Contemporary Readingsin Law and Social Justice
ISSN: 1948-9137, e-ISSN: 2162-2752
Vol 18 (01), 2026
pp.159 - 179

# Algorithmic Governance and Data Protection in Algerian Smart Cities: An Analysis of Law 18-07

**Meriem Belkessam[1], Ahmed Radji Mokaddem[2]**

[1]Lecturer class A, university Bordj Bouariridj, Algeria. Email: meriem.belkessam@univ-bba.dz

[2]Phd Student, University Bordj Bouariridj, Cyber Justice Laboratory, Algeria. Email: ahmedradji.mokaddem@univ-bba.dz

## ABSTRACT:

Algeria's transition into a data-driven society is anchored in Law No. 18-07 and its 2025 modernization, which seeks alignment with international standards like the GDPR. However, the rapid deployment of AI-driven smart cities introduces complex socio-technical risks, including algorithmic discrimination and affinity profiling, that challenge existing regulatory boundaries. This paper analyzes the efficacy of Algeria's legal and institutional architecture in mitigating these automated harms within urban governance. The research finds that while the framework demonstrates high formal convergence with global models, it is fundamentally undermined by the lack of an explicit right to an explanation, the absence of proxy-based anti-discrimination rules, and the broad exclusion of national security data from oversight. Furthermore, the National Authority (ANPDP) faces persistent implementation hurdles due to an institutional technical expertise gap required for auditing complex AI systems. Ultimately, the study characterizes the framework as partially adequate but structurally insufficient. It proposes a strategic roadmap for legislative reform and technical capacity building to ensure substantive algorithmic accountability

**Keywords:** Algorithmic Governance, Algerian Smart Cities, Data Protection, Algorithmic Discrimination, Affinity Profiling, Law No. 18-07, GDPR Alignment

**Received: 22/06/2025** **Accepted: 25/11/2025** **Published: 16/01/2026**

## Introduction

The transition of Algeria into an increasingly data-driven society began with the foundational Law No. 18-07, a statutory architecture designed to fill a historical legal vacuum by establishing core principles of lawfulness, fairness, and purpose limitation in the handling of natural persons' identities [1]. As the digital landscape continued to evolve, the 2025 amendments were enacted to modernize this framework, primarily seeking alignment with international standards like the General Data Protection Regulation (GDPR) to facilitate international judicial cooperation and address the complex challenges of Big Data and cloud-based processing [2]. While these reforms introduced institutional enhancements such as Data Protection Officers (DPOs) and mandatory Data Protection Impact Assessments (DPIAs), the move toward an automated society reveals critical regulatory blind spots [1].

At stake in this legislative evolution is the transparency of the black box of AI and the protection of individuals from algorithmic bias, particularly given that the explicit exclusion of data related to defense and national security under Article 6 may shield pervasive smart city surveillance systems from effective oversight and non-discrimination audits [1]. This essay argues that while the Algerian framework possesses a high level of formal convergence with the European regulatory model, it fundamentally lacks the substantive right to an explanation of algorithmic logic and an explicit prohibition of proxy discrimination necessary to ensure equity [1]. Consequently, the current legal architecture serves as an incomplete shield against the opaque forms of automated discrimination that define the contemporary digital era.

## 1. The Mechanics and Socio-Technical Risks of AI-Driven Urban Governance

### Conceptual Definitions of AI Governance

AI-driven governance in smart cities is defined as the increasing instrumentation of urban environments with pervasive computing and digitally enabled devices to monitor, manage, and regulate city flows and processes in real time[3]. This model integrates smart city infrastructure, such as sensors and the Internet of Things (IoT), with advanced AI technologies, including machine learning, predictive analytics, and computer vision[3]. Through these technologies, sensitive governance functions like traffic management, public safety, resource allocation, and service delivery are increasingly automated or enhanced by data-driven insights[4]. In the Algerian context, this represents a fundamental shift toward a comprehensive constitutional framework where cognitive computing assumes a central role in administrative and political decision-making[5].

This transition allows public authorities to move from traditional, reactive management toward automated policy execution based on continuous data streams[3]. Concrete examples include intelligent transportation systems that adjust signals based on live vehicle flow and centralized control rooms that coordinate emergency responses based on sensor data[4]. However, the autonomous nature of these systems and their dependency on massive, often skewed datasets create inherent vulnerabilities that facilitate algorithmic discrimination and affinity profiling[5].

Identifying these risks requires an examination of the specific AI applications currently deployed within the urban fabric.

### Typology of Deployed Urban AI Systems

Representative AI systems in modern smart city governance include predictive policing, which utilizes machine learning to identify crime hotspots, and smart traffic management, which employs computer vision and real-time analytics to optimize mobility[4]. Public safety is further augmented by digital surveillance networks and coordinated emergency response systems, while citizen services often rely on integrated ticketing and real-time passenger information displays[4]. In the social sphere, public employment agencies have begun deploying profiling tools to predict job prospects, and welfare administrations use risk-scoring algorithms to detect fraud among recipients[6]. These widespread operational examples extend to migration management, where automated systems are used for language identification and border surveillance[6]. Furthermore, many cities are integrating urban operating systems designed to knock down departmental silos by combining data streams for city-wide regulation[4]. By standardizing these functions through data-driven models, cities create an environment where the categorization of individuals becomes the primary mechanism for distributing public resources. Such pervasive categorization is made possible by a sophisticated operational mechanism that handles urban data in a continuous, real-time cycle.

### The Three-Stage Data-to-Action Cycle

The operational logic of AI-driven governance follows a sequential three-stage loop: data collection, processing, and decision or action[7]. Data collection involves gathering vast volumes of information with high variety and velocity from sources like IoT sensors, cameras, mobile apps, and public databases[8]. This big data is processed using real-time machine learning models and cloud computing to perform feature extraction, inference, and pattern recognition[7]. Finally, these algorithmic outputs translate into governance actions, ranging from automated adjustments to traffic signal sequences to profiling-based interventions in social welfare and policing[3]. These closed-loop systems enable cities to become sentient, reacting dynamically to the behaviors of their residents[8]. This seamless integration of data and action is often promoted as a way to enhance administrative efficiency and transparency[3]. However, the speed and opacity of these decision loops often obscure the points where biased data or flawed correlations initiate systemic unfairness.

