

Mechanisms for Safeguarding Personal Data in the Era of Artificial Intelligence

Rabiaa NACIRI ⁽¹⁾

⁽¹⁾ Lecturer B, Faculty of Law and Political Science,
Department of Law, University of Tindouf (Algeria),
Email: rabiaa.naciri@cuniv-tindouf.dz

Abstract :

The right to privacy is considered one of the most important rights recognized by the Algerian legislator in the constitutional amendment of 2016, as well as under Law No. 18-07 on the protection of natural persons. This law aims to establish a legal framework for safeguarding individuals' private lives and preserving their reputation, honor, and dignity through the protection of their personal data. However, the situation has become more complex with the unreasonable use of artificial intelligence applications, which allows access to individuals' personal information, especially in the absence of specific legal regulations governing violations of personal data. This represents one of the greatest concerns facing the Algerian system.

Keywords:

Personal data, right to privacy, violation, artificial intelligence, legal protection.

Received: 28/03/2026 & Accepted: 01/06/2026 & Edited: 30/06/2026

Corresponding author: NACIRI Rabiaa, email : nacirirabiaa@yahoo.com

آليات حماية البيانات الشخصية في ظل الذكاء الاصطناعي

الملخص:

يعتبر الحق في الخصوصية من أهم الحقوق التي أقرها المشرع الجزائري في التعديل الدستوري لسنة 2016، وأيضاً بموجب القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي من أجل تأطير الحماية القانونية للحياة الخاصة للأفراد والحفاظ على سمعتهم وكرامتهم بحماية معطياتهم الشخصية، لكن ما زاد الأمر تعقيداً هو استخدام تطبيقات الذكاء الاصطناعي بشكل غير معقول وهذا ما يسمح بالدخول للبيانات الشخصية للأفراد، خاصة في ظل عدم وجود تنظيم قانوني محدد يطبق في حالة الاعتداء على البيانات الشخصية وهذا هو أحد أكبر المخاوف التي ترهق المنظومة الجزائرية.

الكلمات المفتاحية:

البيانات الشخصية، الحق في الخصوصية، الاعتداء، الذكاء الاصطناعي، الحماية القانونية.

Mécanismes de protection des données personnelles à l'ère de l'intelligence artificielle

Résumé :

Le droit à la vie privée est un droit fondamental inscrit dans la Constitution algérienne de 2016 et dans la loi 18-07 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Cette loi vise à instaurer un cadre juridique pour la protection de la vie privée, de la réputation et de la dignité des individus par la sécurisation de leurs données personnelles. Cependant, l'utilisation abusive des applications d'intelligence artificielle a complexifié la situation, permettant l'accès aux données personnelles. Ce problème est d'autant plus préoccupant que le système algérien ne dispose pas de réglementation spécifique encadrant les violations de données personnelles.

Mots clés:

Données personnelles, droit à la vie privée, violation, intelligence artificielle, protection juridique.

Introduction

The right to privacy is among the rights recognized by law for individuals, ensuring freedom from interference in their personal affairs and all matters related to their private lives. Naturally, the law protects individuals' rights from violation, infringement, or even access without prior authorization. The right to a private life therefore remains guaranteed and inviolable, and adequate protection must be provided against any form of encroachment. The concept of privacy and private life is relatively recent. The expression "the right to privacy" first appeared in an article published in 1890 by Brandeis and Warren in the Harvard Law Review in the United States. Privacy is closely tied to the essence of the human being and to the personal sphere through which one seeks to protect their feelings, thoughts, and private secrets as an expression of individual identity¹.

However, in light of the technological advancement that has come to permeate our professional, social, and economic lives—and indeed all aspects of our existence—it has become a real threat not only to individuals' data but also to their personal lives. The Internet has turned into a medium for the exchange of information, cultures, and languages, especially through the use of artificial intelligence applications, which have access to all information related to individuals on these platforms. This poses a serious threat to users, particularly when they share personal data they do not wish others to access. Such data has become widely circulated due to the rapid development of electronic storage, processing, and transmission technologies, especially within the field of information and communication technology, and following the proliferation of social media networks that have become central to our daily lives. This topic is of great importance as it addresses one of the most pressing contemporary issues: the widespread use of social media networks and artificial intelligence applications has increasingly endangered our private lives. Therefore, it is essential to ensure adequate protection of individuals' right to privacy and personal data. The Algerian legal system, like other international frameworks, was thus compelled to enact Law No. 18-07, which protects natural persons in the processing of personal data².

