislator adopts a "reactive approach," intervening after the emergence of a problem rather than anticipating risks, and implementing texts are delayed for months or even years after laws are issued, creating a regulatory vacuum that disrupts actual protection[1]. A permanent body tasked with monitoring international technological developments and proposing periodic updates to legal and regulatory texts is also absent, making the legislative development process dependent on circumstantial initiatives rather than a sustainable institutional mechanism. In contrast, as previously noted, European legislation requires periodic reviews every 3-5 years, as Article 97 of the General Data Protection Regulation (GDPR) stipulates submitting evaluation reports every four years.[2]

[1] - Ben Berghout, 2023, p. 449- 451.
[2] - European Union Agency for Fundamental Rights, 2024.

Conclusion

This study has reached a set of key findings:

1.**At the level of conceptual development:** The concept of digital sovereignty in Algeria has moved from a narrow security approach to a comprehensive rights-based approach, reinforced by a solid constitutional framework (Article 47 of the 2020 Constitution) and clear national strategies.[1]

2.**At the level of new legislation:** Algeria has achieved significant legislative progress represented by:

- **Law 25-11:** Enhancing personal data protection through the creation of the DPO position, mandatory impact assessment, organization of records, tightening control over cross-border data transfer, and toughening sanctions.

- **Law 25-14:** Updating the Criminal Procedure Law with explicit recognition of digital evidence and expansion of digital investigation powers.

- **Law 24-06:** Toughening penalties for cybercrimes, especially protecting the right to image and criminalizing attacks on critical infrastructure.

- **Decree 25-320:** Establishing an integrated data governance system, considering data as a "strategic asset," and creating the national interoperability system as an exclusive framework for data exchange between public institutions.

- **At the level of legal gaps:** The study revealed major gaps that still exist:

- **Legislative alignment gap:** Limited alignment of current texts with accelerating technological developments (generative AI, IoT).

- **Digital ethics gap:** Absence of texts prohibiting algorithmic discrimination or guaranteeing the citizen's right to an explanation of automated decisions.

- **Legal protection gap for vulnerable groups:** Despite progress in child protection, people with special needs and other marginalized groups remain outside the scope of special protection.

[1] - Algeria Digital 2030, National Strategy 2025-2029.

- **Implementation gaps:** Weak implementation and oversight mechanisms, lack of institutional coordination, and weak capacities of regulatory bodies.

- **Regulatory gaps:** Absence of supplementary regulatory texts, especially the list of countries with adequate protection and standards for government cloud services.

- **Foresight gap:** Absence of mechanisms for periodic evaluation and review of legislation compared to European models.

Recommendations

In light of the previous findings, the study proposes the following recommendations:

- **Complete the legal system** by issuing a comprehensive artificial intelligence law defining the general principles for its use, classifying applications according to the degree of risk, and prohibiting algorithmic discrimination, inspired by the European Artificial Intelligence Act (AI Act) and other successful experiences.

- **Accelerate the issuance of the law regulating major digital platforms (GAFAM)** while strengthening oversight and accountability mechanisms.

- **Issue the supplementary regulatory texts for Law 25-11**, especially those related to the list of countries with adequate protection for cross-border data transfer.

- **Establish a national mechanism for the periodic evaluation of digital legislation** every two or three years, to transition from a "reactive approach" to a "proactive legislative approach."

- **Create a permanent advisory body** to monitor technological developments and propose legislative amendments, comprising academics, judges, and technical experts.

- **Enhance institutional coordination** by establishing a permanent coordination mechanism between the High Commission for Digitization, the Information Systems Security Agency (ANSSI), and the National Authority for the Protection of Personal Data.

- **Activate the role of the National Authority for the Protection of Personal Data** by providing it with adequate human and material resources, launching actual inspection and oversight campaigns, and publishing periodic reports on its activities.

- **Expand the scope of legal protection** to include people with special needs and other marginalized groups in the digital space.

List of Sources and References:

First: Constitutional and Legal Texts

1- Constitutional Amendment of 2020, issued by Presidential Decree No. 442/20 and signed on 15 Jumada al-Ula 1442 corresponding to 30 December 2020 relating to the constitutional amendment, Official Gazette of the People's Democratic Republic of Algeria, No. 82, dated 30 December 2020, p. 13.

2- Law No. 09-04 of August 5, 2009, containing the special rules for the prevention and combating of crimes related to information and communication technologies. Official Gazette of the People's Democratic Republic of Algeria, No. 47, dated August 16, 2009. P. 5.