### Theoretical Risk Foundations

Within this real-time framework, two primary risks emerge: algorithmic discrimination, where automated systems disadvantage certain individuals or groups, and affinity profiling, which groups people based on assumed interests rather than inherent traits[6,9]. Algorithmic discrimination typically enters the framework through biased training data or design choices that reproduce historical inequalities[6]. For example, a risk-scoring model in public service provision may inadvertently learn associations between poor language skills and a propensity for fraud, resulting in discriminatory outcomes for migrant populations[10]. Affinity profiling manifests through inference mechanisms like pattern recognition and correlation, which link seemingly neutral data—such as device telemetry or browsing habits—to sensitive attributes like religious beliefs or political orientation[9,11]. These mechanisms allow platforms and municipal systems to implement indirect, group-based treatment without directly identifying the individuals involved, effectively bypassing traditional identification-based legal protections[9]. These theoretical risks translate into concrete real-world manifestations across a variety of high-stakes municipal functions.

### Concrete Manifestations of Algorithmic Harm

Algorithmic discrimination manifests prominently in predictive policing, where biased training data can lead to the over-policing of minority neighborhoods despite similar crime levels across the city[10]. In the welfare sector, fraud detection systems have been documented flagged ethnic minorities for intrusive investigations based on nationality indicators, as seen in prominent scandals in the Netherlands[6]. Affinity profiling manifests through differential treatment based on inferred group status, such as ride-hailing services charging higher surge prices to users with low phone batteries who are assumed to be more desperate for immediate service[11]. In public infrastructure, entry to buildings may be restricted by facial recognition systems that underperform for women and persons of color, leading to misidentification and denial of access to essential services[12]. Furthermore, matching algorithms in public employment agencies have been shown to reproduce gender biases by unfairly favoring male candidates for high-paying roles[6]. These manifestations exploit the high volume and velocity of urban data to implement fine-grained social sorting at scale. Such systemic sorting produces profound and often irreversible impacts on the individuals subjected to this governance model.

The manifestations of algorithmic discrimination and affinity profiling are particularly impactful because they occur within a model that prioritizes immediate, large-scale automation over meaningful human oversight[6]. These real-time decisions can lead to the systemic exclusion of vulnerable groups from essential public services, affecting their access to healthcare, social security, and mobility[6]. Because data collection is pervasive, citizens often have little opportunity for escape or contestation, creating a black box environment where errors compound and self-reinforce through feedback loops[4]. In Algeria, these risks are increasingly relevant as emerging smart cities interface with Law 18-07, which requires reinforced transparency and governance for high-risk processing but may struggle against the extraterritorial reach of global platforms[7]. The reliance on opaque systems threatens the legitimacy of public institutions, especially when automated decisions lack moral sensitivity and exacerbate existing inequalities[13]. Ultimately, these risks threaten not just individual fairness but the legitimacy of AI-driven urban governance itself.

## 2. The Evolution of the Algerian Legal and Institutional Framework for Data Sovereignty

### Constitutional and Primary Legislative Pillars

Algeria's data protection system is fundamentally anchored in the Constitution of the People's Democratic Republic of Algeria (2020), which explicitly establishes the protection of individuals in the processing of personal data as a fundamental right under Article 47[14]. The primary legislative pillar is Law No. 18-07 of June 10, 2018, which regulates the protection of natural persons during data processing to ensure that such activities respect human dignity, privacy, and public freedoms[1]. Oversight of this framework is entrusted to the National Authority for the Protection of Personal Data (ANPDP), an independent administrative body established under the Presidency of the Republic with the mandate to deliver authorizations, receive declarations, and ensure that information technologies do not threaten individual rights[15].

### Strategic and Security Institutional Oversight

This system is supported by a robust hierarchy of auxiliary instruments, beginning with Presidential Decree No. 20-05 (2020), which established a national device for information system security placed under the Ministry of National Defense . This decree created a dual-institutional structure: a National Council, responsible for defining the national security strategy, and an Agency for the Security of Information Systems, tasked with investigating cyber-attacks, mapping classified systems, and certifying electronic signature devices . This security framework is further empowered to require any operator to provide the documentation necessary for its auditing missions[16].

The strategic expansion of this regime continued with Presidential Decree No. 23-314 (2023), which created the High Commission for Digitization (Haut Commissariat à la Numérisation) under the direct authority of the Presidency of the Republic . This body is mandated to design and evaluate the national digitization strategy, ensuring that sectoral plans align with national security requirements while fostering digital sovereignty and the development of national human capital . The High Commission serves as a central hub, presiding over intersectoral projects and coordinating with existing security bodies to harmonize the technological transition with legal standards[17].

The most recent evolution in this comprehensive regime is Presidential Decree No. 25-320 (2025), which introduced the national data governance device. This decree establishes unified mechanisms to organize and exchange data between public administrations and service providers through a National Interoperability System[18]. Central to this device are the classification and cataloging frameworks managed by the High Commission, which define data sensitivity levels and security measures. Under this decree, the National Authority for the Protection of Personal Data (ANPDP) is explicitly tasked with controlling the compliance of data classification to ensure the protection of physical persons remains paramount during inter-institutional exchanges.

Together, these constitutional, legislative, and institutional components form a sophisticated regime designed to balance the accelerating needs of the digital economy with the inviolable right to privacy and national security. By integrating strategic oversight, technical auditing, and interoperability standards, the Algerian framework attempts to create an environment of trust for digital transformation . However, the ultimate efficacy of this system remains anchored in the specific provisions and protections defined in the original 2018 legislation, which continues to serve as the primary legal yardstick for individual rights in the processing of personal data.

