International and Comparative
Corporate Law Journal
ISSN: 1388-7084 & E- ISSN: 1875-8290

Legal Protection of Personal Data Amidst the Challenges of Artificial Intelligence

Saida Laibi
University of Hamma Lakhdar - El Oued, Algeria
Email: ostadalaibi@gmail.com

Received: 22/10/2025 **Accepted:** 17/02/2026 **Published:** 15/05/2026

Abstract:
This research examines the legal framework for protecting personal data in light of the rapid advancement of Artificial Intelligence technologies, through an analysis of Algerian Law No. 18-07 dated June 10, 2018, relating to the protection of natural persons in the field of personal data processing. The problem of the study lies in the extent to which the concepts and supervisory and penal mechanisms introduced by the Algerian legislator can accommodate complex technical challenges, such as algorithmic opacity (the "Black Box") and big data processing. The study relied on the analytical method of legal texts, with the use of the comparative method. The study concluded that Law 18-07, despite adopting the principle of technological neutrality, still faces practical difficulties in proving civil and criminal liability for algorithmic errors and in activating the rights of access and objection. The research ended with the necessity of updating technical control mechanisms and enshrining the principle of "privacy by design" to ensure effective protection of private life in the digital environment.
Keywords: Law 18-07; Personal data; Artificial intelligence; National Authority (ANPDP); Digital privacy.

Introduction:

The contemporary world is undergoing a radical digital transformation driven by Artificial Intelligence technologies, which have become structurally dependent on the processing of massive flows of "personal data." If this technological breakthrough has provided innovative solutions in various fields, it has in return produced unprecedented legal and ethical challenges affecting the core of individual rights and freedoms, foremost among them the right to privacy and the inviolability of private life, a right that is no longer merely an intellectual luxury but

has become a cornerstone of the modern rights system, as enshrined by the Algerian constitutional framers in Article 47 of the 2020 constitutional amendment, affirming the sanctity of private life and the confidentiality of correspondence.

In light of this technological dominance, the Algerian legislator addressed the legal gap by enacting Law No. 18-07 relating to the protection of natural persons in the field of personal data processing, drawing inspiration from modern international approaches, particularly the General Data Protection Regulation (GDPR). However, the application of this legal text in an environment dominated by artificial intelligence raises complex issues; machine learning algorithms are characterized by "self-evolving" properties and "programmatic opacity," which may render traditional rules of transparency and prior consent insufficient to provide effective protection of data.

The importance of this study lies in attempting to identify the gap between the Algerian legislative text (Law 18-07) and the rapidly evolving technological reality, and in examining the adequacy of available supervisory and penal mechanisms to regulate the behavior of intelligent systems and prevent their deviations.

Accordingly, the research problem is centered on the following question: To what extent has the Algerian legislator, through Law No. 18-07, been able to establish an integrated legal system ensuring effective protection of personal data in the face of emerging risks of artificial intelligence?

To answer this question, the analytical method of legal texts is adopted, with recourse to the comparative method when necessary, according to the following plan:

• The first chapter: Conceptual framework and challenges of intelligent personal data processing.

• The second chapter: Protection, oversight, and liability mechanisms in Algerian law.

First Chapter: Conceptual Framework and Challenges of Intelligent Personal Data Processing

This chapter addresses the conceptual framework governing personal data protection in the face of intelligent systems, focusing on the adaptation of legal concepts under Law No. 18-07 and the challenges posed by artificial intelligence and big data. It is divided into two sections.

Section One: Adaptation of Artificial Intelligence and Big Data Concepts in Algerian Legislation

Subsection One: Adaptation of Artificial Intelligence as "Automated Processing" under Article 03 of Law 18-07

First: Objective standard and technological neutrality in processing

The legislator defined processing under Article 03 of Law 18-07 as any operation or set of operations carried out by "automated procedures," a definition characterized by "technological neutrality" that allows machine learning and deep learning models to be included within the scope of the law, as they are essentially logical computational operations performed on stored digital data. Through the legal interpretation of this article, it is noted that the legislator did not limit processing to a specific means or purpose but extended protection to include a series of programming acts starting from "collection and recording" and reaching "extraction, use, and communication."

This enumeration corresponds technically to the life cycle of data within artificial intelligence systems, where the training phase corresponds to "recording and storage," while the prediction and decision-making phase corresponds to "use and access" in the legal text.