The concept of personal data was introduced constitutionally for the first time in the 2016 constitutional amendment³, where Article 46 stipulates that: "...

¹ Wassim Chafik Al-Hajjar, *The Legal System of Social Media (A Comparative Study on Privacy, Personal Freedom, Responsibility, and Jurisdiction)*, 1st edition, Arab Center for Legal and Judicial Research, Beirut, Lebanon, 2017, p. 37.

² Law No. 18-07 of June 10, 2018, on the protection of natural persons in the processing of personal data, *Official Journal*, June 10, 2018, No. 34.

³ Law No. 16-01 of 26 Jumada al-Awwal 1437, corresponding to March 6, 2016, containing the constitutional amendment, *Official Journal* issued on March 7, 2016, No. 14.

the protection of natural persons in the processing of personal data is a fundamental right guaranteed by law, and any violation thereof shall be punishable.” The same provisions were reaffirmed in the 2022 constitutional amendment⁴. This was previously established in Article 39 of the 1996 Constitution⁵, which stated that “the inviolability of a citizen’s private life and honor shall not be violated, and the law shall protect them. The confidentiality of correspondence and private communications, in all their forms, is guaranteed.”

There is no doubt that choosing to study the issue of personal data protection is of great importance, given its prominence on the international stage and the growing need to establish a unified international legal framework to protect individuals’ data from breaches or unauthorized access. This need has become especially pressing with the proliferation of digital media, which have become essential in our personal and professional lives to keep pace with global technological advancement.

Based on the above, the central research question that arises from this study is: How effective are the laws that the Algerian legislator has enacted concerning the personal data of individuals in providing sufficient legal protection for it, especially in light of artificial intelligence applications?

To answer this question, we adopted the analytical method by examining the provisions of Law No. 18-07, which protects natural persons in the processing of personal data. This method focuses on analyzing the relevant legal articles pertaining to our topic. We also employed the descriptive method through a survey-based approach that provides a general overview of personal data protection, especially in the context of technological development. Furthermore, we used the comparative method, which relies on comparing one legal framework with another, or a national legal text with foreign ones. In this regard, we sought to compare the Algerian legislation with other international and Arab legal systems, analyzing the legal provisions they have enacted to protect personal data and the right to privacy against the implications of artificial intelligence applications. In examining and discussing this topic, we structured our research into two main sections:

- Section One: The conceptual framework of personal data protection and artificial intelligence.
- Section Two: The legal protection of personal data from artificial intelligence applications.

⁴ Presidential Decree No. 20-442 of December 15, 2020, about the promulgation of the constitutional amendment approved by the referendum of November 1, 2020, *Official Journal* dated December 30, 2020, No. 82.

⁵ Presidential Decree No. 96-438 of December 7, 1996, on the promulgation of the 1996 Constitution, *Official Journal* issued on December 8, 1996, No. 76.

Chapter I: The conceptual framework of personal data protection and artificial intelligence

The issue of personal data protection, being a relatively recent topic in Algerian law, has required the legislator to clearly define the modern terms that have emerged alongside the advent of “artificial intelligence”⁶ applications. Accordingly, we will attempt to examine these concepts from a legal perspective through two main subsections.

Section I: Definition of Personal Data

An individual’s private life is considered an inviolable domain that must not be exposed or publicized, and no one may access it without the individual’s consent. However, technological advancement has made our lives increasingly vulnerable to violation and the disregard of personal privacy. Accordingly, we shall attempt to define what is meant by personal data, particularly in the context of artificial intelligence applications.

Privacy can be defined as a personal sphere that allows an individual to choose whether or not to interact with others, free from interference or intrusion by any undesired party. The Algerian legislator defines personal data in the law concerning the protection of natural persons in the processing of personal data as: “Any information, regardless of its medium, relating to an identified or identifiable person, hereinafter referred to as ‘the data subject,’⁷ either directly or indirectly, in particular by reference to an identification number or to one or more elements specific to their physical, physiological, genetic, biometric, psychological, economic, cultural, or social identity”⁸.