### Original Statutory Architecture and Scope

Law No. 18-07, adopted on June 10, 2018, and coming into full force for existing processors by August 10, 2023, provides the foundational rules for the processing of any information concerning an identified or identifiable natural person[19]. Its material scope covers both fully or partially automated processing and manual processing contained within filing systems, while its personal scope extends to any identified data subject whose physical, physiological, genetic, or socioeconomic identity is being handled[1]. The law is built upon core principles including lawfulness and fairness, purpose limitation, data quality (accuracy and relevance), and storage limitation, which dictates that data cannot be kept longer than necessary for its original purpose[20]. Its primary objective is to define the principles and obligations required during the collection and preservation of data, thereby filling a historical legal vacuum in the Algerian context[21]. Notably, the original text excluded data processed for personal or household use, as well as data handled for national defense and security, or for the prevention and prosecution of criminal offenses[1]. This original architecture established a baseline for protection, yet the rapid evolution of the digital landscape necessitated the substantial updates introduced in 2025.

### Modernization and GDPR Alignment

The 2025 amendments, published on July 24, 2025, were enacted to modernize the 2018 framework and align it with international standards like the GDPR, particularly to facilitate international judicial cooperation through bodies such as Eurojust[2]. A major rationale for these changes was the need to provide an adequate legal framework for data exchanged during criminal investigations, which was previously excluded.[2]. Key specific changes include the introduction of mandatory Data Protection Officers (DPOs) for large-scale processing, the requirement for Data Protection Impact Assessments (DPIAs) when processing poses high risks, and a stringent five-day timeline for notifying the ANPDP of data breaches[1]. Furthermore, the amendments added critical definitions for profiling, pseudonymization, and biometric data, while expanding the

ANPDP’s reach through the creation of regional poles for control and audit[1]. These institutional and procedural enhancements were designed to ensure that the Algerian framework could address contemporary challenges like Big Data and cloud-based processing. By modernizing these rules, the amendments sought to bring Algeria’s core data principles into closer proximity with the European regulatory model.

Analysis of the alignment between Law 18-07 (as amended) and GDPR reveals a substantial adoption of the European model’s core principles, specifically the seven principles found in GDPR Article 5[19]. The principles of lawfulness, fairness, and transparency are substantively equivalent to Algerian requirements for express consent and detailed information provided to the data subject[19]. Purpose limitation and data minimization are strictly mirrored in Article 9 of Law 18-07, which demands that data be collected for explicit, legitimate purposes and be adequate, pertinent, and non-excessive[1]. While Law 18-07 includes a right to erasure (Article 35) as a component of rectification, it is conceptually similar to the GDPR’s right to be forgotten, though the Algerian formulation originally focused more on non-compliant or inaccurate data rather than a general right to delete[20]. Significant divergences remain, such as the Algerian framework’s explicit sovereignty clause in Article 44, which allows the State to block transfers if public security or vital interests are threatened, a power more centralized than the GDPR's adequacy-led approach[22]. These principles are made operational through an elaborate enforcement structure designed to ensure compliance across all sectors.

### Enforcement Powers and Remedial Structures

The primary body overseeing compliance is the National Authority for the Protection of Personal Data (ANPDP), established under Law 18-07 Article 22 and made operational through the appointment of its members in 2022[19]. The ANPDP possesses extensive investigative powers, including on-site inspections of processing locations (excluding private homes) and the right to access any document regardless of professional secrecy claims[1]. Its sanctioning competencies allow for the imposition of administrative fines up to 500,000 DA, the issuance of warnings, and the temporary or definitive withdrawal of authorizations[1]. Data subjects are afforded various remedies, including administrative complaints directly to the Authority and the right to seek compensatory damages through judicial action under Article 47 of the Civil Code[20]. The 2025 amendments further decentralize this oversight by authorizing regional delegations for the ANPDP to conduct audits and monitoring across the national territory[1]. While these mechanisms provide a solid foundation for legal certainty, the practical impact of the framework is defined by both its robust protections and persistent structural gaps.

The main strength of the Algerian framework lies in its strong constitutional foundation and the comprehensive 2025 structural updates, such as the mandatory DPO and DPIA requirements, which institutionalize risk-based governance[7]. Foundational protections are delivered through Articles 32-37, which grant users enforceable rights to information, access, and objection, particularly concerning commercial prospecting[1]. However, limitations are evident in the delayed operationalization of the ANPDP, which only began its activities in 2022, several years after the law's adoption[15]. Practical weaknesses also include the difficulty of enforcing these rules against global social platforms that operate extraterritorially and the ongoing challenge of addressing algorithmic opacity in automated decision-making[7]. Experts have noted that while the framework is formally inspired by GDPR, its material effectiveness relies heavily on the ANPDP's future capacity to provide clear, standardized templates for high-risk processing[22]. In conclusion, the current framework offers a solid legal baseline for protection but faces significant implementation hurdles as Algeria transitions toward its Digital Algeria 2030 vision.

## 3. Legal Efficacy and Barriers in Combating Bias within AI-Generated Outputs

### Statutory Safeguards Against Algorithmic Bias

The Algerian legislative framework, primarily through Law 18-07 and its subsequent amendment, establishes several specific provisions to counter the risks of algorithmic discrimination as it was defined earlier.