Second: Subjection of intelligent systems to prior control obligations

Based on the above legal characterization, artificial intelligence systems, regardless of their degree of software autonomy, remain legally "automated processing tools" subject to procedural obligations imposed by the legislator, particularly the requirement of prior declaration and authorization before the National Authority for Data Protection (ANPDP). However, a precise technical issue arises in this context concerning "generative data" produced autonomously by artificial intelligence based on complex inferences. Although the legislator did not explicitly refer to them, the flexibility of the term "adaptation or modification" in Article 03 allows the judge and legal researcher to extend protection to these new outputs, making Algerian law capable of accommodating software developments without urgent legislative amendments, provided there is a legal interpretation consistent with the digital era.

Subsection Two: Big Data and Its Inclusion within Personal Data

First: Legal standard for determining the "personal" nature of data in the digital environment

Based on paragraph one of Article 03 of Law No. 18-07, the Algerian legislator adopted a broad concept of personal data, considering it as any information allowing the identification of a

natural person directly or indirectly. This legislative definition makes big data a subject of legal protection; although it may not contain explicit names in its original form, its possibility of being linked to other identifying elements such as geographic location or identification number gives it a "personal" character, which requires data processors to comply with the principle of "informed consent" stipulated in Article 07 of the same law.

However, the issue that arises in this context lies in the "inferred data" created by algorithms about individuals without their intervention; thus, the question arises regarding the sufficiency of the current text in addressing "indirect collection" operations carried out through the derivation of hidden behavioral patterns, a gap that requires broad judicial interpretation of the concept of collection to include even automated inference.

Second: Issue of anonymized data (Anonymization) in light of intelligent analysis

The legislative logic in Law 18-07 is based on the fact that data from which identity elements are definitively removed falls outside legal protection due to the absence of a "specific person." Therefore, the legislator in Articles 33 and following required technical measures to ensure data confidentiality and security as part of the obligations of the data controller.

From a legal perspective, anonymization is considered a mechanism for compliance with "digital security" requirements established by the Algerian legislator to reduce risks to private life. However, this legal approach faces a major technical issue represented by the ability of artificial intelligence to "re-identify" individuals, as by linking large and dispersed databases algorithms can restore the identity of anonymized persons, and the danger lies in the fact that anonymization is no longer an absolute guarantee, which legally requires that such data remain under the supervision of the National Authority (ANPDP) as long as the possibility of identity disclosure remains technically present.

Section Two: Emerging Threats to Privacy under Intelligent Systems

If the Algerian legislator, in Law No. 18-07, has established a set of concepts to regulate data processing, the rapid development of artificial intelligence has produced technical risks that go beyond traditional forms of privacy infringement, as the problem is no longer limited to data leakage but extends to the decision-making mechanism within algorithms, which has become opaque and capable of predicting individuals' behavior and classifying them digitally without their knowledge.

Faced with this challenge, a fundamental question arises regarding the resilience of guarantees contained in Algerian legislation against "black box" technologies and emerging re-identification mechanisms.

To address these threats legally, this section is divided into two main subsections:

• **Subsection One:** The issue of "Black Box" algorithms and the right to transparency.

• **Subsection Two:** Risks of re-identification (De-anonymization) and automated classification of individuals.

Subsection One: The issue of "Black Box" algorithms and the right to transparency

The principle of transparency is one of the fundamental pillars of Law No. 18-07, where the legislator required the "data controller" to clearly inform the data subject about the purpose and method of processing, and this threat will be addressed as follows:

First: Opacity of processing and the principle of the right to information.

With reference to Article 31 of Law 18-07, the Algerian legislator grants the data subject the right to obtain accurate and clear information regarding the nature of the processing to which their data is subjected, and this provision in its legislative essence aims to enable the individual to exercise self-monitoring over their privacy and to ensure that processing does not deviate from its original purpose. However, the major legal problem arises when confronting artificial intelligence systems based on “Black Box” algorithms, which are systems characterized by computational complexity that makes it impossible for the data controller to explain the logical mechanism by which the machine reached a specific decision; this technical opacity empties the “right to information” of its actual content. How can the explicit duty of information stipulated in Algerian law be complied with if the decision-making mechanism is not clearly interpretable by humans? This situation creates a stark conflict between the “commercial and software secrets” of companies and the “citizen’s right to digital transparency” legally guaranteed, which renders the legal text insufficient to track concealed algorithmic operations.

