Data Governance and Data Protection in Algeria: The Rights Dimension and the Sovereignty Dimension – An Analytical Study of Law 25-11 an Decree 25-320

حَوكَمة البيانات وحماية المعطيات في الجزائر: البُعد الحقوقي والبُعد السّيادي - دراسة تحليليّة للقانون 25- 11 والمرسوم 25-320



Rachid Attou[1*]

[1] Faculty of Law, Tissemsilt University - Algeria

Laboratory for the Development of Economic Legislation

attou.rachid@univ-tissemsilt.dz

https://orcid.org/0009-0000-9354-9307

Date of transmission: 27/03/2026 date of acceptance: 25/05/2026 date of publication: 01/06/2026

****

Abstract: This study examines the complementary relationship between Law 25-11, which amends and supplements Law 18-07 concerning the protection of personal data, and Presidential Decree 25-320 concerning the national system for data governance, through the duality of the "rights-based/sovereign" dimensions. Its aim is to reveal how the Algerian legislator addresses data from a dual perspective: protecting it as an individual right (the rights-based dimension) and governing it as a strategic state asset (the sovereign dimension). It concludes that Law 25-11 and Decree 25-320 constitute an integrated framework, reflecting a qualitative shift in Algerian legislation, moving it from a logic of theoretical protection to one of practical governance. However, the study reveals implementation and regulatory challenges hindering the effective application of this integration.

Key Words: Rights-based dimension; sovereign dimension; data governance; personal data protection; Law 25-11; Decree 25-320; legislative integration.

الملخص:

تتناول هذه الدراسة العلاقة التكاملية بين القانون 25-11 المعدل والمتمم للقانون 18-07 المتعلق بحماية المعطيات ذات الطابع الشخصي، والمرسوم الرئاسي 25-320 المتعلق بالمنظومة الوطنية لحوكمة البيانات، من خلال ثنائية الجانبين "الحقوقي/السّيادي"؛ بهدف الكشف عن كيفية تعامل المشرع الجزائري مع البيانات من منظور مزدوج: حمايتها كحق للأفراد (البعد الحقوقي)، وحوكمتها كأصل استراتيجي للدولة (البعد السّيادي). وتخلص إلى أن القانون 25-11 والمرسوم 25-320 يشكلان إطاراً متكاملاً يعكس تحولاً نوعياً في التشريع الجزائري، حيث ينتقل به من منطق الحماية النظرية إلى منطق الحوكمة العملية. غير أن الدراسة تكشف عن تحديات تنفيذية وتنظيمية تعيق التطبيق الفعّال لهذا التكامل.

الكلمات المفتاحية: البُعد الحقوقي، البُعد السِّيادي، حوكمة البيانات، حماية المعطيات الشخصية، القانون 25-11، المرسوم 25-320.

---

* Corresponding Author

Introduction:

In the digital age, data constitutes a strategic axis for states, no less important than natural resources or traditional infrastructure. On one hand, it represents a fundamental right for individuals that must be preserved and protected from any violation or illegal exploitation – this is known as the "rights-based dimension" of data. On the other hand, public data constitutes a national asset that must be governed, organized, and leveraged to serve the national interest – this is known as the "sovereign dimension" of data. Algeria has recognized this duality, enacting during the period 2025-2026 two complementary legislative texts: Law 25-11[1], which amends and supplements Law 18-07 and strengthens the protection of personal data, and Decree 25-320[2], which establishes a national system for data governance.

This study stems from a **central problem**, namely: How does the Algerian legislator address data through the duality of the rights-based and sovereign dimensions in Law 25-11 (amending and supplementing Law 18-07) and Decree 25-320, and what are the limits of integration between these two dimensions in light of existing implementation challenges?

The following sub-questions branch out from this central problem:

1.How is the rights-based dimension manifested in Law 25-11 in terms of protection mechanisms and guarantees provided to individuals?

2.How is the sovereign dimension manifested in Decree 25-320 in terms of organizing data as a strategic state asset?

3.How do the two dimensions, rights-based and sovereign, integrate within the two texts, and what are the challenges hindering this integration?

The importance of this study stems from several considerations: it adopts a new analytical approach to both aspects of the subject; it is a dual approach, addressing both the rights-based and sovereign dimensions, and it studies both laws within a single framework, revealing aspects of integration between them. Additionally, it deals with recently enacted legislative texts (2025-2026), and touches upon the issue of digital sovereignty, which has become a national priority.

Regarding **the methodology** adopted, this study employs the descriptive analytical method to analyze the legislative texts and extract their contents and

---

[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]- Presidential Decree No. 25-320 of December 30, 2025, establishing a national data governance system. Official Gazette, No. 87, dated December 30, 2025. p. 4.

implications, and the comparative method to compare certain provisions with international models, particularly the European General Data Protection Regulation (GDPR).

