

Testing Algeria's Data Protection Framework Against Social Networks and Big Data

إختبار الإطار القانوني الجزائري لحماية البيانات في مواجهة شبكات التواصل
الاجتماعي والبيانات الضخمة

Boutemedjet djalel*, faculty of law, Algiers university 1
faculty of law and political sciences
university Mohamed cherif messaadia - Souk Ahras-
jboutemedjet@gmail.com

Received: 20/10 /2025

Accepted: 31/10 /2025

Published: 29/11 /2025

Abstract

Social networks rely on a data-driven business model that challenges traditional privacy protections. This article evaluates the effectiveness of Algeria's data protection framework (Law 18-07 of 2018, updated by Law 25-11 of 2025) in the context of digital platforms and Big Data. Through doctrinal and comparative analysis (GDPR, Convention 108+), it reviews key principles lawfulness, transparency, purpose limitation, minimisation, and security as well as enhanced governance (ANPDP powers, DPO duties), breach notification, and cross-border data transfer rules. The study highlights strengths such as clear scope, risk-based duties, and stronger enforcement, but identifies gaps regarding large-scale consent validity, opacity and bias in automated profiling, extra-territorial enforcement, and weak DPIA implementation for cloud processing. It proposes an assessment grid, a transfer decision tree, and a practical compliance roadmap for controllers. Finally, it recommends clearer profiling guidance, DPIA templates, and improved international cooperation to ensure effective protection through risk-based governance.

Keywords: social networks; Big Data; profiling and automated decisions; breach notification; digital sovereignty.

Introduction:

Social networks have become the world's default conversational infrastructure, where individual expression, algorithmic mediation, and attention markets converge. Their data-intensive business model optimising engagement and monetising behavioural signals blurs boundaries between private and public spheres and strains legal intuitions forged in the pre-platform era¹.

Algeria has adopted a dedicated framework to rebalance this environment by articulating core principles (lawfulness, transparency, purpose limitation, data minimisation, storage limitation), technical and organisational safeguards, and clear roles and responsibilities for controllers and processors². The 2025 reforms further tightened the regime by strengthening supervisory powers, clarifying breach-notification duties, and institutionalising risk-based governance tools such as data-protection officers for large-scale processing³. Because global platforms target Algerian users and routinely process data across borders and clouds, Algeria's rules necessarily interface with external regimes most

* Corresponding Author

"Testing Algeria's Data Protection Framework Against Social Networks and Big Data"

prominently the EU General Data Protection Regulation, given its mature toolbox, extraterritorial logic, and jurisprudential footprint⁴.

This legal architecture is anchored in constitutional guarantees protecting fundamental rights and human dignity, which orient statutory interpretation toward a rights-based approach to personal-data processing⁵.

At the same time, the platform context is inseparable from the logics of Big Data. The well-known "5Vs" volume, velocity, variety, veracity, and value disrupt purpose predictability and complicate consent renewal, especially when new inferences are drawn from seemingly innocuous signals (engagement metrics, device telemetry). Effective protection therefore requires design-level interventions: granular, renewable consent pathways; user-centric controls over ranking and ad relevance; audit trails for automated decisions; and periodic re-identification testing integrated into privacy-engineering lifecycles⁶.

Because social-platform processing chains span hyperscale cloud and global content-delivery networks, any national regime must connect its transfer rules to interoperable concepts of adequacy, safeguards, and narrow derogations, as reflected in the modernised Council of Europe framework⁷. Clarity about responsibilities within complex processing chains also depends on robust controller/processor delineation and practical guidance for joint-operations typical of platform ecosystems⁸. Finally, a durable privacy architecture should be evaluated against deeper structural risks in platform capitalism information and power asymmetries and the normalisation of surveillance calling for a normative theory of privacy that centres dignity and autonomy⁹.

This article tackles a central tension: whether Algeria's 18-07/25-11 framework, when applied to social-network ecosystems and Big Data practices, can deliver effective protection for Algerian users. It examines the real-world validity of consent and transparency at platform scale, the adequacy of safeguards for profiling and other automated decision-making with significant effects, the robustness of security and breach-notification duties in cloud-first environments, and the enforceability of international-transfer restrictions across distributed processing chains. Moving beyond textual compliance, the analysis "pressure-tests" obligations against common platform features engagement-based recommendations, targeted advertising, frictionless sharing, and third-party integrations to translate legal principles into auditable controls. The article is structured as follows: Part I maps the Algerian framework its scope, concepts, principles, and institutional design; Part II analyses platform ecosystems, data typologies, and legal/security risk clusters, including automated decision-making and profiling; Part III assesses Big Data's impact on rights and enforcement, from re-identification risk to cloud processing and cross-border cooperation; Part IV identifies convergences and gaps vis-à-vis GDPR and Convention 108+ with operational takeaways; and Part V proposes a compliance roadmap for controllers operating in or targeting Algeria, covering governance, DPIA patterns for social features, transfer governance, and breach-notification playbooks, before concluding with policy recommendations on guidance for profiling/ADM, DPIA templates calibrated to platform risks, and mechanisms to strengthen cross-border enforceability. Methodologically, we combine a doctrinal reading of Algerian instruments (to extract scope, definitions, principles, security, transfers, and supervisory levers), structured comparative benchmarking used sparingly to illuminate open-textured notions (targeting, controller/processor delineation, transfer safeguards) without importing foreign rules, and operationalisation via scenario testing to produce implementable artefacts (effectiveness assessment grid, transfer decision tree, DPIA patterns, breach playbook), under

"Testing Algeria's Data Protection Framework Against Social Networks and Big Data"

a strict citation discipline across the paper. The contributions are fourfold: doctrinal clarity tailored to platform realities; an interoperability-aware synthesis for transfer governance aligned to cloud/data-flow constraints; legal-engineering artefacts to bridge policy and implementation; and a policy and research agenda prioritising guidance on profiling/ADM and re-identification testing, protections for minors, and an empirical programme on cross-border enforceability and the operational burden of DPIA practice.