Second: the difficulty of exercising the right of objection and access

The Algerian legislator, under Articles 28 and 32 of Law 18-07, grants every natural person the right to access their stored personal data and to object to its processing for legitimate reasons, reflecting the legislator’s intention to establish individual sovereignty over digital data. From a legal perspective, the exercise of these rights requires the system’s ability to identify, isolate, and delete data upon request; however, exercising these rights in an artificial intelligence

environment faces strong technical barriers, as data within intelligent systems is not stored as separate inputs but is instead fused and transformed into complex "numerical weights" that are difficult to trace or delete without affecting the entire system structure. This reveals that the "right of access and objection" guaranteed by Algerian law may become practically impossible if developers do not adopt from the outset the principle of "Privacy by Design," placing individuals in a state of legal incapacity before the power of predictive algorithms that may continue processing data traces even after deletion requests, turning legislative guarantees into purely theoretical provisions lacking technical enforcement mechanisms.

Subsection: risks of re-identification (De-anonymization) and automated profiling of individuals

The process of classification and tracking of digital behavior is among the most serious challenges to the right to privacy, as artificial intelligence systems rely on aggregating scattered data fragments to build precise personal profiles (Profiling) for each individual, placing the guarantees contained in Law 18-07 under real test.

First: re-identification techniques and the collapse of anonymization barriers

Based on the security principles established by the Algerian legislator in Articles 33 and following of Law 18-07, there is an explicit obligation on the data controller to take all technical and organizational measures to protect data from destruction or unauthorized access, which led many institutions to adopt "data anonymization" techniques as a technical solution to comply with legal obligations and ensure that data subjects' identities are not disclosed. However, modern technical reality has revealed a highly complex legal issue represented in the ability of artificial intelligence algorithms to break anonymization through what is known as "re-identification," where by correlating anonymized datasets with other available databases (such as social networks or public records), the machine can infer a person's identity with high precision. The danger lies in the fact that "data anonymization," once considered a legal safeguard exempting companies from liability, has become in the era of artificial intelligence a temporary protection that can be breached, which makes legal texts linking protection to "identifiability" in Article 03 of Algerian law face the challenge of determining when data is truly anonymous and when it becomes personal requiring full protection.

Second: risks of automated profiling and algorithmic decision-making

The Algerian legislator, in Article 07 of Law 18-07, enshrines the principle of "fairness and lawfulness" in data processing, which requires that data not be used in a way that harms the interests or dignity of the data subject. Legally, this provision aims to prevent the exploitation of personal data for discrimination or harmful profiling purposes; however, a new emerging threat appears in the form of "automated profiling," where intelligent systems analyze personal data to predict health status, political tendencies, or creditworthiness, and based on that, automated decisions may deprive individuals of certain rights without any human intervention. The legal problem lies in the fact that Algerian law, despite establishing general safeguards, does not include an explicit provision regulating the "right not to be subject to a purely automated decision," unlike comparative legislation, leaving individuals directly exposed to algorithmic biases and making it difficult to prove abuse in automated processing occurring behind silent screens.

Chapter Two: Protection, oversight, and liability mechanisms in Law No. 18-07

Substantive rules alone are not sufficient to guarantee the sanctity of personal data in the face of technological dominance of artificial intelligence; therefore, it became necessary to establish a procedural and regulatory system capable of enforcing compliance with the law. Accordingly, the Algerian legislator in Law 18-07 did not merely establish general principles but also created institutional foundations represented by the "National Authority for the Protection of Personal Data," and introduced a strict liability and sanction system to deter any violation of individuals' privacy. This chapter seeks to examine the effectiveness of these mechanisms in controlling algorithmic power, and is divided into two sections: Section One: the regulatory role of the National Authority for the Protection of Personal Data (ANPDP); Section Two: the legal liability and sanctions regime in data processing.

Section One: the regulatory role of ANPDP

The National Authority for the Protection of Data is considered the cornerstone of the protective system established by the legislator, as it is the body responsible for monitoring the legality of automated processing and ensuring that it does not deviate from its legal framework. Its powers are particularly significant in the context of artificial intelligence due to the need for both prior and subsequent technical oversight of algorithms.