Relevant provisions within the Algerian legal framework that address these concerns include Article 2, which establishes the general principle that data treatment must respect human dignity, privacy, and public freedoms. Article 3 introduces the legal definition of profiling as any automated use of personal data to evaluate economic status, health, or behavior, which is essential for detecting proxy-based discrimination in urban resource allocation[1]. Article 9 mandates that data must be accurate, complete, and updated, serving as a mechanism to prevent discrimination arising from flawed or biased datasets that might misrepresent specific socio-economic zones[1]. Furthermore, Article 35 grants individuals the right to rectification or erasure of data when processing is not compliant with the law, providing a pathway to challenge biased algorithmic inputs [1]. Article 41 bis requires the designation of a délégué (Data Protection Officer) for high-risk processing, institutionalizing oversight within the entities managing smart city data [1]. Article 45 bis 1 explicitly prohibits judicial or legal decisions from being based solely on automated processing that evaluates a person's personality or behavior [1]. Finally, Article 45 bis 6 requires a mandatory impact study before implementing new technologies that pose high risks to rights and freedoms [1]. These provisions collectively form a regulatory perimeter designed to safeguard the individual against the systemic biases inherent in high-velocity smart city technologies.

The operationalization of these articles ensures that algorithmic discrimination is addressed both directly and indirectly. Articles 2 and 9 function by requiring licit and loyal treatment and high data quality, which prevents the use of proxy variables—such as location data used as a stand-in for race or income—that might inadvertently target specific groups in smart city resource allocation [1]. For instance, a smart grid algorithm that uses geographic data to determine service priority must comply with the Article 9 requirement for relevance, preventing it from discriminating against lower-income districts based on historical consumption patterns. The prohibition of decisions based solely on automated processing under Article 45 bis 1 creates a mandatory human-in-the-loop requirement for decisions producing legal effects, such as the denial of a smart city transit permit or access to automated public services [1]. This preventive effect is reinforced by the ability of data subjects to exercise their right to rectification under Article 35, effectively allowing them to un-bias the datasets that feed predictive urban models. Despite the robustness of these general rules, the framework remains a system of general data protection rather than an AI-specific code, which limits its ability to address the unique complexities of neural networks and deep learning.

### Risk-Based Regulatory Strengths

The Algerian legislative framework possesses specific strengths that provide a targeted defense against algorithmic discrimination. A primary strength is the direct protection found in the non-discrimination principles of the Constitution, which provides a supreme legal basis for Law 18-07's requirement to respect human dignity [1]. Another significant risk-based element is the 2025 introduction of Article 45 bis 6, which mandates a prior study of the impact for treatments involving new technologies likely to cause high risks [1]. This allows the National Authority to audit a smart city AI system before it is deployed, potentially identifying biased outcomes in the simulation phase. Additionally, the triggered right of access under Article 34 enables transparency by requiring the responsible entity to communicate the origin of the data and the purposes of the treatment to the affected citizen[1]. A further strength is the creation of regional poles under Article 27 bis, which decentralizes control and audit functions, theoretically increasing the oversight of localized smart city initiatives across the national territory [1]. These combined elements suggest a proactive rather than reactive stance toward technological harm, yet they are hampered by specific substantive and procedural omissions.

### Substantive Omissions and Procedural Gaps

Critical gaps in the framework remain, most notably the explicit exclusion of data related to defense and national security under Article 6 [1]. This creates a significant blind spot for smart city surveillance systems that may be classified as security tools, potentially shielding them from non-discrimination audits and the oversight of the National Authority. Substantively, there is no explicit prohibition of proxy discrimination, where non-protected attributes are used to target protected groups, a common failure in algorithmic decision-making. Furthermore, while the 2025 amendments introduced profiling, they do not provide an explicit right to an explanation for the specific logic used by an algorithm, unlike international standards such as the GDPR which mandate meaningful information about the logic involved [23]. This lack of transparency regarding the black box of AI makes it difficult for citizens to prove that an automated decision was actually discriminatory in practice. Enforcement weaknesses are also evident, as the National Authority is centralized and may lack the high-level technical expertise required to audit complex smart city architectures, despite the creation of regional poles [1]. These gaps collectively reduce the law's ability to provide a complete shield against the more opaque forms of algorithmic bias.

### Verdict on Practical Effectiveness

The practical effectiveness of Law 18-07 against smart city AI risks—such as discrimination via biased data and opaque decisions—is therefore rated as moderate but critically limited by infrastructure and institutional maturity. While the law mandates data quality and impact studies, the real-world barrier is the technical literacy of the personnel in charge of auditing these systems, a concern raised during parliamentary debates where the need for technical specialization was emphasized[21]. In a practical smart city scenario, such as an AI-driven public health resource distributor, the Article 45 bis 6 impact study might fail if the auditors cannot detect subtle algorithmic biases in the training code [1]. Furthermore, the centralization of the National Authority under the Presidency of the Republic, while providing a safety valve, may slow down the response time required for the fast-moving data streams of an urban digital ecosystem[21]. The resulting effectiveness is negligible in the defense and security sectors where Law 18-07 does not apply, but stronger in administrative and commercial smart city services where the right of access and the presence of a DPO can be actively leveraged by citizens.

In conclusion, the question of whether Law 18-07 adequately addresses algorithmic discrimination in smart cities yields a verdict of partially adequate but structurally insufficient. The 2025 amendments represent a significant leap forward by codifying profiling, mandatory impact assessments, and regional audit poles, which provide the essential legal tools for urban digital governance [1].

However, the broad exclusion of security-related data and the lack of a specific right to algorithmic explanation undermine the practical protection of the citizen in an increasingly surveilled urban environment. The framework effectively sets the standard for loyal data treatment, but it requires further evolution into an AI-specific regulatory regime to match the rapid integration of smart city technologies envisioned in Algeria's 2030 digital transformation strategy[24].

## 4. The Regulatory Struggle Against Indirect Group-Based Sorting and Behavioral Prediction

### Codifying Profiling and Privacy Rights

Relevant provisions within the Algerian legal order begin with the Constitution of 2020, which enshrines the protection of individuals in the processing of personal data as a fundamental right under Article 47[14]. The foundational definition of personal data in Article 3 includes any information relating to a person identifiable indirectly by reference to physiological, psychological, or social identity. The 2025 amendments significantly expanded this scope by introducing an explicit definition of profiling in Article 3, characterized as any form of automated use of data to evaluate or predict aspects of a person's performance, behavior, or movements [1].