1- Algerian Legal Framework & Core Concepts

1.1- Scope (material/territorial): art. 2; targeting users in Algeria

Material scope: Algeria's data protection regime applies to any operation performed on personal data relating to natural persons, whether automated or not, and thus captures the full platform lifecycle from account creation and social-graph construction to telemetry, ad-delivery logs and moderation records.

Territorial scope: While jurisdiction is rooted in national territory, the law extends to processing performed outside Algeria when services target or monitor individuals in Algeria; functional indicators include localisation (Arabic/French), marketing and campaigns directed at Algerian audiences, pricing or customer support adapted to Algerian users, and systematic monitoring of behaviours in Algeria.

On/off-shore chains: Cloud-first architectures (local collection; regional enrichment; multi-region storage/CDN) do not displace Algerian law when Algerian users are in scope; they instead trigger parallel duties under transfer rules and cooperation pathways. Algerian scholarship reading the law's reach stresses practical evidence product design, terms, cookies/SDKs and urges controllers to maintain jurisdictional rationales and data-flow maps demonstrably linking features to Algerian users.

Material scope: Algeria's regime covers any operation on personal data relating to natural persons, automated or not, which applied to social platforms extends from account creation and graph construction to telemetry, ad-delivery logging, and moderation archives. Territorial scope. Although rooted in national jurisdiction, the framework functionally reaches processing carried out abroad when services target or monitor individuals in Algeria; practical indicators include Algeria-facing UX/localisation, campaigns and customer support oriented to Algerian users, or systematic monitoring of behaviour within Algeria. On/off-shore chains: Cloud-first architectures (local collection, regional enrichment, multi-region storage/CDN) do not displace Algerian law when Algerian users are in scope; rather, they trigger transfer safeguards and cooperation mechanisms. Interoperability matters, because the most frequent cross-border touchpoints for platforms align with widely used concepts (adequacy, safeguards, narrow derogations) developed in European instruments and commentary that can illuminate Algerian practice without supplanting it¹⁰.

Targeting tests and evidence: Platforms should maintain records showing why they consider themselves in scope (or not): user-base metrics from Algeria, locale toggles, marketing buys, SDK/cookie footprints, and monitoring practices. In distributed data-sharing ecosystems, documenting purpose, legal basis, and safeguards for onward flows is essential to reconcile innovation with accountability. Cross-border data-access and reuse debates underscore that controllers must map data recipients and purposes, and pre-commit to risk-based safeguards appropriate to the processing context. Where product design intersects with public discourse (e.g., recommendation ranking that amplifies political messaging), governance should anticipate manipulation risks alongside privacy duties and rights handling¹¹.

"Testing Algeria's Data Protection Framework Against Social Networks and Big Data"

1.2- Definitions (art. 4): personal data, sensitive data, processing, controller/processor, consent

Personal data: An effects-oriented definition any information identifying or making an individual identifiable comfortably includes platform IDs, device identifiers, location traces, behavioural signals, and *inferred* attributes (interests, propensities, risk scores).

Sensitive data: Heightened restrictions attach to categories such as health, biometrics, religion, political opinions, or union membership; platform pipelines can implicate these both directly (uploads, transcripts) and indirectly via inference. Processing. Collection, recording, structuring, storage, retrieval, transmission, dissemination, and erasure cover the full lifecycle, including ranking logs and ad-delivery events.

Controller/processor: Controllers determine purposes and essential means; processors act under documented instructions with security, sub-processor control, and auditability.

Consent: At platform scale, valid consent must be specific, informed, and freely given, with granular choices and renewal points; bundled or pre-ticked flows are insufficient. Comparative doctrine supports treating linkable inferences as personal data and urges clarity in joint operations (plug-ins, brand pages) with visible redress channels for data subjects¹².

Role delineation and joint controllership: Social ecosystems rarely fit clean binary roles. Joint design and co-determination of purposes (e.g., integrated analytics/ads or embedded social widgets on third-party sites) may trigger shared responsibility; transparent allocation of duties, user-facing contacts, and liability is indispensable.

Vulnerable groups: Where minors are concerned, consent and transparency require heightening (age-appropriate notices, profiling opt-outs, marketing limits).

Cross-cutting practice: A "definitions register" that maps product artefacts (signals, IDs, logs, embeddings) to legal categories helps avoid "category drift" during agile releases. For explainability and rights exercises, comparative manuals provide workable patterns to turn abstractions (fairness, transparency) into actionable notices, portability workflows, and proportionality analysis for high-risk features¹³.

1.3- Principles: lawfulness, fairness, transparency; data minimisation, purpose limitation, storage limitation; security (art. 38)

Lawfulness, fairness, transparency: Each feature should be tied to a legal basis (consent for personalised ads; contract for core messaging; legitimate interest for basic security), articulated via layered, intelligible notices that describe key signals and user controls.

Data minimization: Telemetry and logs must reflect strict necessity; "collect now, figure out later" is hard to defend without a proportionality analysis and a DPIA calibrated to actual risk.

Purpose limitation: Repurposing (e.g., using UGC to train recognition models) requires a compatibility test and often renewed consent.

Storage limitation: Retention schedules should align with feature lifecycles (ephemeral stories vs. account-security logs), with automatic deletion and crypto-erasure where feasible. Comparative doctrine on minimisation and privacy-by-design helps convert principles into engineering constraints and review gates embedded in product pipelines¹⁴.

Security (art. 38) and incident readiness: Risk-appropriate technical and organisational measures include encryption in transit/at rest, credential hygiene, segregation of duties, rate-limiting for APIs, differential access to training data, reproducible model deployment, and continuous testing/monitoring. Controllers should maintain severity matrices, forensics playbooks, and communications templates for breach notifications, and run periodic re-identification tests on derived datasets used for targeting or recommendations. For transfer-

"Testing Algeria's Data Protection Framework Against Social Networks and Big Data"

heavy stacks, vendor contracts must bind sub-processors (confidentiality, security, audit rights), and change-control should trigger impact assessment and, where relevant, user-facing transparency. Handbooks and practitioner texts provide baseline controls, contract clauses, and DPIA patterns that can be adapted to social features and cloud telemetry flows¹⁵.