We will address all of this through three main sections, followed by a conclusion containing the most prominent findings and recommendations, as follows:

- **Section One:** The Rights-Based Dimension – Personal Data Protection in Law 25-11
- **Section Two:** The Sovereign Dimension – Data Governance in Decree 25-320
- **Section Three:** Integration between the Rights-Based and Sovereign Dimensions – Mechanisms of Integration and Limits of Application

THE FIRST TOPIC

The Rights-Based Dimension – Personal Data Protection in Law 25-11

The rights-based dimension of data represents the aspect related to protecting the fundamental rights and freedoms of individuals against the risks arising from the processing of their personal data. This section focuses on analyzing Law 25-11 from the perspective of the guarantees and rights it establishes, through three main requirements: the philosophy of protection upon which it is based (First requirement), the mechanisms for enhancing preventive protection (Second requirement), and the punitive and supervisory guarantees (Third requirement).

First requirement: The Philosophy of Protection in Law 25-11

Law 25-11 is based on an integrated protection philosophy that moves Algerian legislation from a logic of theoretical protection to a logic of practical protection. This requirement analyzes the intellectual foundations upon which the amendment was based, by tracing the transition from theory to application (First section), reviewing the historical background represented by Law 18-07 (Second section), and analyzing the reasons for the amendment related to legislative gaps and technological developments (Third section).

First section: From Theoretical Protection to Practical Protection

Law 25-11 represents a qualitative shift in the philosophy of personal data protection in Algeria, as it came to amend and supplement Law 18-07, moving the legislator from the logic of theoretical protection based on general principles to the logic of practical protection based on tangible implementation

mechanisms. After six years of applying Law 18-07[1], practical application revealed numerous gaps that necessitated legislative intervention to enhance the effectiveness of protection and respond to rapid technological developments.

The fundamental difference between the two laws lies in the nature of the approach adopted. While Law 18-07 was content with defining general principles such as lawfulness, transparency, purpose specification, and explicit consent (Articles 7 to 11)[2], Law 25-11 translated these principles into concrete procedural mechanisms, which will be detailed in the Second Requirement. These mechanisms included the introduction of the Data Protection Officer (DPO) position under Article 41 bis, the mandatory Data Protection Impact Assessment (DPIA) under Article 45 bis 6, the regulation of mandatory registers under Articles 41 bis 2 and 41 bis 3[3], and the strengthening of the National Authority's powers under Article 27 bis[4].

However, this integration between the two laws does not affect the penal provisions contained in Articles 56-67 of Law 18-07[5], which remained in force without amendment, except as may be provided for in other texts such as Law 24-06[6]. Thus, an integrated legal system is formed, combining preventive protection (Law 25-11) through procedural mechanisms, and punitive protection (Law 18-07) through deterrent penal provisions (Articles 54 to 74) [7].

Second section: The Historical Background – Law 18-07 as the Foundation of Protection

Law 18-07, dated June 10, 2018[8], was issued to form the first comprehensive legal framework of its kind in Algeria for the protection of personal data. It established a set of fundamental principles inspired by international standards, foremost among them the principle of lawfulness and transparency, the principle of purpose specification, the principle of data

[1] - Law No.18-07 of June 10, 2018, relating to the protection of natural persons in the field of processing of personal data, Official Gazette, No. 34, dated June 10, 2018, p. 11.
[2] - Ibid, Articles 7 to 11.
[3]- Articles 41 bis 2 and 41 bis of the Law No. 25-11.
[4]- Ibid, Article 27.
[5]- Articles 56-67 of the Law No. 18-07.
[6] - 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, dated April 30, 2024. P. 4.
[7]- Articles 54-74 of the Law No. 18-07 of June 10, 2018, Official Gazette, No. 34.
[8] - Ibid, Law No.18-07.

minimization, the principle of proportionality, the principle of explicit consent, and the principle of the security and confidentiality of processing[1].

Law 18-07 also provided for the establishment of the National Authority for the Protection of Personal Data as an independent supervisory body, tasked with overseeing the implementation of its provisions, granting it broad powers including inspection, investigation, and imposing administrative sanctions[2]. This institutional foundation constituted a qualitative leap in the path of data protection and made Algeria a pioneering country in the region in this field. However, it was not without some shortcomings in the face of the continuous evolution of technology.

Third section: Reasons for the Amendment – Legislative Gaps and Technological Developments

The practical application of Law 18-07 revealed several gaps that necessitated legislative intervention. The most prominent of these gaps include:

- The absence of a permanent position within institutions to follow up on data protection issues.
- The lack of a systematic mechanism for risk assessment before commencing processing operations.
- Insufficient mandatory documentation of processing operations and violations, making supervision and tracking difficult.
- Weak mechanisms for controlling cross-border data transfers.

These gaps formed the basis upon which Law 25-11 later built its implementation mechanisms (DPO, DPIA, register organization). In addition, rapid technological developments, especially in the fields of artificial intelligence, big data, and cloud computing, imposed new challenges that were not present when Law 18-07 was issued, necessitating an update of the legal framework to keep pace with these developments.

Regarding penalties, Law 25-11 kept the provisions of Articles 56-67 of Law 18-07 unamended, merely adding administrative supervisory mechanisms

---

[1] - Mohamed. A, Yousef, Z. (المتعلق بحماية 18-07حماية المعطيات الشخصية في الجزائر على ضوء القانون رقم الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي) (*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 121-125.

