

Artificial Intelligence and Personal Data Protection: An Analytical Study of the Provisions of Law No. 25-11

Ghribi Yahia *

University of "Ammar Telidji" Laghouat (Algeria)
Research Laboratory on Law and Society Development
y.ghribi@lagh-univ.dz

📅📅📅

Date of submission: 23/03/2026

- Date of acceptance: 30/05/2026

- Date of publication: 05/06/2026

ABSTRACT:

The contemporary digital revolution presents unprecedented legal challenges concerning the protection of personal data. While Artificial Intelligence (AI) applications serve as a primary catalyst for innovation and socio-economic development, they simultaneously impose fundamental risks to data privacy and integrity. Recognizing these complexities, the Algerian legislature has sought to modernize the legal framework by enacting Law No. 25-11, which amends and supplements Law No. 18-07 concerning the protection of natural persons in the processing of personal data. Accordingly, this analytical study aims to evaluate the adequacy and efficacy of the current legal and institutional framework, with a particular focus on the capacity of newly introduced mechanisms to fortify data protection amidst the rapid advancements in AI technologies.

key words : Law No. 25-11, Personal Data, Artificial Intelligence (AI), Automated Processing, The National Authority.

Introduction:

Recent decades have witnessed an unprecedented and rapid proliferation of Information and Communication Technologies (ICT), particularly within the burgeoning field of Artificial Intelligence (AI). This technological surge has consolidated the role of personal data as a fundamental pillar of both the digital economy and the information society. Against the backdrop of these transformative shifts characterized by the ubiquity of digital data processing and the pervasive integration of information systems and networks personal data, which resides at the very core of individual privacy, has emerged as a dual-natured instrument. While it serves as a primary catalyst for socio-economic advancement, it has simultaneously become a focal point for various forms of infringement and illicit exploitation.

*-Author Correspondent:

Consequently, these dynamics have engendered complex legal and security challenges that jeopardize individual privacy and fundamental rights, necessitating a robust legislative framework capable of striking a delicate balance between the inherent right to privacy and the pragmatic imperatives of the digital era.

The contemporary digital revolution characterized by rapid advancements in Artificial Intelligence (AI) presents unprecedented legal complexities regarding the protection of personal data. While AI technologies serve as a primary catalyst for innovation and socio-economic development, they simultaneously impose fundamental challenges to the sanctity of private life and data integrity. The exponential expansion in the utilization of information technologies for the collection, storage, and processing of personal data has increasingly underscored the inherent risks associated with information systems and their pervasive threat to individual privacy.

This exigency has galvanized international, regional, and national efforts to establish specialized principles and regulatory frameworks aimed at providing comprehensive protection for natural persons in this domain. Such measures serve as an institutional embodiment of Article (12) of the Universal Declaration of Human Rights (UDHR), which proscribes any arbitrary interference with an individual's privacy¹. Furthermore, these measures are in strict pursuance of Article (17) of the International Covenant on Civil and Political Rights (ICCPR), which prohibits any arbitrary or unlawful interference with an individual's privacy, as well as any unlawful attacks upon their honor and reputation².

Consequently, there has been a global burgeoning of interest in establishing fundamental rules and principles designed to provide comprehensive protection for personal data, given its intrinsic nexus with the sanctity of private life. Furthermore, the creation of specialized regulatory bodies to oversee compliance with data processing principles within the digital environment is increasingly recognized as the optimal administrative paradigm for ensuring the efficacy of such legislation and fostering rigorous adherence to its mandates³.

The Algerian legislator has consistently aligned with this global legal trajectory through the enactment of Law No. 25-11 (dated July 24, 2025), which substantively amends and supplements Law No. 18-07 relative to the protection of natural persons in the processing of personal data⁴. This legislation was enacted to reinforce the

¹ See: Article (12) of the Universal Declaration of Human Rights, adopted by the UN General Assembly in Paris on December 10, 1948, via Resolution 217 A (III).

² See: Article (17) of the International Covenant on Civil and Political Rights, adopted and opened for signature, ratification, and accession by UN General Assembly Resolution 2200A (XXI) of December 16, 1966.

³ See: Mona Al-Ashqar Jabbour and Mahmoud Jabbour, *Personal Data and Arab Laws: Security Concerns and Individual Rights*, 1st ed., Arab Center for Legal and Judicial Research, League of Arab States, Council of Arab Ministers of Justice, Beirut, 2018, p. 169.

⁴ See: Law No. 25-11 of 28 Muharram 1447, corresponding to July 24, 2025, amending and supplementing Law No. 18-07 of 25 Ramadan 1439, corresponding to June 10, 2018, relating to the protection of natural persons in the processing of personal data, Official Gazette (OG) No. 48, p. 14.

existing legal framework and to regulate protective mechanisms in response to emerging digital challenges. It establishes a comprehensive set of statutory and institutional rules designed to ensure the effective protection of personal data particularly as any infringement thereof constitutes a grave violation of human dignity and fundamental rights. These measures are necessitated by the profound challenges imposed by the digital revolution and the 'Open Virtual World,' where the pervasive dissemination of personal data has rendered the preservation of its security, integrity, and confidentiality increasingly complex.

The Refined Significance of the Study:

The significance of this study emanates from its focus on the critical equilibrium between the imperatives of technological advancement and the necessity of upholding the fundamental rights and freedoms of natural persons. In the contemporary legal landscape, the protection of personal data has transcended its role as a mere statutory obligation; rather, it has become a definitive benchmark for measuring a state's progress and the efficacy of its legislative framework in aligning with the complex exigencies of the digital age.

The Refined Research Objectives:

This study seeks to achieve a multifaceted set of objectives, most notably:

- To scrutinize the nascent legal framework for personal data protection in light of the substantive provisions established by Law No. 25-11.
- To examine the primary statutory measures introduced by the legislator to mitigate the unprecedented challenges posed by Artificial Intelligence (AI).
- To evaluate the functional efficacy of the institutional and regulatory mechanisms mandated by Law No. 25-11 in safeguarding personal data processed within the digital environment, and to assess their resultant implications for the fundamental right to privacy.

The Refined Research Problematic:

Against this backdrop, the present study addresses the following pivotal question: To what extent has the Algerian legislator effectively responded to the profound challenges posed by Artificial Intelligence (AI) regarding personal data protection under Law No. 25-11? Furthermore, what are the newly instituted legal and structural mechanisms adopted to reinforce this protection and align with contemporary digital advancements?

Methodology and Research Structure:

To address this problematic, a multifaceted approach incorporating descriptive and analytical methodologies has been employed. Additionally, a comparative method is utilized where necessary to contrast the Algerian legislative stance with select foreign jurisdictions. The research is structured into two primary chapters: the first examines the Protection of Personal Data in the Context of Artificial Intelligence, while the second explores the legal foundations for safeguarding personal data in the digital environment.

Section I : Protection of Personal Data in the Context of Artificial Intelligence

This chapter delineates the conceptual framework of Artificial Intelligence (AI) and examines its transformative impact on personal data, along with the requisite protective measures. This inquiry is structured into two thematic sections: the first explores the conceptual foundations of AI, while the second investigates the interplay between AI technologies and data privacy.

Subsection I: The Conceptual Framework of Artificial Intelligence

Elucidating the concept of Artificial Intelligence necessitates a dual-faceted linguistic and terminological analysis, as follows:

A. Defining Artificial Intelligence

Artificial Intelligence has emerged in the contemporary era in both its physical and virtual forms with unprecedented velocity. This rapid evolution mandates a rigorous definitional inquiry, commencing with its linguistic roots followed by its specialized terminological significance.