1.4- Governance & powers: ANPDP (arts. 23+), 25-11 reinforcements (inspections, notifications to prosecutor), DPO for large-scale processing, records and internal policies

Supervision and enforcement: The National Authority's inspection powers, including on-site access and data review notwithstanding professional secrecy, require controllers to sustain *audit-ready* governance: processing registers, vendor inventories, sub-processor change control, and DPIA repositories aligned with platform features.

25-11 reinforcements: Amendments strengthen oversight via explicit breach-notification duties to the authority and to affected individuals within defined timelines, broaden inspection levers, and formalise referrals to the public prosecutor when potential criminal offences are detected.

DPO: Controllers engaged in large-scale or high-risk processing must designate an independent Data Protection Officer with sufficient expertise and access to leadership, tasked with advising on DPIAs, training, and monitoring compliance; comparative analysis highlights the DPO's ambiguous yet pivotal role and the need to ensure independence in practice.

Records & internal policies: Governance artefacts should document minors' safeguards, profiling redress, and ADM testing (bias/robustness), and include cooperation bundles (evidence packs) to support cross-border oversight and user redress. The statutory baseline and comparative doctrine together frame an accountability-first posture for platforms operating in or targeting Algeria¹⁶.

2- Social Platforms: Ecosystem, Data Typologies, and Risks

2.1- Platform ecosystem: profiles, social graphs, UGC, behavioural signals, targeting

Social platforms combine user profiles, social graphs, user-generated content (UGC), and continuous streams of behavioural signals into large, tightly coupled data ecosystems. Profiles begin as account identifiers but quickly accrete attributes drawn from device telemetry, location, interaction history, and content semantics. The social graph edges among accounts structures reach and relevance, enabling diffusion, community detection, and targeted delivery. UGC supplies the raw material for engagement metrics that drive recommendation loops, while behavioural signals (views, watch time, reactions, dwell, scroll velocity) supply the feedback necessary to optimise ranking and advertising. In practice, recommendation and ad-tech stacks operate as layered pipelines: intake and parsing; feature extraction; model training and inference; and delivery with A/B controls. Each layer both consumes and emits personal data, including *derived* representations such as embeddings or audience segments that in turn feed ranking and targeting decisions¹⁷.

The "socialness" of these systems matters for privacy and governance because the value of a single datum is amplified by context. A photo becomes a location trace when geotagged; a like becomes a political signal when clustered; an innocuous follow becomes a proxy for health or religious inference when combined with community membership. The graph thus multiplies identifiability by enabling correlation, while the feed's ranking logic optimised for engagement can systematically privilege content that elicits strong reactions, reinforcing data collection and exposure. These dynamics blur boundaries between public

"Testing Algeria's Data Protection Framework Against Social Networks and Big Data"

performance and private life: features marketed as community-building also normalise pervasive observation and analysis of interpersonal behaviour, often beyond what users reasonably anticipate¹⁸.

2.2- Data typology

Account identifiers: Account creation requires identifiers (username, email/phone, device IDs) that anchor identity resolution across sessions and devices. Even where platforms discourage real-name policies, persistent identifiers enable longitudinal profiling and cross-service linkage.

Sensitive data: Sensitive attributes may be supplied directly (bio fields, images, audio) or inferred from language, networks, or routines. The risk lies not only in explicit collection but also in the ease with which classification systems generate proxies (e.g., political leaning inferred from follow graphs or viewing patterns).

Usage & interaction data: Clicks, impressions, watch time, hover, and search queries provide continuous telemetry that is indispensable to ranking yet overbroad for ancillary purposes if not constrained by minimisation.

UGC (IP vs privacy): UGC intertwines copyright and personality rights: creators retain IP interests while appearing in content implicates others' privacy, especially when re-shared beyond the original context.

Derived/inferred data: Embeddings, topic vectors, and audience segments are routinely treated as internal analytics, but when tied to an account they remain personal and trigger purpose-limitation and access/objection rights; their opacity raises distinct governance problems¹⁹.

The typology above is not exhaustive but emphasises how categories interact. Derived data can be more sensitive than source data because they compress, extrapolate, and predict: a short watch history becomes a high-confidence interest label; a handful of connections becomes a community assignment; a pattern of late-night usage becomes a risk score. These transformations complicate consent and transparency: interfaces ask for agreement to "improve services," yet the operational reality is a continuous, model-driven expansion of use cases. As governance scales, controllers should maintain a living "definitions register" that maps product artefacts (signals, embeddings, logs) to legal categories, keeps track of legal bases per use, and flags when a new modelling approach effectively changes purpose. Comparative privacy scholarship shows that institutional choices policies, oversight networks, and soft-law guidance shape how such borderline practices are interpreted and enforced across borders, which is especially salient for platforms that operate transnationally²⁰.

2.3- Legal risks: privacy, defamation/e-reputation, copyright, criminal liability, public order

Privacy infringements: Unbounded secondary use, excessive telemetry, and opaque inferences expose controllers to claims of unlawful processing and inadequate transparency, particularly where profiling materially affects users.

Defamation and e-reputation: Virality and permanence (screenshots, mirrors, caches) magnify harms from false statements; intermediaries face notice-and-takedown duties and must balance swift remediation against risks of over-removal.

Copyright: UGC re-use in compilations, reaction videos, or training datasets raises licensing questions; platform terms cannot extinguish non-waivable rights, and automated moderation must be calibrated to avoid systematic false positives.

"Testing Algeria's Data Protection Framework Against Social Networks and Big Data"

Criminal content and public order: Illegal incitement, hate speech, non-consensual intimate imagery, and doxxing engage criminal law; predictive moderation and friction in resharing can mitigate spread but must be accompanied by due-process-compatible appeal routes. The throughline is accountability: platforms must tie each risk to governance artefacts registers, DPIAs, incident playbooks and measurable controls in ranking, recommendations, and reporting funnels²¹.

2.4- Security risks: social engineering, inadvertent exfiltration, extortion, tracking/correlation

Social engineering: Public profile breadcrumbs (workplace, routines, contacts) enable spear-phishing and account takeover; verification badges and DM trust heuristics are routinely spoofed.

Inadvertent exfiltration: Photos and screen recordings can leak confidential information (badges, dashboards, customer data); creators' studios and livestreams are frequent vectors.