[2] - Berkani, F. حماية الحق في الخصوصية في التشريع الجزائري (*Protection of the right to privacy in Algerian legislation*). Algerian Journal of Law and Political Science, 1(10), 2022. p. 996.

that enhance the effectiveness of the existing punitive system through precautionary preventive measures[1].

Second requirement: Mechanisms for Enhancing Preventive Protection in Law 25-11

The added value of Law 25-11 lies in the preventive mechanisms it introduced to enhance the protection of personal data before any violation occurs. This requirement analyzes the most prominent of these mechanisms, represented by the introduction of the Data Protection Officer (DPO) as an internal privacy guardian (First section), the mandatory Data Protection Impact Assessment (DPIA) as a mechanism for assessing risks before they occur (Second section), and the organization of registers as a tool for transparency and control (Third section).

First section: The Data Protection Officer (DPO) as an Internal Privacy Guardian

Law 25-11 introduced, under Article 41 bis[2], the position of "Personal Data Protection Officer" (DPO), acting as an internal "privacy guardian" within institutions. It mandated public and private institutions and administrations to appoint one, informing the National Authority of this appointment. Therefore, this position represents a qualitative shift in the concept of data protection supervision, moving from external supervision (the National Authority) to internal supervision (an officer within the institution). According to Article 41 bis 1, the officer undertakes several basic tasks:

- Informing and advising the controller and users of their obligations.
- Monitoring compliance with this law and internal operating procedures.
- Advising on the Data Protection Impact Assessment (DPIA) and monitoring its implementation in accordance with the provisions of Article 45 bis 6.
- Article 41 bis 1 also considers the officer a "point of contact with the National Authority."

The law requires the officer to possess professional qualities and specialized knowledge in data protection law and practices, ensuring performance quality and effective internal control[3].

Second section: The Data Protection Impact Assessment (DPIA) as a Mechanism for Assessing Risks Before They Occur

---

[1]- Article 27 bis, Articles 41 bis and 41 bis 2 of the Law No. 25-11.

[2]- Ibid, Articles 41.

[3]- Ibid, Articles 41.

Law 25-11 mandated, under Article 45 bis 6, conducting a prior risk assessment study before commencing any processing operation considered high-risk. The article states that "when a type of processing, particularly using new technologies, is likely to result in a high risk to the rights and freedoms of natural persons, the controller must, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on personal data." [1]

The assessment must include, at a minimum:

- A general description of the processing operations.
- An assessment of the risks to the rights and freedoms of data subjects.
- The measures envisaged to address those risks and the guarantees ensuring the protection of data.

The purpose of the impact assessment is to identify potential risks to the rights and freedoms of individuals, assess their severity, and propose necessary measures to address them before harm occurs. In this sense, the DPIA represents a proactive mechanism that reinforces the principle of prevention in data protection, moving protection from a reactive phase to a proactive one.

Third section: Organizing Registers as a Tool for Transparency and Control

Law 25-11 introduced two mandatory registers aimed at enhancing transparency and traceability:

- Register of Processing Activities (Article 41 bis 2): Includes all data processing operations carried out by the institution, specifying their purpose, the type of data processed, the category of data subjects, and the retention period.
- Automated Register of Data Processing (Article 41 bis 3): Documents all automated operations affecting personal data.

Additionally, the law (Article 43) mandated institutions to maintain a special register of violations, containing an updated inventory of each personal data violation, stating its date, nature, effects, and the measures taken to address it. These registers are made available to the National Authority upon its request, enabling it to exercise effective oversight over the extent of compliance with the law. [2]

---

[1]- Ibid, Articles 45 bis 6.

[2]- Articles 41 bis 2, 41 bis 3, Article 43 of the Law No. 25-11.

Third requirement: Punitive and Supervisory Guarantees

No law is complete without supervisory and punitive mechanisms that ensure compliance and achieve deterrence. This requirement presents the punitive and supervisory guarantees in Law 25-11, by analyzing the National Authority's powers in supervision and inspection (First section), examining the new penal system between deterrence and punishment (Second section), and a critical evaluation of the effectiveness of protection on the ground (Third section).

First section: Powers of the National Authority in Supervision and Inspection

The National Authority exercises its supervisory powers to protect data under Articles 46 to 51 of the law amending and supplementing Law 18-07, which expanded its scope of intervention and granted it more effective supervisory tools. The most prominent of these powers include[1]:

- Establishment of regional monitoring and audit hubs, bringing supervision closer to the concerned institutions (Article 27 bis).
- Power of temporary or permanent withdrawal of authorization (Article 48): If processing is found to affect national security or is contrary to morals and public order.
- Power of inspection and verification within institutions, with the assistance of judicial police officers, with the possibility of requesting all necessary documents and information (Articles 49-51).
- Power of warning and notification before imposing sanctions, giving institutions the opportunity to rectify their situations (Article 46).
- Power to propose legislative and regulatory amendments to public authorities (Article 25).

These expanded powers enable the National Authority to play an effective supervisory role, transitioning from a mere advisory body to a real executive body.