1. The Linguistic Definition of Artificial Intelligence:

Standard linguistic lexicons do not provide a singular, holistic definition for 'Artificial Intelligence' as a compound term. Consequently, a linguistic deconstruction is required defining 'Intelligence' and 'Artificial' independently to derive a synthesized meaning that encapsulates the essence of the combined term, as follows:

a. Intelligence :

In the Arabic linguistic tradition, Intelligence is defined as 'acuteness of mind, cognitive perception, speed of comprehension, and the innate capacity for discernment and inference¹'. "Etymologically, the term Intelligence is derived from the Arabic root (dh-k-w). Linguistically, it is expressed through the paradigm '*dhaka-yadhku-dhaka'an*', where the term signifies acuteness of the heart (intellect) and celerity of intuition²'. "In this sense, human intelligence refers to 'an individual's innate capacity for comprehension, analysis, inference, and discernment, underpinned by intuitive acumen and the ability to adapt to diverse situational contexts.³

b. Artificial :

The term Artificial is derived from manufactured material. It denotes that which is not naturally occurring, characterized by human invention, synthesis, and assembly. This concept is predicated on the utilization of diverse scientific and cognitive methodologies as essential tools for producing various industries, ranging from primary and heavy manufacturing to advanced electronic systems⁴. Consequently, the term 'Artificial' is derived from the verb '*istana'a*' (to manufacture

¹ See: Ibn Manzur, *Lisan al-Arab*, vol. 13, Dar Sader, Beirut, 1990, p. 208.

² See: Abu al-Fadl Jamal al-Din Muhammad ibn Mukram Ibn Manzur, *Lisan al-Arab*, vol. 6, 4th ed., Dar Sader for Printing and Publishing, Beirut, 2005, p. 37.

³ See: Mu'jam al-Ma'ani al-Jami' (Universal Lexicon), available at: <https://www.almaany.com/ar/dict/ar-ar/>

⁴ See :Ahmad Mukhtar Umar, *Dictionary of Contemporary Arabic*, 1st ed., Alam al-Kutub, Cairo, 2008, p. 273.

or fabricate). It signifies anything created by human hands or innovated through human labor and diligent effort¹.

Based on the foregoing, it can be concluded that the linguistic term 'Artificial Intelligence' refers to a constructed or innovated capacity designed to simulate human acumen; in essence, it involves imbuing man-made entities with intellectual attributes. Furthermore, the linguistic essence of the phrase centers on a qualitative understanding predicated on scientific and cognitive foundations across various technological media. This implies that the core and evolution of AI are rooted in accumulated scientific and technical knowledge, which is built upon the efficacy and velocity of cognitive comprehension².

2. The Terminological Definition of Artificial Intelligencem:

To establish a precise terminological framework for Artificial Intelligence (AI), it is imperative to examine its definition from both technical and legal perspectives, as follows:

a. The Technical Definition of Artificial Intelligence:

The genesis of the term 'Artificial Intelligence' is attributed to pioneering mathematicians and probability theorists, most notably Alan Turing. Turing conceptualized computers as entities capable of utilizing available information to identify patterns, thereby facilitating problem-solving and decision-making processes. In his seminal 1950 research paper, '*Computing Machinery and Intelligence*', he explored the feasibility of constructing intelligent machines, proposing a methodology to test their intelligence and evaluate their capacity to exhibit behavior equivalent to human cognitive performance.

In 1956, the American computer scientist John McCarthy, a founding father of the field, defined Artificial Intelligence as: 'The science and engineering of making intelligent machines'³, with a specific emphasis on intelligent computer programs⁴. This foundational perspective was further evolved by Stuart Russell and Peter Norvig, who describe AI as: 'The study of agents that perceive their environment and take optimal actions to achieve their goals'⁵. This definition marks a pivotal shift toward autonomous agency. Furthermore, contemporary scholarship defines AI as a modern science dedicated to designing intelligent software and systems capable of simulating human cognitive behaviors such as analysis, reasoning, and decision-making without direct human intervention⁶. Other academic perspectives characterize it as a suite of computational and software frameworks that

¹ Academy of the Arabic Language, *Al-Mu'jam al-Wasit*, vol. 1, 4th ed., Dar al-Da'wah, Cairo, 2004, p. 519.

² See: Omar Nafe' Reda al-Abbasi, *The Legal System of Artificial Intelligence*, 1st ed., Arab Center for Publishing and Distribution, Cairo, 2023, p. 21.

³ See: Nils J. Nilsson, *The Quest for Artificial Intelligence: A History : of Ideas and Achievements*, Cambridge University Press, 2010, p163.

⁴ See: John McCarthy, *What is AI*, Stanford University, 2007, p2.

⁵ See Stuart Russell & Peter Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed., Pearson, 2021, p1.

⁶ See: Ahmad Atef Abdel-Moneim, *Artificial Intelligence and its Modern Applications*, Dar al-Fikr al-Jam'i, Alexandria, 2020, p. 12.

perform functions typically requiring human intelligence, such as deductive reasoning, learning from experience, and adaptive flexibility¹.

b. The Definition of Artificial Intelligence from an International Law Perspective:

To date, there is no single, globally unified treaty that provides a comprehensive definition of Artificial Intelligence. However, various international bodies and conventions have begun to establish operational definitions aimed at elucidating the nature of AI and its profound legal implications. Among these significant:

1) The European Parliament's Definition:

In its 2020 resolution, the European Parliament defined Artificial Intelligence as: 'Software systems capable of receiving, processing, and interpreting data or inputs, and applying solutions or actions to achieve specific objectives'². It is noteworthy that this definition prioritizes the functional utility of these systems, emphasizing their data-driven operational capacity. Consequently, this renders such systems subject to legal oversight concerning data quality, integrity, and transparency³.

In 2021, the European Union introduced the Artificial Intelligence Act (AI Act) proposal, marking the first comprehensive legal framework globally designed to regulate AI. The proposed regulation defines an AI system as: 'A software system developed with specific techniques (including machine learning and logic-based approaches) that operates with a degree of relative autonomy to generate outputs such as content, predictions, or decisions that influence the environments they interact with'⁴. This definition reinforces the ethical and legal paradigms that states and institutions must adopt, effectively bridging the gap between technical capabilities and their broader socio-environmental and ethical implications⁵.

2) The OECD's Definition of Artificial Intelligence:

In its 2019 recommendations, the Organisation for Economic Co-operation and Development (OECD) defined Artificial Intelligence as: 'A set of systems and applications designed to simulate and enhance human cognitive capabilities to achieve specific objectives.'⁶ This definition underscores the critical importance of AI in replicating human cognitive processes. Consequently, it mandates that AI-

¹ See: Adel Abdel-Halim, Introduction to Artificial Intelligence and its Applications, Anglo-Egyptian Bookshop, Cairo, 2019, p. 25.

² European Parliament, Resolution of 20 October 2020 with recommendations to the vi Commission on a civil liability regime for artificial intelligence, 2020, p3.

³ See: Ahmed Oraibi Fadaam, Artificial Intelligence and International Responsibility: A Legal Analysis of Challenges and Solutions within the Framework of International Law Written, Iraqi Journal of Humanitarian, Social and Scientific Research, T No. 18A-1-Sept 2025, p689.

⁴ European Commission, Proposal for a Regulation laying down harmonised rules on Artificial Intelligence Artificial Intelligence Act.

⁵ See: Ahmed Oraibi Fadaam, op. cit., p690.

⁶ OECD, Recommendation of the Council on Artificial Intelligence, 2019, p7.

specific legislations remain intrinsically linked to the protection of individual rights, most notably privacy and the autonomy of decision-making.

3) UNESCO's Definition of Artificial Intelligence:

Within its 2021 Recommendation on the Ethics of Artificial Intelligence, UNESCO defined AI as: 'A set of systems based on computer science and digital technologies aimed at simulating human mental processes such as adaptive learning, data analysis, and decision-making with varying degrees of autonomy¹.' This definition is particularly significant in legal scholarship as it highlights the concept of 'Autonomy,' which is central to determining legal liability and the ethical governance of personal data processing.