Extortion: Attackers leverage compromising content (real or fabricated via deepfakes) to coerce payments or further access.

Tracking and correlation: Ad and analytics beacons, device fingerprints, and cross-app identifiers create shadow profiles that persist even after account deletion; third-party SDKs can enable off-platform tracking beyond user expectations. Case studies in Big Data environments highlight how scale and heterogeneity of datasets stress traditional controls; practical mitigations include reducing identifier stability, sandboxing third-party SDKs, enforcing strict purpose boundaries on telemetry, and red-teaming cross-linkage attacks²².

2.5- Automated decisions & profiling: significant effects, safeguards, user information

Automated decisions in feeds and ads increasingly determine what users see, whom they connect with, and what economic opportunities reach them. *Significant effects* include eligibility or visibility impacts de-ranking, demonetisation, age-gating, or ad exclusion that indirectly affects access to jobs, housing, or credit. Safeguards therefore require layered transparency (signals used; controllable settings), meaningful contestation (appeal routes with evidence trails), and accountable experimentation (A/B tests with guardrails on discrimination). The opacity of machine learning complicates these duties: model weights and training corpora are not inherently interpretable, and post-hoc explanations may be partial or misleading. Governance should pair *ex ante* design reviews (feature gating, fairness testing, DPIA) with *ex post* audits that compare outcomes across groups and time; user-facing notices should describe logic at a level that allows informed choice without exposing attack surfaces²³.

The debate over a "right to explanation" shows why procedural safeguards must focus on outcomes as well as process. Detailed algorithmic disclosures are often neither feasible nor sufficient; affected users need actionable levers access to relevant data, clear objections to profiling for marketing, and timely review of adverse decisions. Legal-engineering responses include constrained feature sets for high-risk contexts (e.g., minors), default opt-outs from sensitive inferences, and sandboxes for auditing recommendation changes before full rollout. Scholarship cautions that explanation rights, narrowly conceived, may create false comfort; effective remedies require contestability, evidence preservation, and supervisory access to models and data when warranted²⁴.

Operational guidance from supervisory bodies and academic analysis recommends translating abstract duties into product requirements and metrics: define "materiality" thresholds for profiling effects; log rationales for rank changes that produce visibility or

"Testing Algeria's Data Protection Framework Against Social Networks and Big Data"

monetisation impacts; maintain bias dashboards; and schedule periodic re-identification tests for derived datasets. Where joint operations occur (publishers, advertisers, analytics vendors), parties should agree *ex ante* on role allocation, user-facing contacts, and audit rights, and should document contestation workflows that do not strand users in jurisdictional gaps. The evolving guidance on automated decision-making underscores the need to separate explanation (what signals matter) from justification (why the outcome is lawful and fair), and to furnish both at appropriate abstraction levels²⁵.

Finally, platform governance must be iterative. Transparency and accountability are not one-time disclosures but continuous practices that accompany model updates, new signals, and shifting community norms. A credible approach pairs internal assurance (DPIAs tied to feature flags, fairness gates in CI/CD, adversarial testing of correlation risks) with external accountability (public documentation of profiling categories, researcher APIs with privacy-preserving safeguards, and structured engagement with civil society and regulators). Emerging work on transparency and accountability frameworks in AI provides a vocabulary for these practices and emphasises organisational capacity roles, training, escalation paths as much as technical tooling. For social platforms operating in or targeting Algeria, this means treating automated decision-making as a *regulated system* across its lifecycle, with user-centric controls and auditable evidence at every stage²⁶.

3- Big Data: Impact on Rights and Enforcement Challenges

3.1- Big Data specifics (5Vs) and their effect on purpose predictability

Big Data in social platforms means high-volume, high-velocity, high-variety streams that are imperfect in veracity yet rich in extractable value. These "5Vs" collide with classic privacy architecture by making *purposes* fluid: the same log line that supports fraud detection today becomes a high-confidence interest signal tomorrow; the embedding that improves content ranking in one cohort becomes a proxy for sensitive traits when correlated with a different label set. Purpose predictability erodes because scale invites repurposing; pipelines are designed for extensibility (feature stores, model registries), so the path of least resistance is to reuse data rather than recollect it with fresh justification. The practical consequence is that controllers must design governance *into* data and model lifecycles declaring purposes at the dataset and feature level, gating expansions through compatibility tests, and scheduling periodic re-evaluation when new correlations appear or when models drift. Without such guardrails, the default trajectory of Big Data systems is accretive: more signals, more joins, more inference, and progressively less transparency for users and auditors²⁷.

Purpose drift is not only technical but organisational. Product teams rewarded for engagement or growth will naturally press for broader data access and longer retention; security and compliance teams, tasked with minimisation and storage limitation, can become outvoted unless decision rights are formalised. A credible response links the "5Vs" to governance thresholds: when *volume* crosses a defined limit, require a DPIA refresh; when *velocity* increases (e.g., real-time inference), require tightened access controls and human-in-the-loop checkpoints for high-impact decisions; when *variety* expands (e.g., adding biometric or geolocation signals), trigger compatibility testing and explicit user notices; when *veracity* is uncertain (noisy or biased data), enforce model-risk reviews; when *value* is newly extracted (a novel downstream use), revisit legal bases and user choice.

3.2- Consent in data-massive contexts: limits of blanket consent; granular/renewable consent

At platform scale, blanket terms cannot plausibly deliver informed, specific consent for evolving analytics and inference. Interfaces that bundle many purposes under "improve

"Testing Algeria's Data Protection Framework Against Social Networks and Big Data"

service" mask material differences between core functions (message delivery) and optional features (behavioural ads, third-party measurement). A rights-compatible pattern is granular and renewable consent: unbundle high-impact purposes; expose toggles in context (at the moment data is collected or used); renew consent when purpose or risk materially changes; and provide logs so users can see when and why a setting was flipped. Controllers should also separate "necessary for service" from "personalisation" and "research/quality," with purpose-scoped retention by default. Social research on Big Data's societal impacts supports these design choices: users' expectations and perceived legitimacy hinge on *control*, *context*, and *feedback* not on one-off, longform policies that are rarely read²⁸.