Second section: The Penal System Between Deterrence and Punishment

Law 25-11 retained the penal system stipulated in Law 18-07 (Articles 46-51) as is, without making any amendments. These penalties varied between imprisonment, which may reach five (5) years, and fines of up to 500,000 DZD, in addition to administrative supervisory mechanisms such as warnings and notices (Article 46) before imposing penalties, and temporary suspension if processing is found to affect national security or is contrary to morals and public

[1]- Ibid, Articles 25, 27, 46-51.

order (Article 48). All of this enhances the effectiveness of the existing punitive system through precautionary preventive measures[1].

It can be said that this penal system represents a balance between general deterrence (protecting society) and specific deterrence (reforming the offender), as alongside custodial sentences, there are alternative penalties such as fines, proportionate to the type of violation.

Third section: Effectiveness of Protection on the Ground (Critical Evaluation)

Despite the significant progress made by Law 25-11, the effectiveness of protection remains contingent on several factors:

- **Readiness of the National Authority:** The National Authority needs sufficient human and material resources to effectively exercise its supervisory functions.
- **Qualification of Officers:** The DPO position requires specialized training that may not be widely available at present.
- **Culture of Compliance**: The culture of legal compliance in the digital domain remains limited within many institutions.
- **Actual Supervision:** Despite Law 25-11 strengthening the powers of the National Authority for the Protection of Personal Data and expanding its tasks and supervisory powers, the published activities of the Authority until early 2026 focused on awareness-raising, training, and institutional cooperation. No tangible supervisory measures, such as field investigations, probes, or imposing sanctions on violators, had been issued by the National Authority until early 2026, which hinders the achievement of the desired legal deterrence.

THE SECOND TOPIC

The sovreign Dimension – Data Governance In Decree 25-320

The sovereign dimension of data represents the aspect related to the state's organization of its data as a strategic asset, and the governance of its flow and investment to serve the national interest. This section focuses on analyzing Decree 25-320 from the perspective of governance and organization, through three main requirements: the philosophy of governance and the transition from fragmentation to discipline (First requirement), the technical structure of governance (Second requirement), and the institutional distribution of powers (Third requirement).

[1]- Ibid, Articles 46-51.

First Requirement: The Philosophy of Governance – From Fragmentation to Discipline

Decree 25-320 is based on a comprehensive governance philosophy aimed at moving public data from a state of fragmentation and duplication to a state of discipline and organization. Therefore, this requirement analyzes the intellectual foundations upon which the decree was based, by reading the decree's preamble, which considers data a strategic asset (First section), analyzing the transition from traditional governance to comprehensive digital governance (Second section), and defining the scope of the system's application and sovereign exceptions (Third section).

First section: Data as a Strategic Asset

Presidential Decree No. 25-320 of December 30, 2025[1] represents a qualitative shift in the concept of data governance in Algeria, where it has become "a strategic resource no less important than infrastructure and human capital,"[2] thus redefining the relationship between the state and data and placing it among the strategic national assets.

This new perception of data has profound implications for public policies, as it imposes on the state the adoption of a sovereign approach in dealing with data, ensuring its protection from hacking and espionage, and organizing its flow and investment to serve the national interest. It also imposes on public institutions the engagement in a comprehensive digital transformation process that places data at the heart of their concerns.

Second section: The Transition from Traditional Governance to Comprehensive Digital Governance

The decree's preamble defines the strategic objective of the system as moving from "traditional governance based on paper and fragmented digitization to comprehensive digital governance centered on data." The system aims (according to Article 1) to "entrench state sovereignty over data of national interest" and "ensure organized, secure, transparent, and effective management of public data."[3]

---

[1] - Presidential Decree No. 25-320 of December 30, 2025, establishing a national data governance system. Official Gazette, No. 87, dated December 30, 2025. p. 4.

[2] - From the speech of the Prime Minister during his supervision of the launch of the National Data Governance System, website: Office of the Prime Minister, People's Democratic Republic of Algeria. Date: 09/02/2026. https://www.premier-ministre.gov.dz/ar/post/%D9%83%D9% Accessed on: 10/03/2026.

[3]- Article 1 of the Presidential Decree No. 25-320.

This transition requires a comprehensive restructuring of how the public administration deals with data, in terms of:

- **Standardization:** Establishing unified standards for data classification and cataloging[1].
- **Integration:** Connecting different information systems to ensure data exchange via the national interoperability system[2].
- **Security:** Securing data against hacking and espionage via the secure national network[3].
- **Quality:** Ensuring data accuracy, reliability, and timeliness[4].

This transition aims to overcome the state of fragmentation and duplication suffered by the public administration, where the same data exists in multiple databases and different formats, weakening the effectiveness of public decisions and wasting time and effort.

Third section: Scope of the System's Application and Sovereign Exceptions

Article 2 of the decree defines the scope of application of the national system for data governance, covering "all public institutions and administrations, bodies, and institutions entrusted with a public service mission." [5]

Article 3 defines key terms:

- **Data Source:** Public institutions and administrations responsible for data classification, cataloging, reliability, and quality.
- **Data User:** Institutions that benefit from and use data within the framework of their missions. [6]

Article 4 stipulates that personal data remains subject to the provisions of Law 18-07 and its amendments (Law 25-11). [7]

This broad scope reflects the comprehensiveness and depth of the project. However, Article 18 of the decree exempts two main categories from the scope of application:

- Data exchange carried out for national defense and security purposes.
- Data related to the powers of the judicial authority and those pertaining to judicial work[1].