B. The Legislative Definition of Artificial Intelligence:

1. Definition of National Legislation:

At the legislative level, national lawmakers in various Arab jurisdictions have largely refrained from establishing an explicit and definitive legal definition for Artificial Intelligence, opting instead to regulate its practical applications. In Jordan, for instance, an examination of specialized statutes such as the Copyright Law No. 22 of 1992 and the Patent Law No. 32 of 1999 reveals a noticeable legislative silence regarding a direct definition of AI. Nevertheless, the Jordanian legislator has maintained a proximity to AI concepts through functional terminology. Specifically, Article 2 of the Electronic Transactions Law No. 15 of 2015 defines an 'Electronic Agent' (or Electronic Mediator) as: 'An electronic program utilized to execute or respond to an action automatically, for the purpose of generating, sending, or receiving data messages.' This definition closely aligns with the functional attributes of AI systems, particularly their capacity for autonomous operation without direct human intervention.

It is evident that the Jordanian legislator has closely approached the functional essence of Artificial Intelligence, recognizing it as an electronic program effectively an algorithmic framework that processes information through various dimensions. By defining the 'Electronic Agent,' the legislator has implicitly aligned with the conceptual and technical parameters of AI systems.

Similarly, the Egyptian legislator has refrained from establishing a standalone, explicit definition for AI. However, within the framework of Law No. 175 of 2018 on Combating Information Technology Crimes, a comprehensive definition of 'Electronic Processing' was established, representing the foundational role of AI. The Egyptian legislator defines processing as: 'Any electronic or technical operation, performed wholly or partially, to write, collect, record, preserve, store, merge, display, send, receive, circulate, publish, erase, change, modify, retrieve, or derive electronic data and information... utilizing any electronic, magnetic, or optical media, or any emerging technologies.' Furthermore, in the context of personal data

¹ UNESCO, Recommendation on the Ethics of Artificial Intelligence, 2021, p5.

protection, the legislator emphasizes 'Data Analysis,' which constitutes the hallmark of AI capabilities.

This legislative trend is further mirrored by the Algerian legislator in Law No. 25-11 (relative to the protection of individuals in the processing of personal data). Article 3 defines 'Processing' as: 'Any operation or set of operations performed upon personal data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction¹.' By encompassing 'automated means' and 'alignment/combination,' the Algerian law effectively covers the technical mechanisms through which AI systems interact with personal data.

Similarly, the Algerian legislator, through Law No. 25-11, established an explicit and comprehensive definition of 'Personal Data Processing.' Under Article 3, processing is defined as: 'Any operation or set of operations performed upon personal data, whether by automated means or otherwise, including collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or any other form of making available, alignment or combination, as well as blocking, encryption, erasure, or destruction².' This broad and inclusive definition ensures that modern technological processes particularly those driven by Artificial Intelligence are strictly governed by the legal safeguards intended to protect individual privacy and data integrity.

Furthermore, 'Electronic Communication' is defined as: 'Any transmission, emission, or reception of signs, signals, writing, images, sounds, data, or information of any nature, conveyed via wire, optical fiber, electromagnetic systems, or any other similar technical means.³' This expansive definition serves as the fundamental technical framework through which AI systems interact and exchange data. By encompassing various physical and virtual mediums, the law ensures that the digital flow of information remains subject to legal governance, regardless of the underlying technology employed.

From the foregoing, it is evident that the Algerian legislator, by establishing an explicit definition for the processing of personal data via automated means and electronic communication the very core of AI's functional role has effectively addressed the contemporary digital revolution. This proactive legislative approach aligns with the rapid advancements in Artificial Intelligence, which pose unprecedented legal challenges to data protection. While AI technologies serve as a primary catalyst for innovation and economic development, they simultaneously present fundamental challenges regarding the right to privacy and the sanctity of personal data.

¹ See: Article 3, Paragraph 3 of Law No. 25-11.

² See: Article 3, Paragraph 5 of Law No. 25-11

³ See: Article 3, Paragraph 11 of Law No. 25-11

In contrast, the French legislator has yet to establish an explicit and definitive legal definition for Artificial Intelligence, despite the existence of various technical frameworks. Consequently, legal jurisprudence (Doctrine) has undertaken the task of defining this concept. Although a unified and universally accepted definition remains elusive, the conceptualization of AI has proven to be and continues to be a fertile ground for scholarly debate. Jurisprudential efforts have produced a multitude of definitions, yet they have not reached a consensus on an all-encompassing and exclusive.

2. Legal Jurisprudential Definitions of Artificial Intelligence

Legal jurisprudence (Doctrine) has offered various definitions for Artificial Intelligence, most of which remain closely aligned with its technical essence. It is often defined as: 'A set of software programs designed to enable machines to achieve specific objectives by mimicking human behavior, or at times, exceeding human capabilities.' Others view AI as the capacity of digital computers and machines to perform tasks that simulate human intelligence, such as reasoning, learning from past experiences, and executing complex cognitive processes¹. Furthermore, AI is characterized as: 'Human-made intelligence embedded within machines or computers,' or the science of enabling machines to perform actions that traditionally require human intellect essentially seeking to transpose human cognitive functions into hardware and software systems².

Subsection II: The Impact of AI on Personal Data and Protection Mechanisms

This section explores the implications of Artificial Intelligence through the following frameworks:

A. The Impact of AI on Traditional and Emerging Perspectives of Data Privacy:

1. Traditional Perspectives of the Right to Data Privacy:

Every individual possesses the inherent right to maintain their privacy and lead a life shielded from unauthorized publicity. Defining 'privacy' remains a complex task due to its relative nature, varying across environments and evolving alongside political, social, and religious shifts. While its elements are not exhaustive, they fundamentally encompass emotional and family life, health status, financial disclosures, private communications, political opinions, and the sanctity of one's domicile, name, and professional identity. This right has garnered significant recognition through international instruments and constitutional protections.

The integration of Artificial Intelligence has fundamentally altered the jurisprudential grounding of this right. Historically, the protection of personal data was viewed primarily through the lens of criminal law; however, the advent of AI in data processing has accentuated its civil dimension. This digital revolution has shifted

¹ See: Khalid Hassan Ahmed Lutfi, *Artificial Intelligence and its Protection from Civil and Criminal Perspectives*, Dar Al-Fikr Al-Jami'i, Alexandria, 2021, pp. 14-15.

² See: Abdullah Saeed Abdullah Al-Wali, *Civil Liability for Damages Caused by Artificial Intelligence Applications in UAE Law*, Dar Al-Nahda Al-Ilmiyya, UAE, 2021, p. 29.

the nature of potential infringements from third-party 'criminal acts' to 'regulatory and civil interventions.' Consequently, personal data has become the primary subject of protection in the AI era a distinction that was largely absent in earlier traditional legislations. This shift prompted the United Nations to establish a guiding framework for commercial enterprises, mandating respect for individual privacy and prohibiting the exploitation of data for commercial gain, under penalty of civil and criminal liability¹.

2. Emerging Dimensions of the Right to Data Privacy in the AI Era:

New manifestations of the right to data protection have emerged, most notably the 'Right to Digital Data Control.' The pervasive use of smart devices and the necessity of global information networks have made individuals increasingly reliant on AI systems that possess 'infinite memory' and the capacity to store vast amounts of data indefinitely. Consequently, legal jurisprudence has solidified the 'Right to be Forgotten.' This essential right empowers users to demand that their personal data not be retained perpetually and ensures that such data is not processed or stored by 'Data Controllers' in the absence of a legitimate or lawful justification².