3- Law 18-07 of June 10, 2018, relating to the protection of natural persons in the field of processing of personal data, Official Gazette of the People's Democratic Republic of Algeria, No. 34, dated June 10, 2018, p. 11.

4- Law No. 24-06 of April 28, 2024, amending and supplementing Ordinance No. 66-156 of June 8, 1966, containing the Penal Code. Official Gazette of the People's Democratic Republic of Algeria, dated April 30, 2024. P. 4.

5- Law No. 25-11 of July 24, 2025, amending and supplementing Law No. 18-07 of 10 June 2018 relating to the protection of natural persons in the field of processing of personal data, Official Gazette, No. 48, dated July 24, 2025, p. 14.

6- Law No. 25-14 of August 3, 2025, containing the Code of Criminal Procedure. Official Gazette of the People's Democratic Republic of Algeria, No. 54, dated August 13, 2025, p. 7.

7- Presidential Decree No. 20-05 dated January 20, 2020, relating to the establishment of a national system for the security of information systems, Official Gazette, No. 04, dated January 26, 2020, p. 5.

8- Presidential Decree No. 23-314 dated September 6, 2023, establishing a High Commission for Digitalization and defining its tasks, organization and operation, Official Gazette, September 6, 2023. No. 59, p. 9.

9- Presidential Decree No. 25-320 of December 30, 2025, establishing a national data governance system. Official Gazette of the People's Democratic Republic of Algeria, No. 87, dated December 30, 2025. p. 4.

Second: Articles and Research Papers

10- Belhadj, Khaldia., & Feraoun, Mouhamed. Digital sovereignty. Journal of Research in Law and Political Science, 11(1), 2025. 461-477. p. 463.

11- Ben Berghout, Lila. Cybersecurity and protection of digital data privacy in Algeria in the era of digital transformation and artificial intelligence. International Journal of Social Communication, 10(1), 2023. 443-457. p. 449.
12- Berkani, Fadhila. Protection of the right to privacy in Algerian legislation. Algerian Journal of Law and Political Science, 1(10), 2022. 983-1009. p. 988.
13- Mohamed Al-Eidani, Yousef Zarrouk. Protection of Personal Data in Algeria in Light of Law No. 18-07 on the Protection of Natural Persons with Regard to the Processing of Personal Data. Journal 'Maalem for Legal and Political Studies' – 2018, Volume 2, Issue 3, Pages 115-130. p. 119.
14- Egger, Amina. Digital sovereignty in a globalized world: Challenges and stakes. Journal of Legal and Political Studies, 10(2), 2024. 71-83. p. 75.
15- Hamil, Moustapha. Digital sovereignty: Challenges and structural solutions. Digitization Journal for Media and Communication Studies, 2(3), 2022. 48-62. p. 54.

Third: Official Documents and Strategies

16- National People's Assembly. (Parliamentary Session 2024-2025). Proposed law on regulating major digital platforms. Parliamentary document.
17- Algeria Digital 2030, National Strategy 2025-2029. People's Democratic Republic of Algeria, Commission for Digitization, 2025.
18- National Strategy for Information Security 2025-2029, People's Democratic Republic of Algeria, Commission for Digitization, 2026.
19- National Authority for the Protection of Personal Data, 2026. People's Democratic Republic of Algeria.
20- State of Algerian Software Engineering. (2020). Analyse du Référentiel National de Sécurité de l'Information (NISR).
21- The National Strategy for Digital Transformation in Algeria - For a Digital Algeria 2030, Presidency of the Republic, High Commission for Digitalization, 2024.

Fourth: Official Data, Statements, and Media Sources

22- European Union Agency for Fundamental Rights, 2024. the General Data Protection Regulation (GDPR).
23- Hannes Snellman Digital Horizon. Chapter XIII of the AI Act: Final Provisions. (2024). https://digitalhorizon.hannessnellman.com/ai-strategy/ai-regulation-air/ Viewed on: 13/12/2025.
24- UNICEF. Child Online Protection in Algeria: Assessment Report, 2021, p. 15.
25- Al-Quds Al-Arabi Newspaper (2025).. A proposed law in the Algerian parliament to restrict content on social media platforms such as Facebook, TikTok, and YouTube quickly sparked concerns. https://www.alquds.co.uk/%D8%B3%D8%B1%D8%B9%D8%A7%D9%86
Viewed on: 27/10/2025.