Subsection One: the legal nature of the National Authority and its administrative powers

The Algerian legislator, under Article 19 of Law 18-07, established an independent administrative authority with legal personality and financial autonomy placed under the authority of the President of the Republic, namely the National Authority for the Protection of Personal Data. Regarding its nature and powers:

First: institutional independence and composition of the authority

Articles 19 and 20 of Law 18-07 show that the legislator ensured the "independence" of this authority to guarantee neutrality in supervising both public and private entities, as it is composed of judges and figures recognized for competence in digital and legal fields; this pluralistic composition aims to create a supervisory reference capable of understanding the technical complexity of artificial intelligence and aligning it with legal texts. The problem lies in the fact that this independence, despite being legally affirmed, still requires massive technical and human resources to keep pace with global companies developing AI systems, placing the authority before the challenge of balancing administrative dependency and digital sovereignty in decisions of approval or refusal of complex processing.

Second: decision-making powers and prior authorization regime

Law 18-07 grants the authority, under Articles 13 to 18, the power to issue processing authorizations and receive declarations as a prior control mechanism aimed at verifying the legality of processing purposes before initiation. Legally, any artificial intelligence system intending to process Algerian citizens' data must obtain authorization if the processing involves specific risks such as sensitive or biometric data; however, the problem emerges in cross-border processing carried out via cloud computing, where the legislator faces difficulty imposing prior authorization on international platforms using AI to collect citizens' data from outside national territory, which requires activating international cooperation powers to prevent data leakage under the guise of "smart services" available online.

Subsection Two: technical oversight and investigative mechanisms in intelligent processing

The Algerian legislator did not limit the authority to administrative functions but reinforced it with field inspection mechanisms allowing access to automated processing systems to ensure compliance with the law.

First: inspection power and access to information systems

Articles 24 and following of Law 18-07 grant officers of the National Authority, who hold judicial police officer status, the power to enter premises where data processing is carried out and to access all documents and technical means used in processing. This power aims to enable "algorithmic audit" to ensure that artificial intelligence does not process more data than authorized or engage in unlawful profiling. The legal and technical issue lies in the difficulty of physical inspection, as AI algorithms are often stored in cloud servers outside physical company premises, which causes traditional inspection powers to face obstacles of technical sovereignty and the difficulty of decoding complex systems requiring specialized experts who do not necessarily hold judicial authority.

Second: investigation of complaints and urgent protection measures

Article 23 of the same law grants the authority the power to receive complaints from individuals who believe their rights have been violated due to data processing, and to issue warnings or suspend authorizations temporarily or permanently.

Based on the legal grounding of this right

The Authority plays the role of an "administrative protector" of the privacy of Algerians against the dominance of tech companies, as it has the right to freeze any intelligent processing proven through investigations to involve serious risks to private life. However, the problem lies in "response speed"; artificial intelligence processes millions of data points in fractions of a second, whereas administrative and judicial investigation procedures in Algeria may take a long time, which may result in the Authority's decision to withdraw authorization or freeze processing arriving too late, after digital harm has already occurred and data has been leaked or widely exploited. This necessitates activating mechanisms of "proactive automated oversight" instead of relying solely on traditional administrative reaction.

Second requirement: the legal liability regime and sanctions in the field of data processing

The recognition of rights and imposition of obligations under Law No. 18-07 is not complete without a legal liability system ensuring compensation for harm resulting from data misuse, and a penal system deterring violators. The importance of this requirement increases in the context of artificial intelligence due to the difficulty of identifying the "perpetrator" of digital harm and qualifying the criminal act, which will be addressed in the following two branches:

• **First branch: the problem of determining civil liability for errors in intelligent processing.**

• **Second branch: the penal system and punitive measures under Law 18-07.**

First branch: the problem of determining civil liability for errors in intelligent processing

Civil liability is the legal means of compensating individuals for harm caused to their privacy due to unlawful processing, and the Algerian legislator has established general and specific rules governing this aspect as follows:

First: the basis of the "data controller's" liability under Algerian law

Referring to Law 18-07, the legislator has imposed on the "data controller" (the natural or legal person who determines the purposes and means of processing) the obligation to ensure data security and integrity. In case of any leak or abusive processing, the affected person has the right to claim compensation based on the rules of tort liability established in Algerian civil law. Legally, this obligation is considered an "obligation of result" with regard to protecting data from unauthorized access, which facilitates the burden of proof for the harmed individual once a breach or misuse occurs. However, the major legal problem in the context of artificial intelligence lies in the "multiplicity of actors"; who is civilly liable when an intelligent system makes an error? Is it the algorithm developer, the company operating the system, or the system itself which made an "autonomous" and unforeseen decision? This fragmentation of liability makes it difficult for the victim in Algeria to identify the true defendant, especially since Law 18-07 has not explicitly adopted the concept of "joint liability" capable of accommodating the complexity of digital supply chains.