It is worth noting that personal data have evolved alongside the development of the Internet. They are no longer limited to a person’s name, surname, and postal address, but have expanded and diversified to include one’s image and voice, in addition to a range of other data related to financial capacity, behaviors, habits, preferences, and even more profoundly, biometric data related to the human body. Personal data may thus contain sensitive

⁶ Artificial intelligence is defined as “one of the modern computer sciences that seeks advanced methods to perform tasks and make inferences that, even within limited boundaries, resemble those attributed to human intelligence.” Ammar Awad Saleh, *Digital Transformation from the Past to the Future in the Age of Artificial Intelligence*, in the collective peer-reviewed volume *Digitalization as a Mechanism for the Modernization of Public Services: Reality and Prospects*, Arab Democratic Center, Ahmed Draia University of Adrar, Algeria, 2025, p. 15.

⁷ The “data subject” is any natural person whose personal data are the subject of processing. Article 3(4) of Law No. 18-07 on the protection of natural persons in the processing of personal data (op.cit.).

⁸ Article 3(1) of Law No. 18-07 on the protection of natural persons in the processing of personal data (op.cit.).

information concerning individuals' private lives. This right lies at the core of personal freedom and constitutes a fundamental pillar of human rights and public liberties, requiring respect from both authorities and individuals, while at the same time necessitating protection against unlawful violations of this right⁹. The European Court of Human Rights, in its decision of December 16, 1992, held that the concept of private life is not limited to defining an intimate sphere in which a person may live his or her personal life as desired, excluding the outside world entirely; rather, it must also include the individual's right to develop relationships with others. Privacy is reflected in the right to secrecy—meaning the non-disclosure of personal data to third parties—the right to anonymity, the right to solitude, the right to the confidentiality of private written and electronic correspondence, and the right to the protection of one's personal image¹⁰.

A review of various international conventions and comparative legislations shows that most provide a nearly unified definition of personal data. The French Law on Information Technology and Liberties defines personal data as “any information relating to an identified or identifiable natural person, directly or indirectly, by reference to an identification number or to one or more elements specific to their identity.”¹¹ This definition corresponds to Article 2(a) of the European Convention on Human Rights (1950) and Article 1 of the African Union Convention on Cyber Security and Personal Data Protection¹². The Tunisian legislator defines it as “any data, regardless of its source or form, that renders a natural person identified or identifiable, directly or indirectly, excluding information connected with public life or deemed as such by law”¹³.

All the aforementioned definitions converge on the same meaning: personal data encompass all information related to an individual's private life, which no one has the right to access. Even with the existence of artificial intelligence applications, there must be national and international legal mechanisms to combat this phenomenon and set clear limits to it. Personal data are generally divided into two main categories. The first category consists of

⁹ Aicha Ben Kara Mostefa, *Mechanisms for the Protection of Personal Data in Algerian Legislation in Accordance with the Provisions of Law No. 18-07*, *Journal of Legal and Political Sciences*, University of El Oued, Algeria, Vol. 10, No. 1, April 2019, p. 747.

¹⁰ Wassim Chafik Al-Hajjar, op.cit., p. 38.

¹¹ Law No. 78-17 of January 6, 1978, on Information Technology, Files, and Liberties, *Journal Officiel de la République Française* of January 7, 1978, known as the “Data Protection and Liberties Law,” as amended in 2004.

¹² Article 1 of the African Convention stipulates that: “Personal data: any information relating to an identified or identifiable natural person, directly or indirectly, by reference to an identification number or to one or more elements specific to their identity.”

¹³ Tunisian Organic Law No. 63 of July 27, 2004, on the protection of personal data, Article 4, p. 2.

direct personal data, such as name, surname, postal address, and email address. The second category includes indirect personal data, such as phone number, social security number, national identity card number, and confidential passwords.

It is also worth noting that individuals' personal data form an integral part of the data used to feed artificial intelligence applications of various types and fields. The personal data used in processing serve as the "fuel" for these technologies and applications. For example, the collection and processing of such data to predict the occurrence of a crime have enabled many social media platforms to use artificial intelligence to determine new demographic characteristics. AI technologies rely on algorithms that help gather information about the activity of all known users within a specific social network, in order to assess or identify certain behaviors¹⁴.