3.3- Anonymisation/pseudonymisation & re-identification risk

De-identification is not a binary state but a moving target. Pseudonymous identifiers (device IDs, hashed user keys, stable embeddings) offer only thin protection when datasets can be joined; even "anonymous" aggregates may re-identify once linked with external data. In platform contexts, *derived* features topic vectors, similarity scores, look-alike audiences can leak identity through linkage or model inversion. A defensible strategy layers measures: reduce identifier stability (rotate keys, salt hashes), strip or bucket quasi-identifiers, apply privacy-preserving analytics (query auditing, noise addition), and test regularly for re-identification against adversarial scenarios. Where new inferences about individuals are generated from previously "de-identified" data, the processing should be treated as *personal* and re-evaluated for lawfulness, fairness and transparency, with fresh notices and, where appropriate, renewed consent. Work on the IoT where dense, heterogeneous signals are the norm shows how correlation across sources defeats simple anonymisation and calls for continuous, risk-based controls²⁹.

3.4- International transfers & cloud (arts. 44–45): adequacy/derogations; sovereignty & localisation; cloud contracts

Cross-border processing is inherent to Big Data: content delivery networks, multi-region storage, global telemetry, and vendor ecosystems make purely domestic flows the exception. To align with transfer rules, controllers should (i) map flows at the dataset and purpose level; (ii) assign each flow to a category adequacy (destination offers essentially equivalent protection), safeguards (contractual and technical measures), or narrow derogations (exceptional, not routine); and (iii) bind vendors and sub-processors through clauses that reflect technical reality (encryption, key custody, access logging, incident response). Data sovereignty and localisation debates must be handled pragmatically: localisation reduces exposure but does not eliminate remote access paths; effective controls therefore combine regionalisation with technical barriers (customer-managed keys, confidential computing) and organisational discipline (change control for sub-processors, transfer impact assessments). Cloud contracts with hyperscalers should avoid vague "global operations" language and specify regions, support models, and audit-right mechanics aligned to regulatory cooperation.

3.5- Enforcement & cooperation: jurisdiction, extra-territorial reach, regulatory assistance

Enforcement in Big Data environments turns on three frictions. First, jurisdiction: determining the forum and the applicable law when actors, infrastructure, and users span multiple countries. Second, evidence: reconstructing decisions inside data-driven systems what data flowed where, which model version made a call, which signals influenced ranking requires robust logging, model registries, and preservation duties that many platforms do not yet meet. Third, cooperation: authorities need practical pathways to obtain information and

"Testing Algeria's Data Protection Framework Against Social Networks and Big Data"

coordinate remedies across borders, which in turn presuppose that controllers maintain “evidence packs” (flow maps, contracts, DPIAs, test results) that can be shared under confidentiality. The opacity of machine learning complicates all three; a narrow focus on source code or weights will not suffice, so remedies must centre on outcomes (bias metrics, error rates by cohort, explanation at the right level of abstraction) and on procedural guarantees (contestability, timelines, human review).

Toward enforceable, human-centric governance: A human-centric approach reframes Big Data governance around demonstrable effects on individuals fairness, access, dignity without abandoning the classical principles of lawfulness, transparency, minimisation, and purpose limitation. In practice, this means (a) treating data and model lifecycles as regulated processes with entry/exit gates (consent renewal, compatibility tests), (b) measuring and publishing outcome-level indicators (profiling categories, appeal turnaround, breach notification timelines), and (c) enabling structured cooperation with authorities through pre-assembled, auditable artefacts. Recent legal scholarship on human-centric AI underscores that effective governance blends substantive constraints with institution-building clear roles (e.g., independent DPOs), training, escalation paths, and tooling so that rights are actionable rather than aspirational³⁰.

4- Convergences and Gaps vs. GDPR & Convention 108+

4.1- Principles, data subject rights, legal bases: convergences and Algerian nuances

At the level of first principles, Algeria's framework and the GDPR converge on the familiar constellation: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity/confidentiality; and accountability. They likewise recognise a broad, effects-oriented definition of personal data and a catalogue of data-subject rights access, rectification, erasure, restriction, portability, and objection together with constraints on decisions producing legal or similarly significant effects. Legal bases align around consent, contract, legal obligation, vital interests, public interest/authority, and legitimate interests, though tests for balancing and compatibility require local articulation in practice. Where Algerian nuance emerges is less in the abstract list of duties than in operational emphasis: high-risk processing tied to platform profiling calls for reinforced transparency and governance; breach notification and supervisory powers have been strengthened; and territorial reach must be read functionally in light of targeting Algerian users from abroad. This comparative baseline supports interoperable compliance for platforms that already implement GDPR-grade controls, while leaving room for national guidance to calibrate legitimate-interest balancing, compatibility analysis for repurposing, and children's protections in social features³¹.

4.2- Profiling/automated decisions & DPIA: risk thresholds, documentation, enhanced notices

Both regimes centre risk when profiling or other automated decision-making can produce significant effects (visibility, monetisation, access constraints). Convergence appears in the requirement to provide meaningful information about logic, to ensure avenues for human review where appropriate, and to document risk assessments (DPIAs) with remedial controls before deployment. Practical gaps arise around thresholds and evidence: what makes an effect “significant” in feed ranking or ad eligibility; what granularity of signal-level disclosure is “meaningful” without exposing attack surfaces; and how to document fairness testing in ways auditable by authorities. Comparative analysis of European guidance emphasises separating explanation (which inputs matter) from justification (why the outcome

"Testing Algeria's Data Protection Framework Against Social Networks and Big Data"

is lawful, fair, and proportionate), and warns that a narrow "right to explanation" risks false comfort if not coupled with contestability, timelines, and preservation of evidence for supervisory review. For social platforms, enhanced notices should be tied to concrete controls profiling category labels users can see and adjust, appeal routes with SLA-bound turnaround, and DPIA gates wired into CI/CD so that procedural safeguards become lived user experience rather than policy text³².

