Artificial Intelligence and Big Data in the Algerian Legislative Space

الذكاء الاصطناعي والبيانات الضخمة في الفضاء التشريعي الجزائري



Chekirin Mohamed Cherif[1]
University Of Djilali Bounaama, m-chekirine@univ-dbkm.dz [1]

Received: 01./10/2026 *Accepted:01/11/2026* *Published:.17/11/2026*

Abstract:

This article centres its analysis on Algerian legislation governing artificial intelligence (AI) and big data, in particular Law No. 18-07 on personal-data protection — recently amended by Law No. 25-11 of 24 July 2025 — and Order No. 09-04 on ICT offences. Through a technically grounded analysis of machine learning, deep learning, large language models, and explainable AI, it identifies specific failures that these instruments, even as amended, cannot address, drawing on Algerian legal scholarship and institutional practice as the primary reference points. Foreign models (the European Union, France, Germany, Saudi Arabia and the African Union) are examined only for mechanisms genuinely transferable to Algeria's own legislative and institutional context. The study concludes with a legislative reform roadmap prioritising Algeria's regulatory capacity and recent legislative developments over further reliance on comparative transplantation.

Keywords: *Artificial Intelligence | Big Data | Machine Learning | Large Language Models | Explainable AI*

ملخص:

تُركّز هذه المقالة تحليلها على التشريع الجزائري الناظم للذكاء الاصطناعي والبيانات الضخمة، وتحديدًا القانون رقم 18-07 المتعلق بحماية المعطيات الشخصية -المعدَّل مؤخرًا بالقانون رقم 25-11 المؤرخ في 24 يوليو 2025- والأمر رقم 09-04 المتعلق بالجرائم المعلوماتية. ومن خلال تحليل تقني مؤسَّس لتقنيات التعلم الآلي والتعلم العميق والنماذج اللغوية الكبرى والذكاء الاصطناعي القابل للتفسير، تحدد الدراسة أوجه القصور التي يعجز هذان النصان، حتى بعد تعديلهما، عن معالجتها، معتمدة على الفقه والممارسة المؤسساتية الجزائرية كمرجعية أساسية. أما النماذج الأجنبية (الاتحاد الأوروبي، فرنسا، ألمانيا، السعودية والاتحاد الإفريقي) فلا تُستحضر إلا لتوظيف آلياتها القابلة فعليًا للتطبيق في السياق الجزائري، وتُختتم الدراسة بخارطة طريق تشريعية تُعطي الأولوية للقدرة التنظيمية الجزائرية والتطورات التشريعية الحديثة.

الكلمات المفتاحية: الذكاء الاصطناعي؛ البيانات الضخمة؛ التعلم الآلي؛ النماذج اللغوية الكبرى؛ الذكاء الاصطناعي القابل للتفسير.

1- Corresponding author: Chekirin Mohamed Cherif, e-mail: m-chekirine@univ-dbkm.dz

INTRODUCTION

The accelerating diffusion of artificial intelligence and big-data systems into social, economic, and administrative life confronts Algerian law with a structural challenge: its principal instruments — Law No. 18-07 of 10 June 2018 on the protection of personal data and Order No. 09-04 of 5 August 2009 on ICT offences — were conceived before deep learning, large language models, and population-scale algorithmic decision-making existed[1]. This mismatch is not merely theoretical: courts confronting algorithmic harm must rely on civil-liability analogies drawn from pre-digital tort law, and the National Authority for the Protection of Personal Data (ANPDP) has, until recently, lacked the express statutory tools to supervise AI-driven processing.

Law No. 18-07 itself has just been amended — by Law No. 25-11 of 28 Muharram 1447 AH corresponding to 24 July 2025[2] — confirming that Algerian legislation in this field is actively evolving and that its adequacy to AI-specific risk is a live, not a settled, question. This article accordingly centres its analysis on Algerian law: it examines, provision by provision, why Law No. 18-07 (as amended) and Order No. 09-04 remain structurally inadequate to specific categories of AI system, situates this critique within Algerian legal scholarship, draws on foreign models only where they illuminate a specifically Algerian gap, and proposes a reform roadmap grounded in Algeria's own institutional capacity.

1. Theoretical Framework and Algerian Legal Scholarship

Examining the legal challenges posed by artificial intelligence to personal data protection in Algeria requires an understanding of both the relevant theoretical frameworks and national legal scholarship. While comparative regulatory theories provide useful analytical perspectives, Algerian legal scholarship offers essential insights into the interpretation and application of domestic legislation. Accordingly, this section examines these two dimensions to establish the conceptual and doctrinal foundations for assessing the adequacy of Algeria's legal framework in addressing AI-driven data processing.