Building upon the aforementioned, the 'Right to Digital Data Control' represents a modern legal construct, formally enshrined within the European Union through the General Data Protection Regulation (GDPR) of 2016. Its significance is paramount for social media users, whose personal data is frequently harvested without their knowledge or explicit consent for commercial exploitation by advertising firms. Moreover, the prolonged retention of data often exceeding the original purpose of collection directly contravenes European data protection principles. Consequently, it has become imperative to establish a unified international framework to determine maximum retention periods. Furthermore, digital platforms should be mandated to develop AI algorithms capable of the automated erasure of personal data upon the expiration of legal retention periods. This includes the complete removal of comments and tangential information associated with a user's profile immediately following account deletion or platform exit.³

B. Foundations and Regulatory Standards for Personal Data Protection in the AI Era

The rapid evolution of digital data processing, characterized by the pervasive integration of intelligent systems into all facets of human life, has created a profound intersection with fundamental individual rights. Most critical among these is the right to privacy, as the processing and circulation of sensitive data now touch the very core of human dignity an issue that increasingly preoccupies legal scholars seeking to establish robust protective frameworks. The correlation between 'Digital Identity' and

¹See :Sawsan safi Salih, The Impact of Artificial Intelligence on Personal Rights, Journal of Education for Humanities, Volume (05), Special Issue, April 2025, p. 1035.

² See: Sawsan safi Salih, op. cit., p1036.

³ See: Sawsan safi Salih, op. cit., p1036.

the personal data of users within these intelligent environments manifests primarily through the following dimensions:

1. Data Collection and Storage within Intelligent Environments

Artificial Intelligence, particularly through Autonomous Learning Algorithms, has introduced sophisticated methods for collecting and storing user data, effectively transforming it into high-dimensional technical databases. This technological leap has significantly amplified the capacity for large-scale data retention, processing, and dissemination, thereby posing a direct threat to individual privacy. Consequently, it has become increasingly feasible to reconstruct an individual's professional, social, financial, and medical profile and even their private relationships by accessing stored data aggregates and digital activities processed via internet platforms and virtual environments¹.

This technological trajectory has fundamentally altered the interaction with the human essence, shifting from traditional nominal identification to a paradigm governed by data and algorithmic processing within virtual environments. Consequently, the natural human personality has been transposed into a 'Digital Persona' a legal fiction existing within a virtual society predicated on self-quantification and technical algorithms. This transformation has facilitated the rise of global conglomerates whose primary function is the systematic collection, classification, and reproduction of user data into a form of 'Intangible Grey Matter' susceptible to possession, exploitation, and trade. Prominent examples include the data harvesting mechanisms of Google (notably through 'Cookies'), Wikipedia, and Facebook. In this context, personal data has evolved into a strategic source of wealth, power, and competitive advantage among the dominant entities controlling the digital landscape².

The pervasive nature of data collection and storage has facilitated both authorized and unauthorized access to these algorithmic infrastructures. This accessibility enables the scrutiny, utilization, and even the exploitation of personal data, often disregarded for its private and sensitive character. Such practices constitute a profound infringement upon the inherent personal rights of the data subject. Consequently, this necessitates the establishment of robust legal safeguards to mitigate these violations and ensure the sanctity of individual privacy against technological encroachment.

2. Data Processing and Algorithmic Autonomy:

The systematic collection of data embedded within digital identities has paved the way for advanced technologies to process and deploy this information through complex algorithmic frameworks. These systems often operate with a high degree of

¹ See: Ibrahim Attia Mahmoud, The Right to Digital Identity in Light of Personal Data Protection and Informational Privacy: A Comparative Descriptive and Analytical Study, Journal of Economic and Legal Research, Mansoura University, Issue 84, June 2023, p. 520.

² See: Khalid Hassan Ahmed, The Right to Personal Data Privacy Between Legal Protection and Technical Challenges: A Comparative Study, Dar al-Kutub wa al-Dirasat al-Arabiya, Cairo, 2020, p. 85..

functional autonomy and self-management, largely beyond the direct oversight of natural persons. This digital dominance - characterized by the autonomous exploitation of data without explicit authorization - constitutes a direct infringement upon the data subject's privacy¹. Such practices represent a significant breach of personal data security and a threat to the integrity of the 'Digital Identity.' Consequently, the processing of data via AI algorithms has emerged as a fundamental challenge in the technical nexus between digital identity and intelligent systems. This creates a critical intersection where personal data, which embodies the right to privacy, overlaps with the essential elements required for the very existence and functionality of a digital identity².

For the technical processing and retention of personal data to be deemed legally permissible, several mandatory conditions must be satisfied. These include:

- a. **Legitimacy and Specification of Purpose:** Data collection and retention must serve a lawful, specific, and predefined purpose that is clearly communicated to the data subject.
- b. **Accuracy and Security:** The collected and stored data must be accurate, intact, and protected by robust objective and personal security measures.
- c. **Lawfulness of Processing:** The processing of data must be conducted through lawful means, consistently aligned with the original purpose for which the data was collected and stored.
- d. **Storage Limitation:** The retention of data must not exceed the duration necessary to fulfill the intended purpose. Consequently, data storage and retention must terminate once the underlying necessity for such data ceases to exist³.

It is observable that the continuous proliferation and pervasive use of Artificial Intelligence (AI) have significantly expanded the scope of automated personal data processing. This technological surge has simplified the reconstruction of 'Digital Identities', making individuals increasingly identifiable and their data more accessible for storage and processing often without their adequate knowledge of the nature, methods, or underlying objectives of such technical operations. Consequently, this creates a critical legal lacuna that necessitates the development of robust regulatory frameworks to address unauthorized processing. Moreover, it is imperative to establish mechanisms that ensure the right to 'Informational Self-Determination', enabling data subjects to monitor and control the storage of their data, strictly limiting such activities to the extent permitted or necessitated by the specific, intended purpose of the retention.

¹ See: Ibrahim Attia Mahmoud, op. cit., p. 521.

² See: Khalid Hassan Ahmed, op. cit., p.73.

³ See: Articles (1-6) of the Egyptian Personal Data Protection Law No. 151 of 2020.

3. Legal Protection of Personality Rights Against the Implications of Artificial Intelligence:

Individual control over personal data has emerged as a fundamental legal concern, necessitating robust protection against the indefinite retention of information. Such retention inherently restricts basic rights, most notably the 'Right to be Forgotten' the right of individuals to have their data erased when they no longer wish for it to be part of the collective digital memory. Despite this, data often remains stored by third parties and resurfaces long after the processing necessity has lapsed. To mitigate this risk, there has been a significant push to hold digital platforms and data controllers accountable. This right gained substantial momentum in Europe following the landmark ruling of the Court of Justice of the European Union (CJEU) in Case C-131/12 (Google Spain v. AEPD), dated May 13, 2014. Consequently, the European legislature emphasized the imperative of establishing concrete guarantees to safeguard this right within the digital ¹.

4. Substantive Rights under the General Data Protection Regulation (GDPR) 2016:

The European Legislature, through the General Data Protection Regulation (GDPR) of 2016, established a comprehensive framework of rights designed to protect individuals against the risks inherent in all forms of personal data processing. These include the Right to be Informed and the Right of Access, as enshrined in Article 15. This article confirms the data subject's right to obtain verification as to whether their personal data is being processed and, if so, to access such data and related information. Furthermore, the Right to Rectification, stipulated in Article 16, empowers the data subject to have inaccurate personal data corrected and incomplete data supplemented via a supplementary statement. Other pivotal protections include the Right to Restriction of Processing, the Right to Object, and the crucial Right not to be subject to a decision based solely on automated processing, including profiling.

C. Risks to Personal Data in the AI Era

Personal data within the digital sphere is exposed to multifaceted risks arising from Artificial Intelligence integration, primarily including:

- 1) **Privacy Threats and Cyber-Criminality:** The massive aggregation of data by various entities and corporations raises significant concerns regarding its potential use in facilitating illicit acts, commonly known as Cybercrime. The density of data collection increases the vulnerability of individuals to unauthorized exploitation and algorithmic manipulation.
- 2) **Encroachment on the Right to Private Life:** The misuse of information technology has expanded the scope of violations against individual privacy² In this context, computer systems may become a direct target for

¹ See: Sawsan safi Salih, op. cit., p103.8

² See: Maghabeb Naeem, Risks of Information Technology and the Internet to Private Life and its Protection: A Comparative Study, Halabi Publications, Lebanon, 1998, p. 161.

criminal activity, specifically through breaches of confidentiality. Personal data can be surreptitiously accessed via specific web-based platforms, leading to serious privacy violations. These manifest in the unauthorized use, distribution, or disclosure of sensitive personal information - such as medical records or financial status - obtained through illicit means and subsequently leaked to the public¹. Accordingly, Article 5 of the General Data Protection Regulation (GDPR) mandates that both corporate entities and governmental institutions adhere to fundamental principles when processing personal data. These principles encompass transparency, purpose limitation, data accuracy, storage limitation, integrity, and confidentiality. Furthermore, data controllers are legally obligated to respond to data subjects' requests regarding the right of access, rectification, or erasure (the right to be forgotten), in strict accordance with the provisions of Articles 15 through 17 of the aforementioned Regulation².