---

[1]- Ibid, Articles 6-7.
[2]- Ibid,Articles 9-10.
[3]- Ibid, Article 11.
[4]- Ibid, Article 3.
[5]- Ibid, Article 2.
[6]- Ibid, Article 3.
[7]- Ibid, Article 4.

These exceptions reflect the balance sought by the decree between the principle of transparency and the requirements of national sovereignty and security, and also preserve the confidentiality and independence of judicial work.

Second requirement: The Technical Structure of Governance

The added value of Decree 25-320 lies in the establishment of an integrated technical structure that governs the process of data governance and regulates its flow. In this requirement, we will analyze the main technical components of the system, represented by the Data Classification Reference (First section), the Data Source Cataloging Reference (Second section), and the National Interoperability System as the exclusive framework for data exchange (Third section).

First section: The Data Classification Reference – Classification Standards and Implementation Mechanisms

Article 6 of the decree establishes the Data Classification Reference as one of the fundamental components of the system. This reference aims to:

- Determine data sensitivity levels (public, internal, confidential, highly confidential).
- Define the permitted uses for each data category.
- Specify the types of protection and security procedures applicable to each category[2].

Thus, this classification is an essential condition for applying the principle of "protection based on risk level," where greater security resources are allocated to the most sensitive data. It also enables the organization of data access according to specific permissions, reducing the risks of leakage and breach.

Second section: The Data Source Cataloging Reference – Towards Unification and Organization of Sources

Article 7 of the decree establishes the Data Source Cataloging Reference as a second essential element of the system. This reference aims to:

- Inventory and define data sources using a unified model.
- Organize data and simplify access to it.
- Improve data quality and reduce the duplication of the same data and the redundancy of its sources[3].

---

[1]- Ibid, Article 18.
[2]- Ibid, Article 6.
[3]- Ibid, Article 7.

This reference addresses a chronic problem in the public administration, where the same data exists in multiple databases and different formats, leading to inconsistencies and undermining trust in it. Cataloging data sources allows for the identification of the "official source" for each piece of information, making it a reference for other institutions, thereby enhancing data reliability and quality.

Third section: The National Interoperability System – The Exclusive Framework for Data Exchange

Articles 8 to 11 form the backbone of the system. Articles 9 and 10 of the decree establish the National Interoperability System as the most important component of the system. This system enables the secure, organized, and efficient exchange of digital data between various public institutions and administrations, bodies, and institutions entrusted with a public service mission. Article 8 states: "The High Commission for Digitization, in coordination with the concerned parties, is responsible for preparing the aforementioned references." [1]

This system is characterized by several features:

- **Exclusive Framework:** The National Interoperability System is the sole framework for data exchange between public institutions[2].
- **Secure Infrastructure:** It operates via a dedicated secure national network, separate from the internet[3].
- **Unified Referential:** It relies on the Data Classification Reference and the Data Source Cataloging Reference[4].

Article 11 stipulates: "The High Commission establishes the infrastructure of the secure national network separately from the internet network." [5]

Regarding access and usage conditions, Article 12 requires any institution wishing to access the system to classify and catalog its data according to the two references. Article 13 also requires the data user to obtain the consent of the data source through the national system[6].

In this sense, the National Interoperability System represents the backbone of data governance in Algeria, ensuring a secure and organized flow of data between institutions and breaking down the silos between different information systems.

---

[1]- Ibid, Article 8.
[2]- Ibid, Article 9.
[3]- Ibid, Article 11.
[4]- Ibid, Article 9.
[5]- Ibid, Article 11.
[6]- Ibid, Articles 12-13.

Third requirement: The Institutional Distribution of Powers

Decree 25-320 assigned specific tasks to national bodies to implement and oversee the system, within a clear distribution of competencies. In this requirement, we present the roles of these bodies, starting with the High Commission for Digitization in a leadership and management position (First section), moving to the National Council for Information Systems Security in the role of functional regulation (Second section), and finally to the integration between the Information Systems Security Agency and the National Authority in the security and rights-based dimensions (Third section).

First section: The High Commission for Digitization – Leadership and Management

The decree assigned several essential tasks to the High Commission for Digitization (Articles 8, 11, 17):

- Preparing, updating, and coordinating the Data Classification Reference and the Data Source Cataloging Reference with the concerned parties[1].
- Deploying and managing the National Interoperability System[2].
- Establishing the infrastructure of the secure national network separately from the internet[3].
- Ensuring data security during the transmission phase[4].

Article 17 stipulated: "The High Commission for Digitization is responsible for deploying and managing the national system and ensures data security during its transmission phase." [5]

These tasks place the High Commission in a leadership and management position for the national data governance system, reflecting the legislator's confidence in its technical and organizational capabilities.

Second section: The National Council for Information Systems Security – Functional Regulation

The National Council for Information Systems Security is responsible, under Article 14 of the decree 25-320, for deciding on any matter related to the functionality of the national data governance system[6]. The Council undertakes the task of ensuring the functional integrity of the system through:

- Reviewing the performance of the National Interoperability System.