Second: the difficulty of proving moral damage and causal link

Algerian judiciary recognizes the right to compensation for both material and moral damage resulting from violations of private life, in line with Article 07 of Law 18-07 which imposes fairness in processing. In the context of artificial intelligence, harm is often "moral" (such as reputational damage resulting from incorrect automated classification). However, the problem lies in proving the "causal link" between programming error and the resulting harm. Due to the opacity of black-box algorithms, neither the victim nor the court can understand how a technical defect led to the harmful outcome.

This "evidentiary incapacity" may lead to companies escaping civil liability under the argument of "technical force majeure" or "autonomous machine action," which requires the Algerian

judge to adopt a standard of "objective liability" or "presumption of fault" to protect the weaker party in the digital relationship.

Second branch: the penal system and punitive measures under Law 18-07

The Algerian legislator did not limit itself to civil compensation but dedicated an entire chapter to criminal sanctions under Law 18-07 to deter any intentional violation of personal data. This system is detailed as follows:

First: crimes related to violation of processing conditions and confidentiality

The legislator provided, in Articles 51 to 66 of Law 18-07, prison penalties ranging from six months to five years and heavy fines for anyone who processes data without authorization or refuses to comply with decisions of the National Authority.

Legally, these provisions aim to protect the "digital public order"; merely operating an artificial intelligence system processing Algerian data without legal authorization constitutes an independent offense regardless of whether harm occurs. The problem lies in defining "criminal intent" in algorithmic crimes: can a company be held criminally liable for a "discriminatory decision" made automatically by artificial intelligence? Current legal texts focus on "material acts" (such as leakage or non-declaration), but may not cover "smart crimes" committed through algorithmic manipulation to mislead public opinion or target specific groups, requiring an update of penal provisions to keep pace with advanced cybercrime.

Second: complementary penalties and criminal liability of legal persons

The Algerian legislator recognizes the possibility of criminal liability of legal persons (companies) for offenses committed on their behalf, including complementary penalties such as confiscation, closure of premises, and publication of the judgment nullifying processing.

Legally, these penalties are among the most deterrent for major tech companies, as banning a company from processing data in Algeria effectively halts its digital activity. However, the problem lies in "jurisdiction"; most AI-based companies are transnational and do not have physical establishments within Algerian territory. This digital reality makes enforcement of criminal sanctions under Law 18-07 almost impossible without specialized international judicial cooperation agreements, potentially rendering penal provisions ineffective against companies managing Algerian data from abroad.

Conclusion:

At the conclusion of this modest study on "the protection of personal data in light of artificial intelligence under Law No. 18-07," it can be said that the Algerian legislator has taken a major step by enacting this specialized legal framework, shifting privacy protection from traditional general rules to a digital and institutional regulatory space. However, the confrontation between "legal texts" and "artificial intelligence algorithms" has revealed gaps that require continuous reassessment.

This study reached the following results and proposals:

First: findings

1. **Flexibility of the legal text:** Law 18-07, through its adoption of "technological neutrality" in Article 03, is capable of accommodating artificial intelligence and big data as legal categories (automated processing) without structural conceptual change.
2. **Shortcomings in transparency mechanisms:** The right to information and access (Articles 28 and 31) is technically hindered by the "black box" phenomenon, making current guarantees difficult to enforce.
3. **Challenge of legal liability:** Civil and criminal liability rules still focus on the "material act" of the data controller, while AI introduces a form of shared liability that is difficult to prove in court.
4. **Digital sovereignty:** The National Authority (ANPDP) remains the key protection pillar, but its effectiveness depends on its ability to exercise cross-border oversight over international platforms processing Algerian data abroad.

Second: proposals

1. **Establishing "privacy by design":** The Algerian legislator should amend Law 18-07 to require AI developers to integrate data protection measures into the core code (Privacy by Design) as a condition for authorization.
2. **Regulating automated decision-making:** Explicitly guarantee individuals the right not to be subject solely to automated decisions (such as credit or employment profiling), and ensure the right to human review.
3. **Strengthening the technical capacity of the Authority:** Equip the National Authority with data engineering and cybersecurity experts to enable real algorithmic audits rather than documentary supervision.