3) Personal data is increasingly susceptible to unauthorized access, commonly referred to as hacking or cyber-intrusion. This involves breaching computer systems via the internet to copy or manipulate data by exploiting digital vulnerabilities within hardware or network infrastructures³. Such intrusions are often executed through the deployment of malware or viruses designed to destroy or alter stored files and data, including the unlawful seizure of personal information during transmission⁴. Furthermore, the techniques for assaulting personal data have diversified to include the use of data-sniffing programs, the exploitation of search engine databases for illicit commercial purposes, and the unauthorized use of network connectivity tools and wireless communication mediums⁵.

4) The expansion of information markets has created a fertile environment for computer-related crimes. Currently, a significant portion of the internet economy revolves around targeted advertising, which relies heavily on the exploitation of personal databases. These datasets possess immense economic value and are frequently traded within the 'Black Market for Information.' Such illicit trade involves the sale of stolen sensitive data, including medical records, private email communications, and proprietary corporate information.[1] The

¹See :Ahmed Abdel Salam Hassan, Salma Ghadban Hussein, Using artificial intelligence to combat cybercrime, Annual Scientific Symposium ... Law and Modern Technology in Light of Contemporary Global Developments, No. 10, pp. 133-134.

² See: Kawther Sadiq Musa, The Right to Privacy and the Risks of Artificial Intelligence, Al-Nahrain Journal of Legal Sciences, College of Law - Al-Nahrain University, Vol. 27, No. 3/P1, 2025, p. 254.

³ See: Abdel Fattah Bayoumi Hegazy, Forgery in Computer and Internet Crimes, 1st ed., Dar al-Kutub al-Qanuniya, Al-Mahalla al-Kubra, 2008, p. 123.

⁴ See : Al-Masri Youssef, Information and Digital Crimes of Computers and the Internet, 1st ed., Dar al-Adala, Egypt, 2011, p. 25.

⁵ See: Hezam Fatiha, Legal Guarantees for the Processing of Personal Data: A Study in Light of Law 18-07, Al-Ijtihad Journal for Legal and Economic Studies, Faculty of Law and Political Science, University of Tamanghasset, Vol. 8, No. 4, 2019, p. 289.

commodification of personal data has thus transformed privacy violations from mere technical breaches into a lucrative global criminal enterprise¹.

Section II: The Legal Basis for Personal Data Protection in the Digital Environment

In alignment with Algeria's strategic transition toward E-Government and in fulfillment of its international obligations, the Algerian legislature has proactively modernized the national legal framework. Notably, Article 47 of the 2020 Constitution enshrines the protection of natural persons in the processing of personal data as a fundamental right. This constitutional mandate ensures that such data is protected by law and expressly penalizes any infringement upon it². In tandem with constitutional guarantees, Articles 303 bis through 303 bis 3 of the Algerian Penal Code stipulate criminal penalties for any intentional infringement upon the sanctity of private life, regardless of the technology employed³. Furthermore, the legislative framework governing digital transactions specifically Articles 61 and 68 of Law No. 15-04 concerning Electronic Signature and Certification prohibits the unauthorized disclosure or use of third-party signature creation data. These provisions underscore the legal obligation to maintain the confidentiality of personal data and strictly prohibit its collection without the explicit consent of the data subject, under the threat of severe penal sanctions⁴. "This approach is further reinforced by Articles 11, 26, and 31 of Law No. 18-05 concerning Electronic Commerce. These provisions mandate that electronic vendors incorporate, within their general terms of sale, robust measures for the protection and confidentiality of personal data. Furthermore, they establish the fundamental principle of 'Purpose Limitation', strictly prohibiting the processing or use of such data for any objectives other than those explicitly specified at the time of collection⁵.

To complete this legislative architecture, the Algerian legislature enacted Law No. 18-07, subsequently amended and supplemented by Law No. 25-11, concerning the protection of natural persons in the processing of personal data⁶. This specialized framework serves as the primary legal instrument for safeguarding the sanctity of private life and personal data within the digital environment⁷. Law No. 25-11

¹ See: Al-Sharif Ali Bashir & Abdel Ghani Jumaa, Applications of Artificial Neural Networks, Tishreen University, Latakia, 2012, pp. 7-9.

² See: Article 47 of Presidential Decree No. 20-442, issued on December 30, 2020, regarding the issuance of the Constitutional Amendment approved in the referendum of November 1, 2020, Official Gazette of the People's Democratic Republic of Algeria, No. 82, published on December 30, 2020, p. 13.

³ See: Articles 303 bis to 303 bis 3 of the Algerian Penal Code, amended and supplemented by Law No. 24-06, dated April 28, 2024, Official Gazette No. 30.

⁴ See: Articles 61 and 68 of Law No. 15-04, dated February 1, 2015, defining the general rules for electronic signature and certification, Official Gazette No. 06, published on February 10, 2015, pp. 6-16.

⁵ See: Articles 11, 26, and 31 of Law No. 18-05, dated May 10, 2018, concerning Electronic Commerce, Official Gazette No. 28, published on May 16, 2018, pp. 4-10.

⁶ See: Law No. 18-07, dated June 10, 2018, concerning the protection of natural persons in the processing of personal data, Official Gazette No. 34, published on June 10, 2018, pp. 11-24.

⁷ See: Yazid Bouhalit & Abderrahmane Fetnaci, The Administrative and Penal Protection of Personal Data pursuant to Act 18-07, Journal of Legal and Political Research, Vol. 06, No. 02, December 2021, pp. 56-57.

specifically aims to regulate processing operations, ensuring their legitimacy and integrity, particularly when interacting with Artificial Intelligence algorithms. Under this framework, lawful processing necessitates a precise definition of legal concepts and strict adherence to data quality principles. This section explores the legal foundations of personal data protection in the digital sphere through the following points:

Subsection I: Legal Definitions of Personal Data

This section elucidates the definition of personal data and the newly introduced legal concepts under Law No. 25-11.

A. Definition of Personal Data:

Defining Personal Data The Algerian legislature provided a comprehensive definition of personal data in Article 3(1) of Law No. 25-11, describing it as: 'Any information, regardless of its support, relating to an identified or identifiable natural person hereinafter referred to as the "Data Subject" directly or indirectly, particularly by reference to an identification number or to one or more factors specific to their physical, physiological, genetic, biometric, mental, economic, cultural, or social identity.' > In comparison, the Tunisian legislature defines it as: 'Any data, regardless of its source or form, that renders a natural person identified or identifiable, directly or indirectly¹. Conversely, the French legislature, pursuant to Law No. 2004-801 (amending Law No. 78-17), focuses on the processing aspect, defining personal data within the context of: 'The automated processing of personal data, as well as the non-automated processing of personal data contained or intended to be contained in files².

Based on the definition provided in Article 3 of Law No. 25-11, it can be inferred that the scope of legal protection extends to identified or identifiable natural persons. This identifiability is established through specific distinctive elements relating to their physical, physiological, genetic, biometric, mental, economic, cultural, or social identity³. Consequently, this framework encompasses criminal acts targeting confidential or protected data, as well as infringements upon personal data linked to the constitutionally guaranteed sanctity of private life⁴.