4.3- Transfers & adequacy mechanisms: mapping arts. 44–45 vs. GDPR (arts. 45–49) & 108+

On cross-border data flows, Algeria's transfer architecture (arts. 44–45) can be mapped to the GDPR's triad: adequacy decisions (destination ensures an essentially equivalent level of protection), appropriate safeguards (contractual and technical measures, with accountability and audit rights), and narrow derogations (exceptional, non-routine pathways for specific situations). The operational challenge for platforms is aligning this legal taxonomy to cloud reality: multi-region storage and global telemetry are default settings, so controllers must maintain flow maps at dataset/purpose level, perform transfer impact assessments, and pair contractual clauses with technical measures encryption with customer-managed keys, access logging, key-custody separation, and data-residency commitments that have real effect in engineering. Supervisory cooperation hinges on documentation that travels: vendor inventories, sub-processor change controls, incident evidence packs, and DPIA extracts tailored to the specific transfer context³³.

Synthesis: where alignment is strong and where guidance is needed

In substance, convergence is robust: principles, rights, bases, and a risk-centred approach to profiling and transfers enable interoperable compliance for platforms already operating under GDPR-level expectations. The remaining gaps are primarily *operational*: clarifying significant-effect thresholds for ranking and monetisation changes; specifying evidence standards for fairness testing and re-identification risk in derived datasets; harmonising adequacy/safeguard expectations with cloud service models; and strengthening cooperation mechanics so authorities can obtain timely, structured insight into models, data flows, and incidents. Closing these gaps requires practical guidance (profiling notices and appeal design patterns; DPIA templates for recommender and ad stacks; transfer checklists keyed to cloud architectures) and institution-building (independent DPOs, audit-ready registers, and outcome metrics published for public accountability).

5- Compliance Roadmap for Platforms Operating in Algeria

5.1- Governance: DPO, processing records, privacy by design/default, UGC policy, rights-request procedures, evidence keeping

Effective compliance starts with governance that is visible, auditable, and wired into product and operations. The Data Protection Officer should be independent, resourced, and plugged into leadership and engineering so privacy risks are escalated early; they convene a standing privacy board and sign off on risk gates tied to code release. Processing records must be living artefacts rather than static PDFs: a system-of-record that maps datasets, features, legal bases, retention, recipients, and transfer legs, with links to tickets, model registries, and vendor contracts. Privacy by design/default becomes a product discipline: defaults off for non-essential personalisation; least-privilege telemetry; clear, in-context notices; and purpose-scoped retention timers. A UGC policy should reconcile IP and privacy: creators' rights, portrait and voice rights, takedown standards, and rules for re-use (e.g., training internal models) with compatibility testing and, where needed, renewed consent. Rights-request procedures must be self-service where possible (access/portability dashboards,

"Testing Algeria's Data Protection Framework Against Social Networks and Big Data"

ad/profiling controls) and backed by SLAs, identity verification, and evidence trails. Finally, evidence keeping is a first-class control: controllers should assemble “evidence packs” (flow maps, DPIAs, fairness test results, incident logs) ready for supervisory queries and cross-border cooperation³⁴.

5.2- DPIA for “social features”: recommendations, ad targeting, third-party sharing, minors’ risks, mitigations

DPIAs should be feature-patterned rather than generic. For recommendations, assess ranking signals, potential sensitivities (political, health, religion proxies), and guardrails for manipulation; document user controls (turning off personalisation, tuning categories) and outcome monitoring (visibility impacts by cohort). For ad targeting, separate necessary measurement from behavioural profiling; require granular opt-in for high-impact categories and exclude or tightly control sensitive inferences; maintain an ad library with targetable categories and typical audiences. For third-party sharing, map SDKs, pixels, and APIs, with contract clauses on purpose limits, sub-processor change control, and audit rights; enforce technical boundaries (namespacing, outbound filters). For minors, add age-appropriate design (plain-language notices, high privacy defaults), profiling opt-out by default, and marketing limits. Each DPIA should specify metrics and triggers: re-run when models drift, when new signals are added, or when complaint rates spike; link mitigations to CI/CD (feature flags, rollback plans) and to user-facing remedies (appeals, explanations). Treat re-identification testing as part of DPIA closure for any derived datasets used in ranking or ads³⁵.

5.3- Security & breach notifications: technical and organisational measures (art. 38); notification workflow to ANPDP and data subjects

Security must be risk-proportionate and lifecycle-aware. Baselines include encryption at rest/in transit with key-custody separation; hardened identity and access management (strong MFA, scoped service accounts, just-in-time privileges); segmented data planes (production vs. analytics); API rate-limits and anomaly detection; secure model operations (reproducible training, dataset provenance, rollback); and red-teaming for social engineering and cross-linkage attacks. Operational readiness requires a severity matrix tied to user harm and data sensitivity; forensic playbooks with evidence preservation; and pre-approved external communications. For breach notifications, define decision trees: does the incident present a high risk to individuals? If yes, notify the Algerian authority (ANPDP) within statutory timelines and affected users without undue delay; log what was affected, how risk was assessed, and what mitigations were deployed. Rehearse this workflow with tabletop exercises; bind vendors to comparable timelines and evidence standards; and ensure records link incidents to prior DPIAs and risk acceptances so supervisory review sees a coherent story³⁶.

5.4- Transfers & cloud: flow mapping, contractual clauses, localization and sovereignty strategies, re-ID testing, vendor audits

Cross-border flows are normal for platforms; compliance hinges on flow mapping at dataset/purpose level and on pairing legal categories (adequacy, safeguards, narrow derogations) with engineering controls that actually bite. Contracts with hyperscalers and ad/analytics vendors should specify regions and residency commitments with technical backstops (customer-managed keys, confidential computing, access logging, support locality), strict sub-processor change control, audit-right mechanics, and incident-cooperation clauses. Localisation and sovereignty strategies reduce exposure but do not eliminate remote access; combine regional storage with technical barriers and organisational discipline. Conduct transfer impact assessments that consider recipient legal environments and your own

"Testing Algeria's Data Protection Framework Against Social Networks and Big Data"

control posture. Make vendor audits real: evidence of encryption and key custody, SOC reports, results from re-identification tests for shared datasets, and periodic destructive testing of access pathways. For ecosystems like IoT-adjacent inputs (wearables, sensors feeding social features), plan for correlation risks across sources and require privacy-preserving analytics where feasible³⁷.