[1]- Ibid, Article 8.
[2]- Ibid, Article 17.
[3]- Ibid, Article 11.
[4]- Ibid, Article 9.
[5]- Ibid, Article 17.
[6]- Ibid, Article 14.

- Proposing necessary improvements and modifications.
- Deciding on functional disputes that may arise between different parties.

This role represents an additional guarantee for the proper functioning of the system and independence in evaluating its performance.

Third section: The Information Systems Security Agency and the National Authority – Security and Rights-Based Integration

The roles of the Information Systems Security Agency and the National Authority for Data Protection are integrated in implementing the system:

- **Information Systems Security Agency:** Decides on the classification of data security levels within the national data governance system[1]. This role ensures that security aspects are considered in the classification process, in line with the highest standards.
- **National Authority for Data Protection:** Is responsible for monitoring the compliance of the cataloging and classification of personal data with the legislative and regulatory provisions in force[2]. This role ensures respect for rights and freedoms in the governance process.

This integration between the security and rights-based aspects reflects a balanced vision of governance, combining the requirements of national security with respect for fundamental rights. The system was officially put into service on February 9, 2026, under the supervision of the Prime Minister[3].

THE THIRD TOPIC

Integration Between Rights-Based and Sovreign Dimensions – Mechanisms of Integration and Limits of Application

Law 25-11 and Decree 25-320 cannot be understood in isolation from each other; together they form an integrated system reflecting the balance between protecting individual rights and governing the state's strategic assets. This section analyzes the relationship between the two texts, by reviewing points of convergence and integration (First requirement), analyzing implementation challenges on the ground (Second requirement), and exploring future prospects in light of comparative models (Third requirement).

First requirement: Points of Convergence and Integration

Law 25-11 and Decree 25-320 intersect at several levels, together forming a unified framework for dealing with data in Algeria. This requirement analyzes

---

[1]- Ibid, Article 16.

[2]- Ibid, Article 15.

[3]- Office of the Prime Minister, People's Democratic Republic of Algeria. Date: 09/02/2026. https://www.premier-ministre.gov.dz/ar/post/%D9%83%D9% , Accessed on: 10/03/2026.

the main points of integration between the two texts, represented by integration in personal data protection (First section), integration in regulating data transfer (Second section), and institutional integration between the National Authority and the High Commission (Third section).

First section: Integration in Personal Data Protection – Governance as a Protection Mechanism

The integration between Law 25-11 and Decree 25-320 is evident in providing dual protection for personal data. On one hand, Law 25-11 provides rights-based protection through mechanisms of consent, transparency, and objection[1]. On the other hand, Decree 25-320 provides technical protection through data classification, securing its exchange, and ensuring its quality[2].

This integration makes the protection of personal data a shared responsibility between rights-based bodies (the National Authority) and technical bodies (the High Commission, ANSSI), thereby enhancing the effectiveness of protection and reducing the risks of breach and leakage. Rights-based protection without technical measures remains theoretical, and technical protection without rights-based considerations remains deficient.

Second section: Integration in Regulating Data Transfer – Prior Authorization and the National System

The two texts integrate in regulating data transfer, especially cross-border transfers. Law 25-11 (Article 44) regulates the transfer of personal data across borders by requiring prior authorization from the National Authority, assessing the level of protection in the receiving country[3]. Decree 25-320, on the other hand, regulates data exchange between public institutions via the National Interoperability System, reducing dependence on foreign infrastructure[4].

This integration forms a dual framework for data protection: a legal dimension through prior authorization from the National Authority, and a technical dimension through the secure national infrastructure.

Third section: Institutional Integration – The National Authority and the High Commission

Oversight of the system is distributed among several national bodies with integrated roles defined by the articles:

---

[1]- Articles 7, 32, 34, 36 of the Law No. 25-11.

[2]- Articles 9-11 of the Presidential Decree No. 25-320.

[3]- Article 44 of the Law No. 25-11.

[4]- Articles 8, 9, 11, 17 of the Presidential Decree No. 25-320.

- **The National Authority:** Monitors respect for rights and freedoms in the processing of personal data[1].
- **The High Commission:** Manages the National Interoperability System and oversees data governance[2].
- **The Information Systems Security Agency:** Regulates the security aspect[3].
- **The National Council for Information Systems Security:** Ensures functional integrity[4].

This distribution creates a kind of balance and integration between different considerations (rights-based, technical, security, functional) and reflects a comprehensive vision for data management.

Second requirement: Implementation Challenges on the Ground

Despite the significant legislative progress represented by Law 25-11 and Decree 25-320, the Algerian system for data governance and protection faces several challenges hindering effective application. This requirement analyzes the most prominent of these challenges, represented by the absence of complementary regulatory texts (First section), the problem of coordination between bodies (Second section), and the limitations of human and material resources and the scarcity of expertise (Third section).

First section: Absence of Complementary Regulatory Texts (The List of Countries with Adequate Protection as a Model)

Despite the clarity of general principles in the two texts, some implementation mechanisms remain undefined, most notably:

- The absence of an officially published list of countries providing an "adequate level of protection" according to the Algerian criteria specified in Article 44 of Law 18-07.
- The absence of approved models for binding contractual guarantees stipulated in Article 45 of Law 18-07.