Furthermore, Article 3(3) of the same Law clarifies the nature of processing operations. It defines processing as any operation or set of operations performed through automated means upon personal data, including but not limited to the collection, recording, organization, storage, adaptation, retrieval, consultation, use, disclosure, encryption, erasure, or destruction of such data⁵.

¹ See: Tunisian Organic Law No. 63, dated July 27, 2004, concerning the Protection of Personal Data, Article 4, p. 2.

² Law No. 2004-801 of August 6, 2004, relating to the protection of individuals with regard to the processing of personal data and amending Law No. 78-17 of January 6, 1978, relating to data processing, files, and liberties, JORF, August 7, 2004, No. 182.

³ See: Article 3 of Law No. 25-11

⁴ See: Abboud Jaafar Ali, *Modern Information Technology Crimes against Individuals and Government*, 1st ed., Zein Legal Publications, Beirut, Lebanon, 2013, p. 88.

⁵ See: Article 3(3) of Law No. 25-11

Comparative jurisdictions have consistently sought to define personal data with technical and legal precision. Article 2 of French Law No. 78-17 (dated January 6, 1978) defines personal data as: 'Any information relating to an identified or identifiable natural person, directly or indirectly, by reference to an identification number or one or more factors specific to them.' Similarly, the Egyptian Legislature, in Law No. 151 of 2020, adopted a broader approach, defining it as: 'Any data relating to an identified or identifiable natural person, directly or indirectly, through the linkage of such data with any other information, such as name, voice, image, identification number, online identifier, or data defining psychological, health, economic, cultural, or social identity.' A scrutiny of these legislative positions reveals a fundamental consensus: personal data is defined by the criterion of identifiability, whether achieved through direct elements or indirect indicators. However, the Egyptian legislature notably expanded the scope of identification to include digital identifiers, biometric markers (voice and image), and socio-economic indicators, all of which constitute the core of informational privacy.

From a jurisprudential standpoint, the nature of personal data reflects its intrinsic link to the natural person. It is established that while such data defines an individual's identity, it is not inherently 'confidential' in every context. A crucial distinction must be drawn between privacy and secrecy; information used for social identification and communication is not necessarily secret unless explicitly designated as such by the data subject. Thus, personal data encompasses any indicator or set of data that enables the identification of, or communication with, a natural person, directly or indirectly, by linking their personality to their identifying information¹.

B. Newly Introduced Legal Concepts Under Law No. 25-11:

1 . Modernizing Legal Definitions to Align with Artificial Intelligence Technologies:

The conceptual framework of Law No. 25-11, particularly Article 3, represents a pivotal convergence between legislative text and Artificial Intelligence (AI) advancements. The legislature recognized that the absence of precise definitions for AI-related concepts constituted a significant lacuna in the amended Law No. 18-07, potentially leading to inconsistencies in judicial application and interpretation.

Consequently, the Algerian legislature responded to these technical shifts by incorporating a new set of definitions. Article 3 now includes a sophisticated terminology that reflects the reality of current technological evolutions, most notably: **Biometric Data** is defined as personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allow or confirm their unique identification². This definition is of paramount importance given the proliferation of Artificial Intelligence (AI)

¹ See: Ibrahim Attia Mahmoud, op. cit., p. 509.

² See: Article 3(22) of Law No. 25-11.

systems based on **facial recognition**, fingerprinting, and voiceprint analysis, now widely utilized in security, financial services, and recruitment.

Furthermore, the legislature introduced the concept of '**Profiling**', defined as: 'Any form of automated processing of personal data to evaluate certain personal aspects relating to a natural person, particularly to analyze or predict elements concerning their performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements'¹. Such data, alongside genetic and health information, are classified as '**Sensitive Data**', the processing of which is generally prohibited except in specific legally defined circumstances. This inclusion represents a **legislative breakthrough**, as profiling constitutes the core of AI applications in targeted advertising, recommendation systems, and automated hiring.

Additionally, the law defines '**Pseudonymization**' as: 'The processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information'². This technique serves as a fundamental **risk-mitigation tool** in AI environments, allowing for model training while safeguarding individual identities. Incorporating these definitions transcends mere terminology; it reflects the legislature's intent to establish a functional synergy between legal norms and technological advancements, enabling the precise application of law to digital realities.

2. Principles of Data Quality and Lawfulness of Processing:

Law No. 25-11 mandates that all data processing operations must be conducted with due respect for human dignity, private life, and public liberties. As a general rule, 'Explicit Consent' from the data subject constitutes the primary legal basis for processing. However, this requirement is subject to specific derogations in the interest of public safety and criminal justice. Under Article 45 bis of Law No. 25-11, and notwithstanding the provisions of Articles 7 and 8, prior consent is not required when data processing is strictly necessary for crime prevention, detection, criminal investigations, prosecutions, or the execution of penal sanctions³.

Furthermore, Article 9 establishes rigorous criteria for Data Quality, requiring that all processed data must adhere to the following principles⁴:

- **Lawfulness, Fairness, and Transparency:** Processing must be conducted in accordance with the law and in a transparent manner.
- **Purpose Limitation:** Data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.

¹ See: Article 3(23) of Law No. 25-11.

² See: Article 3(24) of Law No. 25-11.

³ See: Article 45 bis paragraph (4) of Law No. 25-11.

⁴ See: Article 9 of Law No. 25-11.

- **Data Minimization and Accuracy:** Data must be adequate, relevant, and limited to what is necessary (proportionality), as well as accurate and kept up to date.
- **Storage Limitation:** Data must not be kept for longer than is necessary for the purposes for which it is processed.

It is noteworthy that the material scope of Law No. 25-11 explicitly excludes and prohibits certain forms of data processing as specified in Article 5. Furthermore, the following categories of personal data are exempted from the application of this Law: (i) data processed by a natural person strictly for personal or domestic purposes, provided such data is neither disclosed to third parties nor published; and (ii) data pertaining to national defense and state security¹. Additionally, the processing of 'Sensitive Data' is generally prohibited², except under the stringent conditions and safeguards mandated by Article 18 of Law No. 25-11.

Subsection II: Mechanisms for Personal Data Protection Against Artificial Intelligence Challenges

The discourse on Artificial Intelligence (AI) is inseparable from the increasing complexity of data processing operations, a reality that necessitated legislative intervention to strengthen governance and oversight mechanisms. The legislature addressed this necessity through a suite of regulatory instruments introduced by Law No. 25-11, the most significant of which are outlined below:

A. Mandatory Appointment of the Data Protection Officer:

Pursuant to Article 41 bis of Law No. 25-11, every data controller is mandated to appoint a Data Protection Officer (DPO). This officer must be selected based on professional qualities, with particular emphasis on specialized knowledge of data protection law and practices³.

This obligation is crucial within the context of AI complexities, as the presence of a permanent expert within an organization or administration facilitates:

- **Risk Assessment:** Evaluating risks associated with AI systems prior to their implementation.
- **Regulatory Compliance of Profiling:** Ensuring that 'Profiling' operations adhere strictly to legal frameworks.
- **Oversight of DPIAs:** Supervising Data Protection Impact Assessments (DPIA) for high-risk processing operations.

B. Establishment of Regional Oversight Hubs:

The National Authority for the Protection of Personal Data (ANPDP) serves as the primary institutional mechanism for the oversight and protection of personal data. Functioning as an independent administrative body under the Presidency, it ensures respect for the rights of natural persons, including the right to information upon data

¹ See: Articles 5 and 6 of Law No. 25-11.

² See: Article 18 of Law No. 25-11.

³ See: Article 41 bis of Law No. 25-11

collection, the right of access, and the right to rectification or erasure of inaccurate data. Furthermore, data subjects hold the right to object to processing for legitimate reasons, particularly in the context of direct marketing¹.

The Authority possesses extensive powers, ranging from granting authorizations and receiving declarations to conducting on-site investigations and inspections. It is also empowered to impose administrative sanctions and refer matters involving potential criminal offenses to the Public Prosecutor.