Furthermore, Article 18 establishes an a priori prohibition on the processing of sensitive data revealing racial origin or political opinions, which often serve as the hidden targets of affinity-based proxies [1]. For high-risk urban AI, Article 45 bis 6 mandates that the controller perform a mandatory impact assessment when new technologies are likely to engender high risks for rights and freedoms[1]. Procedural safeguards are bolstered by Article 11, which stipulates that no decision producing legal effects can be taken on the sole foundation of an automated processing of data intended to define the profile of the interested party [1].

Finally, Article 36 provides the right to object to processing for legitimate motifs, a vital mechanism for residents to challenge undesirable urban categorization[1]. These specific provisions collectively define the boundaries within which smart city developers must operate to remain compliant with Algerian data protection standards.

The application of these provisions to affinity profiling suggests a framework that is primarily reactive and centered on the individual. Article 3's inclusion of predicted behavior within the definition of profiling directly addresses the preventive mechanisms of affinity mapping, echoing international standards that seek to protect individuals from having their personal preferences or attitudes analyzed through tracking techniques [1,23]. In a smart city context, this would theoretically prevent an automated traffic system from restricting access to certain zones based on an inferred affinity for social unrest without explicit legal authorization. However, the strength of this coverage is mostly indirect; the law focuses on the personal data used to create the group, rather than the group identity itself. While Article 11 restricts automated decisions, its effectiveness depends on proving that the decision was based solely on the AI output, a high evidentiary bar for citizens in a complex urban hierarchy where logic- and knowledge-based approaches may obscure the path to a decision [1,25]. Consequently, the overall coverage strength is moderate, as it relies on broad principles of licit and loyal processing under Article 9 rather than specific restrictions on group-based inferences[1].

### Inference Controls and Preventive Duties

Despite these generalities, the law possesses specific strengths that trigger critical protections against algorithmic sorting. The foremost strength is the Automated Decision Constraint found in Article 45 bis 1, which prevents judicial or administrative decisions from being based on the mere automated evaluation of personality traits [1]. This provides a direct inference control, aligning with the principle that natural persons should be judged on actual behavior rather than AI-predicted characteristics such as nationality or place of residence [25]. A second strength is the Right to Object under Article 36, which allows a data subject to halt the use of their data for prospecting or other illegitimate profiling purposes [1]. Additionally, the mandatory High-Risk Impact Assessment in Article 45 bis 6 serves as a preventive strength by requiring urban authorities to document and mitigate risks to human dignity before deploying affinity-based surveillance tools [1]. This is further supported by the 2025 requirement to appoint a Data

Protection Officer for large-scale processing, ensuring that a specialized professional monitors compliance with internal work procedures and legal obligations[1]. These combined rights and duties create a substantial, albeit fragmented, barrier against the most intrusive forms of urban social sorting.

### The Proxy Data and Inferential Leap Gap

Conversely, the legal framework suffers from explicit gaps and limitations that may render smart city residents vulnerable to proxy-based discrimination. The most serious substantive gap is the absence of specific rules on inferred affinities and proxy-based profiling. Law 18-07, even after the 2025 amendments, does not explicitly address proxy data, where a system uses non-sensitive information (e.g., geolocation) to infer a sensitive attribute (e.g., religious affiliation). While the GDPR provides nuanced guidance on special categories of data and requires informing subjects about the logic of automated processing, Law 18-07 remains critically weak in Article 18, which protects explicit sensitive data but offers no protection against the inferential leap AI makes to recreate those categories through affinities,. Furthermore, the law lacks profiling-specific transparency rules that would require urban authorities to disclose the logic of their affinity groupings to the public, a requirement only partially hinted at in Article 34's right to an intelligible form of data communication. These limitations collectively create a regulatory blind spot where group-based harms can proliferate as long as they do not target a specific, identifiable individual.

### Institutional Maturity and Enforcement Realities

The practical effectiveness of Law 18-07 against these risks is further constrained by the Algerian institutional context. Smart city risks like proxy discrimination require high-level technical auditing, yet the National Authority (ANPDP)—which only installed its members in late 2022 and launched its web portal in 2023—faces challenges in terms of specialized AI expertise and resources for large-scale urban audits[15]. While the Impact Assessment in Article 45 bis 6 is a strong requirement on paper, its practical effectiveness is weak because the law does not provide a clear mechanism for independent third-party verification, often leaving compliance to developers who may not prioritize privacy due to engineering complexities[26]. In a scenario where an Algiers Smart Neighborhood project uses affinity profiling to prioritize utility repairs, the Right to Object in Article 36 may prove negligible for marginalized citizens who lack the legal literacy or political capital to challenge administrative data practices[1]. Algeria's digital maturity is currently focused on the National Strategy for Digital Transformation 2025-2030 and basic ICT infrastructure rather than the granular enforcement of algorithmic fairness, making the track record of rights enforcement against sophisticated AI systems virtually non-existent[24]. The cumulative impact of these institutional and legal shortcomings results in an overall verdict that the law is moderately protective but critically limited in the face of autonomous urban profiling.

In conclusion, the adequacy of Law 18-07 for addressing affinity profiling in smart cities is partially established but remains functionally incomplete. The core protective elements, such as the 2025 definition of profiling and the ban on purely automated decisions, provide a necessary baseline for oversight. However, the manifest insufficiency in addressing proxy categories and the lack of group-harm recognition leave a wide opening for algorithmic biases to influence urban life. The current legal architecture is therefore moderately protective but critically limited, serving as a significant step forward that requires urgent reform to explicitly govern inferred categories and enhance the technical auditing powers of the National Authority[15].