4. **Developing specialized judiciary:** Train judges in digital disputes and artificial intelligence to enable understanding of "digital harm" and application of objective liability rules.

References

Algerian People's Democratic Republic. (2020). *Constitution of the Algerian People's Democratic Republic of 1996, amended and supplemented by Law No. 20-13 of December 30, 2020* (Official Gazette No. 82).

Algerian People's Democratic Republic. (2018). *Law No. 18-07 of June 10, 2018, on the protection of natural persons in the processing of personal data* (Official Gazette of the Algerian Republic, No. 34, June 10, 2018).

European Parliament & Council of the European Union. (2016). *Regulation (EU) 2016/679 of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR)* (Official Journal of the European Union, L 119, Vol. 59, May 4, 2016).

Algerian People's Democratic Republic. (2018). *Law No. 18-07 of June 10, 2018 on the protection of natural persons in the processing of personal data*, Article 3.

Qadri, F. (2020). The legal protection of personal data in Algeria. *Al-Mufakkir Journal, University of Mohamed Khider Biskra*, 15, 48.

See Articles 13–14 of Law No. 18-07 on prior control procedures for automated processing.

Ben Ahmed, A. M. (2018). Mechanisms for protecting personal data in Algerian legislation. *Journal of Rights and Freedoms, University of Biskra*, 6(2), 118.

Algerian People's Democratic Republic. (2018). Law No. 18-07, Article 3(1).

Bouchachi, N. (2021). *Legal protection of the right to digital privacy: A comparative study*. University Thought Publishing House, Alexandria, Egypt, p. 88.

See Articles 33–38 of Law No. 18-07 on data processing security and confidentiality obligations.

Ben Ahmed, A. M. (2018). Risks of re-identification. *Journal of Rights and Freedoms, University of Biskra*, 6(2), 125.

Algerian People's Democratic Republic. (2018). Law No. 18-07, Article 31.

Abdelhay, I. A. (2020). Legal protection of privacy in the face of artificial intelligence challenges. *Journal of Legal and Economic Research, Mansoura University*, 72, 228.

See Articles 28 (right of access) and 32 (right to object) of Law No. 18-07.

Ben Ahmed, A. M. (2018). Mechanisms for protecting personal data in Algerian legislation. *Journal of Rights and Freedoms, University of Biskra*, 6(2), 130.

See Articles 33–34 of Law No. 18-07.

Bouchachi, N. (2021). *Legal protection of digital privacy*, p. 102.

Algerian People's Democratic Republic. (2018). Law No. 18-07, Article 7.

Compare with Article 22 of the GDPR; see risks of automated profiling: Ben Ahmed, A. M. (2018), p. 135.

Qadri, F. (2020). Op. cit., p. 60.

Algerian People's Democratic Republic. (2018). Law No. 18-07, Article 19.

See Articles 20–21 of Law No. 18-07 on the composition of the National Authority.

Ben Ahmed, A. M. (2018). Op. cit., p. 140.

See Articles 13–18 of Law No. 18-07.

See Article 44 of Law No. 18-07 on data transfer outside the country.

See Articles 24–25 of Law No. 18-07.

Qadri, F. (2020). Op. cit., p. 65.

Algerian People's Democratic Republic. (2018). Law No. 18-07, Article 23.

Compare with emergency intervention powers under GDPR: Ben Ahmed, A. M. (2018), p. 145.

See general liability rules in Articles 124 et seq. of the Algerian Civil Code in relation to Law 18-07 obligations.

Abdelhay, I. A. (2020). Op. cit., p. 245.

Algerian People's Democratic Republic. (2018). Law No. 18-07, Article 7.

See difficulties of algorithmic fault proof: Ben Ahmed, A. M. (2018), p. 155.

Algerian People's Democratic Republic. (2018). Law No. 18-07, Articles 51–66.

Bousquiaa, A. (2021). *A concise guide to special criminal law (crimes against persons and property), Vol. 1*. Houma Publishing, Algeria, 18th ed., p. 225.

See Articles 64–65 of Law No. 18-07 on legal persons' liability and supplementary penalties.

Qadri, F. (2020). Op. cit., p. 72.