1.1 Theoretical Framework

The analysis draws selectively on five frameworks from comparative regulatory theory — Lex Informatica, Adaptive Governance, Risk-Based Regulation, Algorithmic Accountability, and Digital Constitutionalism — used only where they clarify a specific gap in Algerian law, not as a substitute for it.

1.2 Algerian Legal Scholarship

Algerian scholarship on personal-data protection has grown substantially since Law No. 18-07's adoption. Ben Othman examines the protection of natural persons in data processing under Law No. 18-07[3]; Al-Khalidi addresses AI governance in judicial work; and recent Algerian journal literature has examined the ANPDP's institutional mandate and the practical obstacles to its independence, including the regional-branch mechanism just introduced by Law No. 25-11[4]. This body of work remains

concentrated on data-protection fundamentals and the ANPDP's institutional design; it has not yet engaged systematically with the AI-specific technical categories — machine learning, deep neural networks, large language models — that increasingly determine how personal data is actually processed. This article addresses that gap: a provision-by-provision analysis of Law No. 18-07, as amended, and Order No. 09-04 against specific AI architectures, prioritising Algerian legislative text, institutional practice, and scholarship, with foreign models cited only for genuinely comparative or theoretical value.

2. AI System Architectures and Their Specific Legal Failures in Algerian Law

Diagnosing the inadequacy of Algerian law requires understanding, for each category of AI system, the precise technical property that generates legal risk and the specific provision it escapes.

2.1 Machine learning

Machine learning systems derive decision functions from statistical patterns in training data rather than human-authored rules. Article 2 of Law No. 18-07 defines 'processing' as discrete operations on data without reaching the training process itself, and Article 14 grants a right of access but nothing equivalent to a right against purely automated decisions: an applicant refused a loan by an ML system has no right to know the decision was automated, no right to human review, and no right to contest it. The gap is

structural, not interpretive: no provision of Law No. 18-07, before or after the 2025 amendment, treats the training phase — during which personal data actually shapes a system's future behaviour toward individuals — as 'processing' at all.

2.2 Deep neural networks

Deep neural networks are opaque even to their designers and prone to amplifying bias latent in training data. Article 12's general duty of 'appropriate technical and organisational measures' sets no standard for bias auditing or interpretability testing, and Law No. 18-07 — unamended on this point by Law No. 25-11, whose 2025 changes target institutional reach rather than substantive AI obligations — contains no anti-discrimination or algorithmic-audit duty.

2.3 Large language models

Large language models generate outputs probabilistically rather than by retrieval; a person harmed by relying on a hallucinated legal or medical output has no clear claim under the Civil Code's fault-based liability (Arts 124–140), and Order No. 09-04 contains no provision for AI-generated disinformation or synthetic media.

2.4 Explainable AI and adversarial manipulation

Explainable-AI methods aside, Law No. 18-07 grants no right to an explanation of automated decisions and no transparency duty for high-risk outputs, leaving algorithmic discrimination difficult to detect or contest in practice; and adversarial manipulation and data-poisoning of AI systems have no analogue in Order No. 09-

04's cybercrime provisions, which target unauthorised access and data interference but not the deliberate corruption of a model's training or inputs.

2.5 Big data

Big-data analytics enable re-identification of anonymised individuals and inference of sensitive attributes from ostensibly neutral data — risks Law No. 18-07 does not contemplate, because it regulates discrete processing operations rather than the analytical systems, AI included, that actually generate these risks.

3. Comparative Models: What They Add to the Algerian Analysis

Five foreign models were examined, not for descriptive completeness, but strictly for mechanisms transferable to Algeria. The EU's twin GDPR/AI Act framework offers the clearest template[5]: risk-based classification, mandatory impact assessments, Privacy by Design, and turnover-based sanctions of up to 4% of global turnover — mechanisms directly adaptable to reforming Law No. 18-07's fixed, disproportionately low penalty ceiling of 500,000 DZD. France's CNIL shows that a supervisory authority's technical capacity can be built ahead of legislative reform, a precedent directly relevant to resourcing the ANPDP's new regional branches under Law No. 25-11. Germany's constitutional grounding of data protection, in human dignity and personal freedom, parallels Articles 39–41 of Algeria's own 2020 Constitution, suggesting that judicial interpretation, not legislation

alone, can extend protection to AI-specific harms. The Saudi Arabia show that a developing civil-law state can build AI-governance capacity rapidly through a single integrated institution — a structural option for the ANPDP itself. The African Union's Malabo Convention, which Algeria has not yet ratified, would require no new domestic legislation, only accession.