## 5. Holistic Evaluation of Enforcement Realities and International Alignment

### Synthesis of Protective Pillars

The Algerian legislative framework offers a multi-layered defense against the harms of algorithmic discrimination—the biased treatment of individuals through automated systems—and affinity profiling, which involves the categorization of persons based on common traits, interests, or attributes frequently inferred through algorithmic patterns rather than explicit declarations.

The framework's strongest protections are found in the synthesis of the 2018 foundational law and the 2025 enhancements, which are increasingly necessary as developers navigate the engineering complexity of translating vague regulations into technical requirements[26].

The most critical protection is the Automated Decision Constraint under Article 45 bis 1, which mandates human intervention by prohibiting decisions with legal effects from being based *solely* on automated processing that evaluates personality traits, thereby aligning with the principle that natural persons should be judged on actual behavior rather than AI-predicted characteristics [1,25]. This is supported by the Mandatory High-Risk Impact Assessment in Article 45 bis 6, which requires developers to audit technologies likely to endanger rights and freedoms before deployment, addressing systemic biases in the simulation phase[1].

Furthermore, the Right to Object under Article 36 empowers citizens to halt the processing of their data for illegitimate motifs, a vital mechanism for residents to challenge undesirable urban categorization[1]. The framework also relies on the Data Quality Mandate in Article 9, requiring data to be accurate and relevant, which prevents the use of proxy variables—such as location data used as a stand-in for race—that might inadvertently target specific groups in smart city resource allocation.

Finally, the explicit Profiling Definition in Article 3 includes the prediction of behavior and movements, capturing the preventive logic of affinity mapping used in autonomous surveillance.

Collectively, these provisions establish a moderate reactive baseline that prioritizes individual autonomy, though they remain structurally dependent on the institutional bodies charged with their oversight.

### Evaluation of Enforcement Capacity

The primary body responsible for the enforcement of these protections is the National Authority for the Protection of Personal Data (ANPDP), an independent administrative authority functionally attached to the Presidency of the Republic[1]. Formally, the ANPDP possesses a robust suite of enforcement tools, including the power to issue administrative sanctions such as warnings, formal notices, and the temporary or final withdrawal of processing authorizations under Article 46[1]. The 2025 amendments significantly bolstered this capacity by establishing Regional Poles under Article 27 bis, decentralizing audit and control functions to increase oversight of localized digital initiatives across the national territory.

However, the real-world capacity of the ANPDP is currently rated as low to medium; while it has the formal power to impose fines of up to 500,000 DA under Article 47, these amounts are often insufficient to deter large-scale commercial entities. Furthermore, the authority's institutional maturity is still developing, as it only installed its members in late 2022 and launched its digital portal in 2023, following a multi-year period of functional inactivity[15].

Despite the positive development of requiring a Data Protection Officer (DPO) for high-risk processing to ensure specialized professionals monitor compliance with internal procedures, the ANPDP faces persistent barriers in specialized AI expertise and the technical infrastructure needed for large-scale urban audits. Consequently, the overall enforcement capacity is formally sound yet practically constrained by the technical and institutional youth of the Algerian digital regulator.

### Structural and Cultural Implementation Barriers

These enforcement limitations are exacerbated by profound implementation challenges that define the Algerian digital landscape.

The most significant substantive barrier is the National Security Exclusion under Article 6, which removes data related to defense and security from the scope of Law 18-07, potentially shielding intrusive surveillance systems from non-discrimination audits [1].

A second challenge is the Technical Literacy Gap among auditing personnel; parliamentary debates have emphasized that without specialized expertise, auditors may fail to detect subtle algorithmic biases embedded in training code[21].

Furthermore, the Algerian digital strategy, as outlined in the National Strategy for Digital Transformation 2025-2030, remains primarily focused on infrastructure and connectivity—such as high-quality interconnection networks and data center availability—rather than the granular ethical governance of AI systems[24].

This focus on digital maturity over algorithmic fairness creates a cultural environment where privacy may be sidelined for the sake of rapid modernization goals, such as reaching 20% of national GDP through the digital economy[24].

Additionally, the Engineering Complexity inherent in AI systems makes it difficult for developers to translate vague legal principles into technical requirements, a difficulty increased by the lack of practical guidance that considers the technical domain[26].

These challenges collectively result in an implementation environment where the law's protective potential is frequently diluted by structural and technical realities.

### International Standard Convergence and Divergence

To bridge these gaps, the Algerian framework has integrated several GDPR-inspired elements, though their adoption varies in degree and effectiveness. The inclusion of a formal definition of Profiling in Article 3 is a substantial adoption of the GDPR Article 4(4) standard, directly strengthening the legal basis for challenging automated evaluations of personality traits[1,23].

Similarly, the Data Protection Officer requirement in Article 41 bis is a substantial adoption that mirrors GDPR Article 37, ensuring that specialized professionals monitor compliance with internal work procedures [1].

The Mandatory Impact Assessment for high-risk technologies represents a full adoption of GDPR Article 35, providing a proactive mechanism for risk mitigation before deployment [1,23].

However, other elements are only partially adopted or weakened by local context; for instance, while the framework provides for the right to data communication in an intelligible form under Article 34, it lacks the GDPR's explicit Right to an Explanation regarding the specific logic of automated decisions[1,23].

Furthermore, the ban on sensitive data processing in Article 18 lacks the GDPR's nuance regarding proxy data, leaving a regulatory blind spot for AI systems that use non-sensitive inputs (like geolocation) to infer protected attributes[1].

The net effect of this GDPR inspiration is a framework that possesses high-level formal convergence with international standards but lacks the accompanying right to logic necessary to pierce the black box of algorithmic discrimination.

### Integrative Effectiveness Verdict

The overall effectiveness of the framework is determined by the interaction of these three pillars: legal provisions, enforcement capacity, and implementation realities.

The legal provisions are currently moderate, possessing strong language on automated decisions and profiling but failing to address inferred affinities directly.

Enforcement capacity is weak, characterized by a regulator with broad formal powers but limited technical staff and a short track record of rights enforcement since its installation in late 2022[15].