In this context, Law No. 25-11 granted the ANPDP the authority to establish Regional Oversight Hubs tasked with auditing and monitoring data controllers and processors². This mechanism aims to decentralize oversight and ensure effective monitoring amid the nationwide proliferation of Artificial Intelligence (AI) technologies. Consequently, the legislature has transitioned from theoretical protection to the imposition of practical mechanisms that safeguard data integrity while bolstering the Authority's role as an independent regulatory body.

However, despite the statutory mandate in Law No. 25-11, these regional hubs have not yet been established, as the executive decree specifying the conditions and modalities for their creation remains pending.

C. Risk Assessment, Breach Notification, and Constraints on Automated Decision-Making:

By its very nature, Artificial Intelligence (AI) encompasses high-risk technologies that may impact fundamental rights and freedoms, particularly when processing vast datasets (Big Data) or employing Machine Learning algorithms that may harbor unintended biases. To manage these risks, Law No. 25-11 introduced new statutory obligations:

1. Data Protection Impact Assessment (DPIA):

The law mandates a prior risk assessment when utilizing new technologies likely to result in high risks to the rights of natural persons. The data controller is obligated to conduct a DPIA that includes a general description of processing operations, an assessment of potential risks, and the measures adopted to mitigate them³.

2. Data Breach Notification:

The legislature requires data controllers to notify the National Authority (ANPDP) of any personal data breach within a maximum period of five (05) days from the date of discovery⁴. This rigorous timeframe is critical in the AI era, where the rapid dissemination of data can amplify the consequences of security failures. Furthermore, the data subject must be informed when a breach is likely to result in a high risk to their rights⁵.

3. Restrictions on Automated Decisions:

¹ See: Articles 32 to 37 of Law No. 25-11

² See: Article 27 bis of Law No. 25-11.

³ See: Article 45 bis (6) of Law No. 25-11

⁴ See: Article 45 bis (8) of Law No. 25-11.

⁵ See: Article 45 bis (10) of Law No. 25-11.

A fundamental constraint has been placed on AI applications under Article 45 bis (1). It explicitly stipulates that judicial rulings or decisions producing legal effects concerning an individual cannot be based solely on 'Automated Processing' intended to define the subject's profile or evaluate specific aspects of their personality¹.

D. Regulating Cross-Border Data Transfers in the Era of Digital Globalization

One of the most profound challenges posed by Artificial Intelligence (AI) applications is their heavy reliance on Cloud Computing infrastructures and international platforms, which inherently raises the complex issue of cross-border data transfers. The Algerian legislature addressed this complexity by establishing stringent protocols in the new Law. Specifically, any transfer of personal data abroad is strictly subject to prior authorization from the National Authority (ANPDP)². The evaluation of such requests is based on rigorous criteria, including:

- **Adequacy of Protection:** The level of legal and technical protection afforded by the recipient country.
- **Fundamental Rights:** The extent to which the recipient country respects human rights and basic freedoms.
- **Independent Oversight:** The existence and effectiveness of an independent regulatory body in the country of destination.

These safeguards clearly demonstrate the legislature's endeavor to balance the benefits of global AI technologies with the preservation of National Data Sovereignty. By preventing any dilution of the protection granted to data subjects, this regulatory framework reflects a sophisticated legislative maturity in reconciling the requirements of national security with the fundamental rights of individuals.

E. Security and Judicial Processing of Personal Data

The legislature dedicated Chapter V bis to regulating the processing of personal data by security and judicial agencies. Pursuant to Article 45 bis, the entities authorized to process personal data for the purposes of crime prevention, detection, investigation, criminal prosecution, and the execution of penal sanctions are strictly limited to the following:

- **The Judiciary:** Including all competent judicial authorities.
- **Authorized Law Enforcement Agencies:** Departments and bodies legally mandated to investigate crimes and identify perpetrators within their specific jurisdictions.
- **Judicial Assistants:** Acting within their legal competencies and for a duration proportionate to their assigned tasks.
- **Prison Administration Services:** Within the scope of their statutory authority and mandates.

Furthermore, any processing conducted under this article must explicitly identify the Data Controller, the specific purpose of the processing, the categories of data

¹ See: Article 45 bis (1) paragraph (1-2) of Law No. 25-11

² See: Articles 45 bis, 45 bis (13), and 45 bis (14) of Law No. 25-11

subjects, and the third parties authorized to access such information. It must also specify the source of the data and the security measures implemented to ensure processing integrity, all while adhering strictly to the fundamental principles of data quality enshrined in Article 9(1) of this Law.

Conclusion:

In conclusion, Law No. 25-11 constitutes a significant milestone in Algeria's legislative trajectory, reflecting a strategic legal recognition of the global digital revolution. As the world transitions toward a data-driven society, personal data has emerged as a high-value asset and a primary target for diverse actors, ranging from sovereign states and public institutions to private entities and even illicit groups. This digital shift has been accompanied by the rise of sophisticated technologies, such as Artificial Intelligence (AI) and Machine Learning, which have heightened the complexity of data processing and introduced unprecedented risks to individual privacy. The pervasive expansion of information technology while a catalyst for progress has intensified concerns regarding the illicit collection, storage, and processing of personal data, fostering a growing sense of vulnerability in the face of modern technological threats.

It is evident from this study that the protection of natural persons in the context of data processing has become a priority for the Algerian legislature. Law No. 25-11 represents a watershed moment in Algerian legal history, aligning the national framework with international standards during an era of increasing AI dependency. Although recently enacted, this law places Algeria among the nations possessing an advanced legal architecture for data protection. Ultimately, the true challenge lies in the efficacy of its enforcement, the promotion of legal awareness, and the empowerment of regulatory bodies to perform their oversight functions competently amidst the rapid and continuous evolution of the AI era.

I . Key Findings and Results:

In light of the foregoing analysis, the study concludes with several pivotal findings regarding the efficacy of Law No. 25-11:

1. **Legislative Gap Closure:** The legislature has successfully addressed previous statutory lacunae by introducing precise legal definitions for critical concepts, such as Biometric Data and Profiling, ensuring a more comprehensive protective scope.
2. **Strengthening the Institutional Framework:** The law has fortified the institutional protection mechanisms by mandating the appointment of a Data Protection Officer (DPO) and granting the National Authority (ANPDP) broader powers to establish Regional Oversight Hubs, thereby fostering a culture of preventive compliance.
3. **Consolidating Data Sovereignty:** The establishment of stringent protocols for cross-border data transfers has bolstered national data sovereignty,

safeguarding information from illicit exploitation—a crucial measure given AI's heavy reliance on global cloud infrastructures.

4. **Balancing Security and Rights:** The regulatory framework achieves a sophisticated balance between national security requirements and the protection of fundamental rights through a specialized legal regime for judicial and security data processing.
5. **Proactive Risk Management:** The law has institutionalized rigorous risk management standards by mandating prior Data Protection Impact Assessments (DPIA) and requiring rapid notification of data breaches, thus shifting the focus from reactive to proactive protection.

II. Recommendations:

Based on the findings of this study, the following recommendations are proposed to enhance the legal and operational framework for data protection in the AI era:

1. **Enactment of a Dedicated AI Law:** Adopting a comprehensive legislative project specifically for Artificial Intelligence, aligned with the foundational principles of the EU AI Act (June 2024), to ensure a risk-based approach to AI governance.
2. **Procedural Harmonization:** Amending Article 46 of Law No. 18-07 to harmonize it with the Code of Civil and Administrative Procedure, explicitly stipulating that ANPDP decisions are appealable before the Administrative Court of Appeal in Algiers.
3. **Accelerating Regional Decentralization:** Expediting the issuance of the executive decree concerning Regional Oversight Hubs to enable widespread auditing and monitoring of data controllers across all jurisdictions.
4. **Strengthening Authorization Protocols:** Repealing the provision that allows data processing to commence merely upon filing an application; processing should strictly require explicit prior approval from the National Authority.
5. **Establishing a National AI Office:** Creating a specialized national entity, modeled after the EU AI Office, to oversee AI systems, manage licensing, and classify prohibited or high-risk systems.
6. **Capacity Building for the ANPDP:** Providing the National Authority with the necessary material, human, and technical resources to effectively perform its complex oversight duties in the digital environment.
7. **International Cooperation:** Strengthening collaborative mechanisms with regional and international counterparts to exchange expertise and combat cross-border data-related crimes.
8. **Technical Guidelines and Standardized Models:** Urging the ANPDP to issue detailed guidelines on Profiling and Automated Decision-making, alongside standardized DPIA templates tailored for modern digital platforms.