4. The Algerian Legislative Framework: Critical Analysis

Algerian legislation is analysed here first and centrally: each provision is read on its own terms, then tested against the AI-specific risks identified in Part II and, where relevant, against the comparative mechanisms above — in that order of priority.

4.1 The 2025 amendment

Law No. 18-07 was substantially amended on 24 July 2025 by Law No. 25-11 — its first revision since 2018. According to the ANPDP's own public statement on the reform, the amendment imposes new obligations on competent authorities that process personal data for the prevention, investigation, and prosecution of offences, and introduces a new Article 27 bis empowering the National Authority to establish regional branches to audit data controllers beyond the capital[6]. This is a genuine, if partial, institutional response to the ANPDP's chronic under-resourcing. It does not, however, touch the substantive deficiencies that bear specifically on AI governance, which remain as follows.

4.1.1 Definitional exclusion of AI training

Article 2's definition of 'processing' does not reach the statistical optimisation by which ML systems learn decision functions, excluding the formative process that determines AI behaviour from the law's scope.

4.1.2 No automated-decision-making rights

Article 14 grants access to one's data but nothing equivalent to a right against automated decisions with significant effects, leaving Algerians unprotected in credit, employment, housing, healthcare, and criminal-justice contexts.

4.1.3 A consent framework incompatible with AI

Article 25 makes consent the primary lawfulness basis but does not address the impossibility of meaningful consent to algorithmically determined, unpredictable outcomes, nor the power asymmetry between AI providers and data subjects.

4.1.4 No algorithmic decision-making provision

The law makes no reference to automated decision-making or profiling, despite these being the primary mechanisms through which AI produces legally significant consequences.

4.1.5 A general security obligation inadequate for AI

Article 12 requires 'appropriate technical and organisational measures' without the specificity AI requires — no bias-auditing, adversarial-robustness, or model-documentation standard.

4.1.6 Sanctions disproportionate to AI-era violations

Even after Law No. 25-11, the maximum administrative fine under Article 68 remains 500,000 DZD — disproportionate to violations by large technology operators and offering no credible deterrence.

4.1.7 Absence of Privacy by Design and cross-border transfer provisions

The law contains neither mechanism, which comparable frameworks treat as essential to data protection in the AI era.

4.2 Order No. 09-04

Order No. 09-04 predates the contemporary AI landscape by a decade, with five deficiencies: silence on algorithmic offences; no provision for deepfakes or AI-generated disinformation; inadequate treatment of AI-powered automated surveillance; electronic-evidence provisions that do not address machine-generated data; and penal provisions offering no basis for criminalising adversarial attacks on AI systems or data poisoning of ML pipelines.

4.3 The Civil Code

The Civil Code's general delictual-liability framework (Arts 124–140) rests on personal fault, direct causation, and certainty of harm — elements systematically difficult to establish where a discriminatory output results from a distributed, opaque, multi-temporal chain running from training data through model architecture to deploying organisation. Algerian law currently

offers no normative anchor for algorithmic accountability and no basis for liability where AI harm is foreseeable but not traceable to a single negligent act.

5. A Legislative Reform Roadmap for Algeria

5.1 Three legislative pillars

(1) a dedicated AI law establishing risk-based classification — prohibited, high-risk, limited-risk, minimal-risk — with mandatory impact assessment and a right to human review, calibrated to Algerian institutional capacity rather than transplanted wholesale from any foreign model; (2) completing Law No. 18-07's reform beyond Law No. 25-11, by adding Privacy by Design, an explicit right against purely automated decisions, a right to explanation, and turnover-based sanctions replacing the current 500,000 DZD ceiling — calibrated, as the EU comparison above suggests, to a percentage of annual turnover rather than a fixed sum, so that penalties scale with the size of the violator rather than losing all deterrent value against large operators; (3) modernising Order No. 09-04 to criminalise adversarial attacks on AI systems, data poisoning, and AI-generated disinformation.

5.2 Three institutional levels

(1) fully resourcing the ANPDP's new regional branches under Law No. 25-11 with the technical specialists and audit powers an AI-supervision mandate requires, once the pending implementing decree is published; (2) building judicial and administrative

capacity through specialised digital-dispute chambers and training on algorithmic evidence and liability; (3) ratifying the Malabo Convention and engaging African and Arab digital-governance forums from a position of updated domestic legislation, not before it.

CONCLUSION

This article has argued, at the theoretical level, that Law No. 18-07, even as amended by Law No. 25-11, and Order No. 09-04 remain structurally inadequate to machine learning, deep learning, large language models, and adversarial AI risks. The reasons are textual and institutional, not a mere absence of legislative attention: the definition of processing excludes training (4.1.1), automated-decision rights are absent (4.1.2), and sanctions and criminal provisions do not scale to AI-era harm (4.1.6, 4.2). Foreign models matter here only insofar as they clarify mechanisms that Algerian law can adapt on its own terms. The recommendations below follow directly from these findings and are ordered by priority and by the body responsible for implementing them.