The practical/contextual factors are negligible, as the national focus remains on ICT infrastructure and the localization of personal data repositories rather than the sophisticated auditing of neural networks[24].

These pillars interact negatively; the strong requirement for impact assessments is undermined by the lack of third-party verification power within the ANPDP, while the broad security exclusions in the law amplify the practical vulnerability of citizens in digital urban spaces.

The Algerian legislative framework can therefore be described as having an advanced formal baseline that is systematically undermined by institutional immaturity and technical gaps. The decisive limiting factor is the lack of specialized AI auditing expertise, which prevents the conversion of legal rights into technical constraints.

In addressing the extent of protection against algorithmic harms, the Algerian legislative framework is partially adequate but critically limited.

## 6. A Strategic Roadmap for Closing Structural Voids through Legislative and Technical Reform

The analysis of the Algerian legislative framework identifies several critical gaps that currently facilitate algorithmic harms within the urban digital landscape.

First, The National Security Exclusion in Article 6 creates a significant regulatory gap by exempting defense and security data from Law 18-07, which effectively shields facial recognition and smart city surveillance from ANPDP oversight while simultaneously stripping away the non-discrimination audits necessary to prevent unchecked algorithmic bias[1].

Second, the absence of proxy-based anti-discrimination rules allows AI systems to use neutral variables, such as geolocation or device telemetry, to infer protected traits like religious affiliation or socioeconomic status, leading to both algorithmic discrimination and affinity profiling while appearing formally compliant with Article 18[1,9].

Third, the framework lacks an explicit Right to an Explanation, which prevents residents from understanding the black box logic of automated decisions that produce legal effects, such as the denial of welfare or transit access[6].

Fourth, a profound technical expertise gap within the National Authority (ANPDP) undermines the efficacy of mandatory impact assessments, as personnel may lack the literacy required to detect subtle biases embedded in complex training code, often struggling with the engineering complexity where developers find vague regulations difficult to translate into technical requirements[21,26].

Fifth, the exclusion of inferred affinities ensures that the law remains centered on identified individuals rather than the collective, group-based sorting that characterizes autonomous urban governance[9].

Finally, the infrastructure-centric focus of the 2030 Digital Strategy prioritizes 5G and data center availability over the granular ethical governance of AI, resulting in an implementation environment where privacy is secondary to rapid modernization goals[24].

These gaps reveal a cumulative pattern where the formal adoption of Law 18-07 is decoupled from the technical and operational reality of AI, necessitating a structured categorization of these voids to prioritize reform.

### Proposed Legislative and Institutional Reforms

To bridge these gaps, legislative reforms should prioritize an Explicit ban on proxy-based affinity profiling, directly amending Article 18 to prohibit the use of non-sensitive data to infer protected characteristics such as racial origin or religious beliefs.

Drawing inspiration from GDPR Article 22, the framework should Codify the Right to an Explanation, requiring urban authorities to provide meaningful information about the logic involved in any automated decision that produces legal effects for a resident [23].

To address the security blind spot, the government should Amend Article 6 to mandate independent human rights audits for security-related AI, ensuring that surveillance tools remain subject to the core non-discrimination principles of the Constitution.

Institutionally, the Algerian executive should Establish a Specialized AI Audit Unit within the ANPDP, staffed by data scientists to overcome the technical literacy gap identified in parliamentary debates[21].

Furthermore, a Mandatory Third-Party Verification process for DPIAs should be instituted for high-risk smart city projects to prevent developers from self-approving biased systems due to engineering complexities[26].

If these targeted reforms were adopted, the Algerian framework would shift from a general data protection code to a functional regime capable of governing the unique risks of autonomous urban systems.

### Operational Capacity and Public Awareness

Complementary non-legislative improvements should focus on Institutional capacity building through technical workshops for ANPDP personnel and the judiciary on detecting algorithmic bias, addressing the technical literacy gap[13].

To support the private sector and public agencies, the ANPDP should Develop National AI Auditing Guidelines that translate the vague requirements of Article 9 into concrete technical standards for data minimization and relevance in smart cities [1].

In terms of Awareness and Education, the Ministry of Post and Telecommunications should lead public campaigns to inform citizens of their Right to Object under Article 36, specifically regarding the use of their data for urban social sorting [1].

Furthermore, International cooperation with bodies like the European Data Protection Board (EDPB) should be prioritized to share best practices for cross-border enforcement against global platforms that operate extraterritorially[2].

Finally, the state should sponsor AI Ethics Pilot Projects in emerging technological poles like Sidi Abdallah to test the efficacy of the Data Protection Officer mandate in real-world urban scenarios.

These measures complement legislative reforms by providing the operational expertise and public legitimacy necessary for effective overall protection.

### Feasibility and Impact Analysis

The feasibility and expected impact of these measures in the 2026 Algerian context are summarized as follows.

First, the Codification of the Right to an Explanation is highly feasible as it aligns with the 2025 goal of international harmonization and would significantly empower data subjects to pierce the AI black box[2] .

Second, the Explicit ban on proxy-based profiling would close the most critical loophole in Law 18-07, though it requires precise legal drafting to avoid stifling legitimate urban analytics.

Third, the Establishment of a Specialized AI Audit Unit is essential to overcome the technical expertise gap, but its success depends on the state's ability to recruit and retain high-level data scientists[21].

Fourth, the Development of Technical Auditing Guidelines is a low-cost, high-feasibility measure that would help developers manage the engineering complexity of AI-driven governance[26].

Finally, Amending Article 6 for Security Audits faces significant political hurdles due to the primacy of national security in the Algerian legal tradition, yet it remains the only way to eliminate the most dangerous regulatory blind spot.

This reform package possesses the realistic potential to meaningfully strengthen the framework by transitioning the Algerian digital landscape toward substantive algorithmic accountability.