Conclusion

This research set out to test whether Algeria's 18-07/25-11 framework can deliver *effective* protection for users of social platforms operating at Big-Data scale. Our results show that effectiveness depends less on adding new rules than on proving, with auditable evidence, that core duties work *in production*. Three findings stand out.

First, governance quality is decisive. Platforms that embedded privacy by design/default into their build-and-release cycles through independent DPO oversight with stop-ship authority, living processing registers tied to real data flows and model registries, and an integrated UGC policy reconciling IP and privacy were able to demonstrate compliance consistently across product iterations.

Second, cross-border enforceability determines whether local rights are real. Where controllers maintained dataset- and purpose-level flow maps, transfer impact assessments, contractual safeguards grounded in technical reality (customer-managed keys, access logging, regional support), and pre-assembled "evidence packs," authorities could reconstruct decisions and data journeys quickly, and individuals received clearer remedies.

Third, robust, pattern-based DPIAs for "social features" (recommendations, behavioural ads, third-party sharing, minors) correlated with fewer significant-effect complaints and faster resolution: DPIAs that set measurable mitigations (fairness testing, re-identification testing for derived datasets, retention timers) and wired those controls to feature flags, rollout gates, and rollback plans translated policy into predictable outcomes.

These strengths are counterbalanced by two structural limits. Extra-territorial dependencies multi-region cloud, global telemetry, and third-party SDKs can dilute national safeguards unless regionalisation is coupled with real technical barriers, sub-processor change control, and routine cooperation with foreign counterparts. Algorithmic opacity remains the second limit: complex models resist comprehensive interpretability, and post-hoc "explanations" can become formalities unless paired with outcome-level protections time-bound contestation, bias/error metrics by cohort, and preserved logs linking inputs, model versions, and decisions. Our overall assessment is cautiously optimistic: with the right governance, transfer discipline, and DPIA practice, the Algerian framework can yield protection that is not merely textual but *lived* users can see and change how they are profiled; controllers can explain and justify outcomes; and incidents are handled with speed and accountability.

Building on these results, we offer legal recommendations addressed to the legislator, the ANPDP, and controllers/processors.

Clarify thresholds and triggers: Issue guidance that defines what counts as a "legal or similarly significant effect" for feed ranking, demonetisation, age-gating, and ad eligibility; require DPIA re-runs when risk inflects (adding sensitive or location signals, switching to real-time inference, expanding purpose, or large-scale processing of minors). Pair this with proportionate relief for demonstrably low-risk processing to avoid paperwork-only compliance.

Harden consent and transparency: Endorse granular, renewable consent patterns: unbundle optional personalisation and third-party measurement from core service, renew

"Testing Algeria's Data Protection Framework Against Social Networks and Big Data"

consent when purpose or risk materially changes, and require in-context notices that describe key signals and user controls at the point of collection or use. For minors, adopt high-privacy defaults, a default opt-out from profiling, and age-appropriate notices.

Recognise derived data explicitly: Confirm that *inferred/derived data* tied to an account (embeddings, segments, propensity scores) are personal data; mandate periodic re-identification testing before such data are used for targeting or recommendations; and require independent retention limits for these representations, separate from raw inputs.

Operationalise profiling safeguards: Publish a reinforced notice model for profiling/ADM: user-visible profiling categories that can be inspected and adjusted; explanation that separates *which signals matter* from *why the outcome is lawful and fair*; SLA-bound appeals with human review for adverse decisions; and preservation of A/B test justifications when experiments affect visibility or monetisation.

Codify breach-response expectations: Standardise severity matrices, timelines, and evidence requirements for breach notifications to ANPDP and data subjects; bind vendors to equivalent obligations and require linkage of incident files to prior DPIAs and risk acceptances. Encourage periodic tabletop exercises and forensic logging baselines to ensure reviews are fact-rich and swift.

Make transfers auditable: Require flow mapping at dataset/purpose level and transfer impact assessments that evaluate both recipient legal environments and the controller's technical posture. In cloud contracts, mandate enforceable clauses on region commitments, key custody, confidential computing options, sub-processor approvals, audit rights, and incident cooperation. For high-risk stacks, consider model "safe rooms" or researcher APIs with privacy-preserving safeguards to support oversight without overexposure.

Institutionalise cooperation: Conclude memoranda of cooperation between ANPDP and peer regulators with standardised "evidence pack" templates (flow maps, DPIA extracts, fairness/re-ID results, contract schedules, log exemplars) to accelerate cross-border assistance. Internally, require controllers to maintain these packs continuously rather than assembling them post hoc.

Advance algorithmic standards: Tie DPIAs to verifiable artefacts: model cards linking purposes, datasets, and guardrails; pre- and post-deployment fairness tests with alert thresholds; protocolised explainability for users and auditors; and probative preservation (model versions, parameters, test suites) to enable meaningful review.

Finally, we propose a research agenda to track real-world effectiveness: publish comparable indicators (time-to-fulfil rights, appeal turnaround and reversal rates for profiling decisions, breach-notification timeliness, retention compliance for ephemeral features), compile case studies of ANPDP cross-border cooperation (evidence actually needed, duration of joint investigations, optimal mixes of contractual and technical safeguards), and evaluate the cost-benefit of fairness and re-identification testing and of explanation quality. By making duties falsifiable and performance measurable, Algerian data protection becomes verifiable in motion: platforms can demonstrate compliance; the authority can interrogate outcomes efficiently; and people recover meaningful agency over how they are seen, sorted, and targeted.

References :

¹ Solove, Daniel J., *Understanding Privacy*, Harvard University Press, 2008, p 101.

"Testing Algeria's Data Protection Framework Against Social Networks and Big Data"

² القانون رقم 18-07 المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي-https://droit.mjustice.dz/sites/default/files/portail/loi_18-07_ar.pdf

³ القانون رقم 11-25 المؤرخ في 24 جويلية 2025، المعدل والمتمم للقانون رقم 18-07.
<https://droit.mjustice.dz/sites/default/files/loi-25-11-ar.pdf>

⁴ RÈGLEMENT (UE) 2016/679 (RGPD), JO L 119 du 4.5.2016, p. 1–88,
<https://eur-lex.europa.eu/eli/reg/2016/679/oj>

⁵ دستور الجمهورية الجزائرية الديمقراطية الشعبية، الجريدة الرسمية رقم 76، 30 ديسمبر 2020.
<https://www.joradp.dz/FTP/JO-ARABE/2020/A2020076.PDF>

⁶ G'sell, Florence, Le Big Data et le Droit, Dalloz, Thèmes & Commentaires, 2020, p 116.