9. **Developing Dual-Competence Professionals:** Implementing specialized training programs to produce Data Protection Officers (DPOs) with dual legal and technical expertise through academic and professional partnerships.
10. **Public Awareness and Legal Literacy:** Intensifying awareness campaigns to elevate social consciousness regarding digital rights and the importance of compliance with the new data protection framework.

List of sources and references:

I. List of sources:

- 1) The Universal Declaration of Human Rights, adopted by the UN General Assembly in Paris on December 10, 1948, via Resolution 217 A (III).
- 2) The International Covenant on Civil and Political Rights, adopted and opened for signature, ratification, and accession by UN General Assembly Resolution 2200A (XXI) of December 16, 1966.
- 3) Presidential Decree No. 20-442, issued on December 30, 2020, regarding the issuance of the Constitutional Amendment approved in the referendum of November 1, 2020, Official Gazette of the People's Democratic Republic of Algeria, No. 82, published on December 30, 2020.
- 4) Law No. 25-11 of 28 Muharram 1447, corresponding to July 24, 2025, amending and supplementing Law No. 18-07 of 25 Ramadan 1439, corresponding to June 10, 2018, relating to the protection of natural persons in the processing of personal data, Official Gazette (OG) No. 48.
- 5) Law No. 18-07, dated June 10, 2018, concerning the protection of natural persons in the processing of personal data, Official Gazette No. 34, published on June 10, 2018.
- 6) Tunisian Organic Law No. 63, dated July 27, 2004, concerning the Protection of Personal Data, Article 4.
- 7) Law No. 2004-801 of August 6, 2004, relating to the protection of individuals with regard to the processing of personal data and amending Law No. 78-17 of January 6, 1978, relating to data processing, files, and liberties, JORF, August 7, 2004, No. 182.
- 8) European Parliament, Resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence, 2020.
- 9) European Commission, Proposal for a Regulation laying down harmonised rules on Artificial Intelligence Artificial Intelligence Act.
- 10) OECD, Recommendation of the Council on Artificial Intelligence, 2019.
- 11) UNESCO, Recommendation on the Ethics of Artificial Intelligence, 2021.

II. Bibliography List setting:

A. Books :

- 1) Abboud Jaafar Ali, Modern Information Technology Crimes against Individuals and Government, 1st ed., Zein Legal Publications, Beirut, Lebanon, 2013.

- 2) Abdel Fattah Bayoumi Hegazy, *Forgery in Computer and Internet Crimes*, 1st ed., Dar al-Kutub al-Qanuniya, Al-Mahalla al-Kubra, 2008.
- 3) Abdullah Saeed Abdullah Al-Wali, *Civil Liability for Damages Caused by Artificial Intelligence Applications in UAE Law*, Dar Al-Nahda Al-Ilmiyya, UAE, 2021.
- 4) Adel Abdel-Halim, *Introduction to Artificial Intelligence and its Applications*, Anglo-Egyptian Bookshop, Cairo, 2019.
- 5) Ahmad Atef Abdel-Moneim, *Artificial Intelligence and its Modern Applications*, Dar al-Fikr al-Jam'i, Alexandria, 2020.
- 6) Ahmad Mukhtar Umar, *Dictionary of Contemporary Arabic*, 1st ed., Alam al-Kutub, Cairo, 2008.
- 7) Al-Masri Youssef, *Information and Digital Crimes of Computers and the Internet*, 1st ed., Dar al-Adala, Egypt, 2011.
- 8) Academy of the Arabic Language, *Al-Mu'jam al-Wasit*, vol. 1, 4th ed., Dar al-Da'wah, Cairo, 2004.
- 9) Ibn Manzur, *Lisan al-Arab*, vol. 13, Dar Sader, Beirut, 1990.
- 10) John McCarthy, *What is AI*, Stanford University, 2007
- 11) Khalid Hassan Ahmed Lutfi, *Artificial Intelligence and its Protection from Civil and Criminal Perspectives*, Dar Al-Fikr Al-Jami'i, Alexandria, 2021.
- 12) Khalid Hassan Ahmed, *The Right to Personal Data Privacy Between Legal Protection and Technical Challenges: A Comparative Study*, Dar al-Kutub wa al-Dirasat al-Arabiya, Cairo, 2020.
- 13) Maghabeb Naeem, *Risks of Information Technology and the Internet to Private Life and its Protection: A Comparative Study*, Halabi Publications, Lebanon, 1998.
- 14) Mona Al-Ashqar Jabbour and Mahmoud Jabbour, *Personal Data and Arab Laws: Security Concerns and Individual Rights*, 1st ed., Arab Center for Legal and Judicial Research, League of Arab States, Council of Arab Ministers of Justice, Beirut, 2018.
- 15) Nils J. Nilsson, *The Quest for Artificial Intelligence: A History : of Ideas and Achievements*, Cambridge University Press, 2010.
- 16) Omar Nafe' Reda al-Abbasi, *The Legal System of Artificial Intelligence*, 1st ed., Arab Center for Publishing and Distribution, Cairo, 2023.

B. Journal article :

- 1) Abu al-Fadl Jamal al-Din Muhammad ibn Mukram Ibn Manzur, *Lisan al-Arab*, vol. 6, 4th ed., Dar Sader for Printing and Publishing, Beirut, 2005.
- 2) Ahmed Abdel Salam Hassan, Salma Ghabban Hussein, *Using artificial intelligence to combat cybercrime*, Annual Scientific Symposium ... Law and Modern Technology in Light of Contemporary Global Developments, No. 10.
- 3) Ahmed Oraibi Fadaam, *Artificial Intelligence and International Responsibility: A Legal Analysis of Challenges and Solutions within the Framework of*

International Law Written, Iraqi Journal of Humanitarian, Social and Scientific Research, T No. 18A-1-Sept 2025.

- 4) Al-Sharif Ali Bashar & Abdel Ghani Jumaa, Applications of Artificial Neural Networks, Tishreen University, Lattakia, 2012.
- 5) Hezam Fatiha, Legal Guarantees for the Processing of Personal Data: A Study in Light of Law 18-07, Al-Ijtihad Journal for Legal and Economic Studies, Faculty of Law and Political Science, University of Tamanghasset, Vol. 8, No. 4, 2019.
- 6) Ibrahim Attia Mahmoud, The Right to Digital Identity in Light of Personal Data Protection and Informational Privacy: A Comparative Descriptive and Analytical Study, Journal of Economic and Legal Research, Mansoura University, Issue 84, June 2023.
- 7) Kawther Sadiq Musa, The Right to Privacy and the Risks of Artificial Intelligence, Al-Nahrain Journal of Legal Sciences, College of Law - Al-Nahrain University, Vol. 27, No. 3/P1, 2025.
- 8) Sawsan safi Salih, The Impact of Artificial Intelligence on Personal Rights, Journal of Education for Humanities, Volume (05), Special Issue, April 2025.
- 9) Stuart Russell & Peter Norvig, Artificial Intelligence: A Modern Approach, 4th ed., Pearson, 2021.
- 10) Yazid Bouhalit & Abderrahmane Fetnaci, The Administrative and Penal Protection of Personal Data pursuant to Act 18-07, Journal of Legal and Political Research, Vol. 06, No. 02, December 2021.

C. Internet websites:

- 1) Mu'jam al-Ma'ani al-Jami' (Universal Lexicon), available at: <https://www.almaany.com/ar/dict/ar-ar/>