This ambiguity creates a state of legal uncertainty for companies and institutions dealing with foreign partners and hinders the data flow necessary for economic activity, leaving companies perplexed about how to organize their contractual relations with their foreign partners. Consequently, all those provisions, measures, and guarantees are insufficient for the success of the tasks

[1]- Article 15 of the decree No. 25-320, and Articles 22-31 of Law 25-11 amending Law 18-07.
[2]- Articles 8, 11, 17 of Decree 25-320.
[3]- Article 16 of the same law.
[4]- Ibid, Article 14.

assigned to the National Authority, and hence the personal data protection system as a whole.

Second section: The Problem of Coordination Between Bodies – Between Text and Application

Although phrases ordering coordination appear in the texts, as in Article 8 of Decree 25-320 which stipulates "in coordination with the concerned parties"[1], they remain general and non-detailed, without specifying permanent mechanisms for consultation, information exchange, and resolution of potential disputes.

This ambiguity creates practical challenges:

- **Overlap in competencies:** especially in areas of joint audit.
- **Duplication of efforts:** wasting time and resources.
- **Absence of dispute resolution mechanisms:** when the viewpoints of different bodies differ.
- **Weak information exchange:** weakening the effectiveness of supervision.

Furthermore, some argue there is a "conflict between the right to personal data protection and other rights such as the right to access information (Article 55 of the 2020 Constitution) and freedom of expression (Article 54)". [2]

Third section: Limitations of Human and Material Resources – Scarcity of Expertise

The competent bodies suffer from a shortage of qualified human resources and adequate material resources necessary to carry out their tasks efficiently, especially given the rapid pace of technology development and increasing violations. This necessitates providing specialized expertise in interdisciplinary fields (legal, technical, security) and sufficient financial resources to develop supervisory systems and keep pace with international developments.

The absence of these resources prevents these bodies from playing their actual role and renders them unable to achieve the objectives for which they were established. Furthermore, the scarcity of specialized personnel in the digital domain at the national level negatively reflects on the ability of these

---

[1] - Article 8 of Decree 25-320.

[2] - 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, No. 82, dated 30 December 2020, p. 13.

Ahmed. I, Dharifi. N, أثر التعديل الدستوري لسنة 2020 على الحقوق والحريات في الجزائر (*The impact of the 2020 constitutional amendment on rights and freedoms in Algeria*). Journal of Legal and Social Sciences, Professor Researcher Journal for Legal and Political Studies , Volume 7, Issue 1, 2022. p. 675- 679.

bodies to attract the necessary expertise, creating a vicious cycle that weakens the entire supervisory system.

Third requirement: Prospects for Development in Light of Comparative Experiences

Lessons can be drawn from successful international experiences to develop the Algerian system for data governance and protection. This requirement reviews the most important of these experiences, represented by the European experience in data protection (GDPR) (First section), the approach of the European Artificial Intelligence Act (AI Act) (Second section), and a statement of the limits of comparison and the specificity of the Algerian context (Third section).

First section: Benefiting from the European Experience (GDPR) in Data Protection

The European General Data Protection Regulation (GDPR) is the most prominent international reference in the field of personal data protection[1]. Accordingly, several lessons can be drawn from this experience to develop the Algerian system:

- **Periodic Evaluation Mechanisms:** Article 97 of the GDPR requires the European Commission to submit an evaluation report every four years[2].
- **Standard Contractual Clauses:** The regulation provides approved models for contracts between parties involved in data transfer.
- **Lists of Countries with Adequate Protection:** The European Commission publishes an official list of countries providing an adequate level of protection, creating legal certainty for companies.

Second section: Drawing Inspiration from the Approach of the European Artificial Intelligence Act (AI Act)

The European Artificial Intelligence Act (AI Act) offers an innovative approach based on classifying AI applications according to risk level (Article 6

[1] - European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation - GDPR). Official Journal of the European Union, L 119, 1-88.

[2] - European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union.

and Annex III)[1]. Accordingly, this approach can be drawn upon in Algeria through:

- **Application Classification:** Identifying high-risk applications requiring strict oversight.
- **Algorithmic Transparency:** Mandating AI system developers to provide clear explanations of how their algorithms work.
- **Human Oversight:** Ensuring humans remain in the loop for critical decision-making [2].

Third section: Limits of Comparison and Specificity of the Algerian Context

Comparing with international models does not aim to replicate their experiences, but rather to extract insights that help develop the Algerian system while considering its specificities:

- **Specificity of the European Model:** It is characterized by strict periodic evaluation mechanisms (Article 97 of the GDPR) and an advanced data protection system, but it reflects European specificities related to a long accumulation of rights-based considerations.
- **Specificity of the Algerian Model:** It combines the rights-based dimension (Law 25-11) and the sovereign dimension (Decree 25-320) in an integrated framework, which constitutes a national specificity that may be more suitable for the Algerian context.
- **The Shared Challenge**: All models face difficulty in balancing data protection and technological innovation, a challenge shared by Algeria with other countries.