## Conclusion: The Pathway to Accountable Governance

In conclusion, the core problem is the current framework's inadequate protection against algorithmic discrimination and affinity profiling in smart cities, caused by systemic gaps in proxy data oversight and a critical technical auditing deficit.

The solution pillars include targeted legislative amendments to codify the right to explanation and ban proxy-based profiling, coupled with essential non-legislative capacity building for the ANPDP and urban developers.

The recommended pathway forward is to first pass urgent legislative amendments to set a clear ethical standard, followed by the recruitment of specialized technical audit personnel, and finally the adoption of granular guidelines for smart city implementation.

This sequence is justified because legislative clarity is a prerequisite for enforcement, and institutional capacity must be established before technical guidelines can be meaningfully monitored.

The realistic prospect of achieving meaningful protection is high if this full pathway is followed, as it leverages the 2025 modernization momentum to close the final gaps in Algeria's digital sovereignty.

## Bibliography

1. *Algerian Law No. 18-07 of June 10, 2018, as Amended and Supplemented by Law No. 25-11 of July 24, 2025 Relating to the Protection of Physical Persons in the Processing of Personal Data*; 2018;
2. People's National Assembly Presentation and Discussion of the Bill Amending and Supplementing Law No. 18-07 Relating to the Protection of Natural Persons in the Processing of Personal Data 2025.

3. Kitchin, R. The Real-Time City? Big Data and Smart Urbanism. *GeoJournal* **2014**, *79*, 1–14, doi:10.1007/s10708-013-9516-8.
4. Rob Kitchin *Getting Smarter about Smart Cities: Improving Data Privacy and Data Security*; National Institute for Regional and Spatial Analysis (NIRSA), Maynooth University, 2016;
5. menasria, samiha Constitutional Governance of Artificial Intelligence -A Foresight Vision for the Algerian Case-. *مجلة دراسات اقتصادية* **2025**, *19*, 192–205.
6. Raphaële Xenidis LEGAL PROTECTION AGAINST ALGORITHMIC DISCRIMINATION IN EUROPE.
7. BOUTEMEDJET, D. Testing Algeria’s Data Protection Framework Against Social Networks and Big Data. *مجلة الفكر القانوني والسياسي* **2025**, *9*, 1295–1311.
8. *Governing Smart Cities as Knowledge Commons*; Frischmann, B.M., Madison, M.J., Sanfilippo, M.R., Eds.; 1st ed.; Cambridge University Press, 2023; ISBN 978-1-108-93853-2.
9. Wachter, S. Affinity Profiling and Discrimination by Association in Online Behavioural Advertising. *SSRN Electron. J.* **2019**, doi:10.2139/ssrn.3388639.
10. Saar Alon-Barkat; Madalina Busuioc; Kayla Schwoerer; Kristina S Weißmüller Algorithmic Discrimination in Public Service Provision: Understanding Citizens’ Attribution of Responsibility for Human versus Algorithmic Discriminatory Outcomes. *J. Public Adm. Res. Theory* **2025**, *35*, 469–488, doi:10.1093/jopart/muaf024.
11. Li, Z. Affinity-Based Algorithmic Pricing: A Dilemma for EU Data Protection Law. *Comput. Law Secur. Rev.* **2022**, *46*, 105705, doi:10.1016/j.clsr.2022.105705.
12. Hacker, P.; Neyer, J. Substantively Smart Cities – Participation, Fundamental Rights and Temporality. *Internet Policy Rev.* **2023**, *12*, doi:10.14763/2023.1.1696.
13. Murikah, W.; Nthenge, J.K.; Musyoka, F.M. Bias and Ethics of AI Systems Applied in Auditing - A Systematic Review. *Sci. Afr.* **2024**, *25*, e02281, doi:10.1016/j.sciaf.2024.e02281.
14. Constitution of the People’s Democratic Republic of Algeria.
15. Guettal, R.; Benkaddour, M.K. A TAILORED COMPLIANCE SOLUTION FOR SECURING PERSONAL DATA PRIVACY UNDER LAW 18-07 IN ALGERIA.
16. Ethania, A.J. *Presidential Decree No. 20-05 setting up a national device for the security of information systems.*; 2020;
17. *Presidential Decree No. 23-314 Establishing the High Commission for Digitization, Its Organization, and Its Functioning*; 2023;
18. مرسوم رئاسي 25-320 منظومة وطنية لحوكمة البيانات.
19. Imad, C. The Protection of Personal Data in Algeria: Between Local Challenges and International Standards. *Pak. J. Life Soc. Sci. PJLSS* **2024**, *22*, 18200–18215, doi:10.57239/PJLSS-2024-22.2.001329.
20. ouafi, hadja The Right to Be Forgotten in Digital Media -A Study within the Framework of the European Union and Algerian Law-. *Rev. Sci. Hum.* **2025**, *36*, 335–346.
21. People’s National Assembly Presentation and Discussion of the Bill Relating to the Protection of Natural Persons in the Processing of Personal Data 2018.
22. BOUTEMEDJET, D.; Kamel, ◌َa.K. Comparing Algeria’s Personal Data Transfer Rules with General Data Protection Regulation. *مجلة الاستاذ الباحث للدراسات القانونية والسياسية* **2025**, *10*, 934–961.
23. *REGULATION (EU) 2016/ 679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - of 27 April 2016 - on the Protection of Natural Persons with Regard to*

*the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/ 46/ EC (General Data Protection Regulation)*;

24. High Commission for Digitalization (HCN); Presidency of the Republic National Strategy for Digital Transformation in Algeria 2025-2030 2024.
25. *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)Text with EEA Relevance.*;
26. Aljeraisy, A.; Barati, M.; Rana, O.; Perera, C. Privacy Laws and Privacy by Design Schemes for the Internet of Things: A Developer's Perspective. *ACM Comput. Surv.* **2022**, *54*, 1–38, doi:10.1145/3450965.