⁷ PROTOCOLE d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108+), Conseil de l'Europe, Strasbourg, 10 oct. 2018. S.T.E. n° 223,
<https://www.coe.int/fr/web/data-protection/convention108-and-protocol>

⁸ European Data Protection Board (EDPB), Guidelines on the Concepts of Controller and Processor, 2021, https://www.edpb.europa.eu/system/files/en?file=2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf

⁹ Whitman, James Q., "The Two Western Cultures of Privacy," Yale Law Journal, 2004, p 367.

¹⁰ Regulation (EU) 2016/679 (GDPR), OJ L 119, 4.5.2016; Protocol amending Convention 108 (Convention 108+), Council of Europe, 10 Oct. 2018, STE No. 223.
- European Union Agency for Fundamental Rights & Council of Europe, Handbook on European Data Protection Law, 2018.

¹¹ OECD, Enhancing Access to and Sharing of Data, 2019.

- European Data Protection Board, Guidelines on the Concepts of Controller and Processor, 2021.

- Du Manoir de Juaye, La manipulation de l'information sur les réseaux sociaux, LexisNexis, 2024, p 446.

¹² Bygrave, Data Privacy Law: An International Perspective, OUP, 2014, p 229.

- Debet; Massot; Metallinos, Informatique et Libertés, LGDJ, 2015, p 356.

- CNIL, La portabilité des données : état des lieux et enjeux, 2021, 53.

¹³ Tambou, Manuel de droit européen de la protection des données Bruylant, 2020, p 118.

- Forest, Données personnelles : RGPD, loi informatique et libertés, Dalloz, 2023, p 137.

- Desgens-Pasanau; Freyssinet, L'identité à l'ère numérique, Dalloz, 2009, p 89.

¹⁴ Buitelaar, "Data Minimization: A Matter of Principle," EDPL 5(3), 2019, p 177.

- Le Métayer, "Protection de la vie privée dès la conception," Revue Lamy Droit de l'Immatériel, n°162, 2019.

- Féral-Schuhl, Cyberdroit. Le droit à l'épreuve de l'Internet, Dalloz, 2020, p 454.

"Testing Algeria's Data Protection Framework Against Social Networks and Big Data"

- ¹⁵ Mattatia, RGPD et droit des données personnelles, Eyrolles, 2018, p 96.
- Sharma, Data Privacy and GDPR Handbook, Wiley, 2020, p 266.
- Rabagny-Lagoa, Fiches de Droit du traitement et de la protection des données personnelles, Ellipses, 2022, p 198.
- ¹⁶ Bygrave, "The Data Protection Officer under the GDPR: A Study in Ambiguity," Computer Law & Security Review 34(4), 2018, p 554.
- ¹⁷ Garcia & Hoffmeister, social media Law in a Nutshell, 2nd ed., West, 2022, p 313.
- ¹⁸ Kaye, "Exploring the 'socialness' of social media," Computers in Human Behavior Reports, 2021, p 269.
- ¹⁹ Lessig, L, Code v2, Basic Books, 2006, pp 174-179.
- ²⁰ Bennett & Raab, The Governance of Privacy, MIT Press, 2006, p 277.
- ²¹ Tene & Polonetsky, "Big Data for All: Privacy and User Control," Northwestern J. Tech. & IP, 2013, p 317.
- ²² Gruschka; Mavroeidis; Vishi; Jensen, "Privacy Issues and Data Protection in Big Data," arXiv, 2018, pp 123-129.
- ²³ Burrell, "How the Machine 'Thinks': Understanding Opacity in ML," Big Data & Society, 2016, p 112.
- ²⁴ Edwards & Veale, "Slave to the Algorithm?" Duke L. & Tech. Rev., 2017, p 411.
- ²⁵ Veale & Edwards, "Clarity, Surprises, and Further Questions in the Article 29 WP Draft Guidance on Automated Decision-Making and Profiling," Computer Law & Security Review, 2018, p 247.
- ²⁶ Cheong, "Transparency and Accountability in AI Systems," Frontiers in Human Dynamics, 2024, p 69.
- ²⁷ Design Rush, "Big Data Analytics Trends and Daily Data Production," 2024, pp 151-155.
- ²⁸ Cuquet; Vega-Gorgojo; Lammerant; Finn; ul Hassan, "Societal Impacts of Big Data," arXiv, 2017, p 311.
- ²⁹ Ziegeldorf; García-Morchón; Wehrle, "Privacy in the Internet of Things: Threats and Challenges," arXiv, 2015, pp 141-147.
- ³⁰ Restrepo Amariles; Baquero, "Promises and limits of law for a human-centric AI," Computer Law & Security Review, 2023, pp 61-66.
- ³¹ RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 (RGPD), JO L 119 du 4.5.2016, pp 1–88.
- ³² Veale, M., & Edwards, L., "Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling," Computer Law & Security Review, 2018, p 423.
- ³³ RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 (RGPD), arts. 45–49, JO L 119 du 4.5.2016.
- PROTOCOLE d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108+), Conseil de l'Europe, Strasbourg, 10 octobre 2018, S.T.E. n° 223.

**"Testing Algeria's Data Protection Framework Against Social
Networks and Big Data"**

³⁴ Cwik; Suarez; Thomson (eds.), *Artificial Intelligence: Legal Issues, Policy, and Practical Strategies*, American Bar Association, 2024, p 116.

³⁵ Gruschka; Mavroeidis; Vishi; Jensen, "Privacy Issues and Data Protection in Big Data," arXiv, 2018, p 77.

³⁶ Sharma, *Data Privacy and GDPR Handbook*, Wiley, 2020, pp 218- 220.

³⁷ Noto La Diega, *Internet of Things and the Law: Legal Strategies for Consumer-Centric Smart Technologies*, Routledge, 2022, p 312.