These insights reveal that the success of any model is not measured by its proximity to Western models, but by its ability to meet the needs of the society it regulates. However, this does not prevent us from drawing inspiration from some successful experiences and appropriate solutions for certain shortcomings we have previously identified, with the aim of addressing them and achieving the necessary data protection and preserving digital sovereignty.

Conclusion:

This study has reached a number of key findings:

---

[1]- European Union Agency for Fundamental Rights (FRA). (2024). GDPR in practice – Experiences of data protection authorities. and Hannes Snellman Digital Horizon. (2024). Chapter XIII of the AI Act: Final Provisions. https://digitalhorizon.hannessnellman.com/ai-strategy/ai-regulation-air/ Viewed on: 27/10/2025.

[2]- Compare with Articles 6 and Annex III, Article 14, Articles 50 and 53/1/d of the European AI Act.

1. At the level of the rights-based dimension (Law 25-11): The law achieved a qualitative shift towards practical protection by introducing the Data Protection Officer (DPO) as an internal privacy guardian, mandating Data Protection Impact Assessments (DPIA) for high-risk processing, organizing mandatory registers and enhancing transparency, tightening control over cross-border data transfers, and strengthening the powers of the National Authority.
2. At the level of the sovereign dimension (Decree 25-320): It established an integrated governance system based on considering data as a strategic state asset, transitioning from fragmented traditional governance to comprehensive digital governance, creating the National Interoperability System as an exclusive framework for data exchange, establishing two national references for data classification and source cataloging, and clearly distributing competencies among national bodies.
3. At the level of integration between the two texts: The law and decree integrate in the following aspects:

   - Personal data protection: where technical governance complements rights-based protection.

   - Regulating data transfer: by combining prior authorization (legal) and the national system (technical).

   - Institutional integration: by distributing roles between the National Authority (rights-based) and the High Commission (technical).
4. **At the level of challenges:** The study revealed the absence of complementary regulatory texts, especially the list of countries with adequate protection; limited institutional coordination despite phrases mandating coordination in the texts; weak human and material resources of supervisory bodies; and scarcity of specialized expertise.
5. **At the comparative level:** Comparison with the GDPR and the AI Act showed that the Algerian system is moving in the right direction, but it needs to strengthen periodic evaluation mechanisms and draw inspiration from the "risk-based" approach in classifying applications.

Recommendations:

In light of the preceding analysis, the following recommendations can be proposed to develop the Algerian system:

1. Issue complementary regulatory texts: especially the list of countries with adequate protection, approved models for contractual guarantees, and standards for government cloud services.

2. Strengthen institutional coordination mechanisms: by establishing a permanent coordination mechanism between the High Commission, the Information Systems Security Agency, and the National Authority, with clear protocols for consultation and information exchange.
3. Develop specialized human resources: through specialized training programs in the fields of data governance and protection, in partnership with universities and higher schools.
4. Establish a national mechanism for periodic evaluation: every two or three years, to assess the effectiveness of legislation and update it according to technological developments.
5. Strengthen the role of the National Authority: by providing it with adequate human and material resources, launching actual inspection and control campaigns, and publishing periodic reports on its activities.
6. Benefit from international experiences: in developing cybersecurity standards and data governance, especially the US NIST framework and the European GDPR.
7. Issue a comprehensive artificial intelligence law: defining general principles for its uses, classifying applications according to risk level, and prohibiting algorithmic discrimination.

Bibliography:

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.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.
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- 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 of the People's Democratic Republic of Algeria , No. 48, dated July 24, 2025, p. 14.

5- 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

1. Berkani Fadhila. حماية الحق في الخصوصية في التشريع الجزائري (*Protection of the right to privacy in Algerian legislation*). Algerian Journal of Law and Political Science, 1(10), 2022. p. 996.
2. Mohamed Al-Eidani, Yousef Zarrouk. حماية المعطيات الشخصية في الجزائر على ضوء القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي) (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.
3. Ahmed Iman, Dharifi Nadiya. أثر التعديل الدستوري لسنة 2020 على الحقوق والحريات في الجزائر (*The impact of the 2020 constitutional amendment on rights and freedoms in Algeria*). Journal of Legal and Social Sciences, Professor Researcher Journal for Legal and Political Studies , Volume 7, Issue 1, 2022. p. 671- 681.

Third: Internet websites

1- Office of the Prime Minister, People's Democratic Republic of Algeria. Date: 09/02/2026. websites: https://www.premier-ministre.gov.dz/ar/post/%D9%83%D9% , Viewed on: 12/02/2026.

2- European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation - GDPR). Official Journal of the European Union, L 119, 1-88. websites: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng , Viewed on: 12/01/2026.

3- European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union. websites: https://artificialintelligenceact.eu/the-act/, Viewed on: 12/01/2026.

4- European Union Agency for Fundamental Rights (FRA). (2024). GDPR in practice – Experiences of data protection authorities. websites: https://fra.europa.eu/en/publication/2024/gdpr-experiences-data-protection-authorities , Accessed on: 10/01/2026.

5- Hannes Snellman Digital Horizon. (2024). Chapter XIII of the AI Act: Final Provisions. https://digitalhorizon.hannessnellman.com/ai-strategy/ai-regulation-air/ Viewed on: 27/01/2026.