Policy Recommendations

1. **Short term (legislative amendments within the existing framework)**
    - **Legislator:** Amend Article 2 of Law No. 18-07 so that

"processing" expressly covers the training of AI systems (see 4.1.1).

- **Legislator:** Add an explicit right against purely automated decisions with significant effects, together with a right to human review and to explanation (see 4.1.2, 4.1.4).
- **Legislator:** Replace the fixed 500,000 DZD ceiling in Article 68 with turnover-based administrative sanctions (see 4.1.6).

2. **Medium term (new instruments and institutional capacity)**
   - **Legislator:** Enact a dedicated, risk-based AI law (prohibited, high-risk, limited-risk, minimal-risk) with mandatory impact assessment, calibrated to Algerian institutional capacity (see 5.1).
   - **Legislator:** Modernise Order No. 09-04 to criminalise adversarial attacks, data poisoning, and AI-generated disinformation (see 4.2).
   - **ANPDP and Government:** Fully resource the regional branches created under Law No. 25-11, with technical specialists and audit powers, once the implementing decree is published (see 4.1, 5.2).
   - **Government:** Ratify the Malabo Convention only after the domestic reform above is in place, so that accession consolidates the national framework instead of

preceding it (see 5.2).

3. **Long term (judicial capacity and research)**
    - **Ministry of Justice and judicial training bodies:** Establish specialised digital-dispute chambers and train judges on algorithmic evidence and liability, including a reform of Civil Code liability (Arts 124-140) to cover foreseeable but untraceable AI harm (see 4.3).
    - **Universities and research bodies:** Integrate AI and data-protection law into legal education, and support empirical studies of how Algerian courts and the ANPDP apply these rules to AI cases, since this article's contribution is theoretical.

Bibliography List:

1. Legislation and Regulatory Instruments:

1. Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1.

2. Journal Officiel de la République Algérienne, No. 48 of 24 July 2025, Law No. 25-11 of 28 Muharram 1447 AH corresponding to 24 July 2025, amending and supplementing Law No. 18-07 of 25 Ramadhan 1439 AH corresponding to 10 June 2018 on the protection of natural persons in the processing of personal data.

2. Journal Articles:

3. Farida Ben Othman, 'Artificial Intelligence: A Legal Approach' (2020) 12(II) Dafatir al-Siyasa wa-l-Qanun.

4. Saddouk El Mehdi & Gharibi Mohamed, 'Effectiveness of the Role of the National Authority for the Protection of Personal Data in the Digital Environment' (2025) 9(2) Majallat al-Fikr al-Qanuni wa-l-Siyasi (ISSN 2588-

1620) 1540–1562.

3. Internet Websites:

5. Algeria, Ministry of Post and Telecommunications (2023), 'Digital Algeria 2025 Strategy: National Plan for Digital Transformation,' detailed website: https://www.mpt.gov.dz (consulted on 25/08/2026).

6. El Itihad (Algerian daily), 'Personal Data Protection: The National Authority Informs All Stakeholders of the Amendments Made to the Law' (3 August 2025), reporting the ANPDP's statement on Law No. 25-11.

1 Algeria, Digital Algeria 2025 Strategy: National Plan for Digital Transformation (Ministry of Post and Telecommunications, 2023).

2 Journal Officiel de la République Algérienne, No. 48 of 24 July 2025, Law No. 25-11 of 28 Muharram 1447 AH corresponding to 24 July 2025 amending and supplementing Law No. 18-07 of 25 Ramadhan 1439 AH corresponding to 10 June 2018 on the protection of natural persons in the processing of personal data.

3 Farida Ben Othman, 'Artificial Intelligence: A Legal Approach' (2020) 12(II) Dafatir al-Siyasa wa-l-Qanun.

4 Saddouk El Mehdi & Gharibi Mohamed, 'Effectiveness of the Role of the National Authority for the Protection of Personal Data in the Digital Environment' (2025) 9(2) Majallat al-Fikr al-Qanuni wa-l-Siyasi (ISSN 2588-1620) 1540–1562.

5 Regulation (EU) 2016/679 (GDPR) [2016] OJ L119/1; Regulation (EU) 2024/1689 (AI Act) [2024] OJ L2024/1689.

6 El Itihad (Algerian daily), 'Personal Data Protection: The National Authority Informs All Stakeholders of the Amendments Made to the Law' (3 August 2025), reporting the ANPDP's statement on Law No. 25-11.