Data collection precedes the processing of data, which can be defined as:

"Any operation or set of operations carried out, whether by automated or non-automated means, on personal data, such as collection, recording, organization, storage, adaptation, alteration, extraction, consultation, use, disclosure by transmission or dissemination or any other form of making available, alignment, interconnection, blocking, encryption, erasure, or destruction. In other words, it encompasses any operation performed by a natural person or entity to modify, alter, or exploit such data for a specific purpose—or without one—using either manual or automated means"¹⁵.

Section II: Definition of Digital Privacy

The concept of privacy, as previously explained, has become closely linked to artificial intelligence applications and, more broadly, to the Internet with all its technologies and tools. The violation of this privacy or of personal

¹⁴ Heba Ramadan Ragab, *Legal Protection of Personal Data in the Digital Age*, pp. 425-426, accessed on July 20, 2025, at 15:14, https://jelc.journals.ekb.eg/article_342109_230222c1382ad502f693fe0c5abe6a9f.pdf

¹⁵ Article 3 of Law No. 18-07 about the protection of natural persons in the processing of personal data (op.cit.) also sets out several concepts related to data processing, including: Sensitive data: Personal data that reveal a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or that relate to their health, including genetic data. All such data indicate a person's gender, race, political or union affiliation, or other connections that may be exploited to harm the data subject, their family, or public order as a whole. Data controller: The Algerian legislator did not limit the definition of the data controller to a natural person but extended it to include legal persons such as companies, associations, public or private bodies, embassies, and others. It is defined as "any natural or legal person, whether public or private, or any other entity that, alone or jointly with others, determines the purposes and means of processing personal data."

data constitutes a serious threat feared by every Internet user. Therefore, in this subsection, we will explore the digital risks that endanger our personal data.

Subsection 1: Definition of Digital Privacy

Legal scholars define digital privacy as “the right of individuals to control their information database in the manner they choose, without interference or violation. This information database includes all of a person’s digital content on the Internet, whether related to email, social media accounts, bank and digital accounts, or personal photographs”¹⁶.

Subsection 2: Elements of Digital Privacy

Digital privacy encompasses several interconnected concepts, which can be summarized as follows:¹⁷

- Bodily Privacy: This refers to the individual’s right to be free from unwanted external interference that affects the privacy and integrity of their body, such as being subjected to compulsory medical procedures or vaccinations.
- Behavioral Privacy: This includes an individual’s ability to act freely as they wish, without surveillance or unwarranted interference, covering aspects such as religious practices, political activities, and other forms of personal behavior.
- Communication Privacy: This concerns an individual’s freedom to communicate through various technological means without having their communications monitored or intercepted by others.
- Data Privacy: Also referred to as *information privacy*, it encompasses the individual’s right to control the flow of their personal data and information—whether it is entirely private and unknown to others or shared confidentially with a specific group. According to the European General Data Protection Regulation (GDPR), personal data include “any information relating to an identified or identifiable natural person,” who can be recognized directly or indirectly, such as through an address, photographs, religious beliefs, or other data linked to a person’s identity.

Chapter II: The legal protection of personal data from artificial intelligence applications

One of the most fundamental rights granted to individuals is the right to the confidentiality of their personal data and private information, also known as the right to privacy. Both national and international legislations have recognized this right in order to provide effective solutions for protecting personal data from

¹⁶ Mezouz Dalila, “Protection of Personal Data in the Virtual Environment in Algerian Legislation (Reality and Challenges)”, *Al-Ijtihad Journal for Legal and Economic Studies*, Vol. 10, No. 1, 2021, p. 128.

¹⁷ Ibid., p. 129.

breaches or hacking attempts, especially in light of the widespread use of artificial intelligence (AI) applications.

Accordingly, this chapter will shed light on this issue through two main sections:

- The first section addresses the legal basis for protecting personal data;
- The second section examines the challenges of establishing a legal framework for personal data protection.

Section I: The Legal Basis for Protecting Personal Data in the Context of Artificial Intelligence

In order to discuss the protection of personal data in the context of AI, it is necessary to refer to the legal provisions established by various legislations—international, Arab, and national—and to identify the similarities and differences among them.

Subsection 1: Protection under International and Arab Legislations

The right to privacy is one of the most essential rights inherent to human personality and is protected at the international level. According to Article 12 of the Universal Declaration of Human Rights (1948):

“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

Similarly, Article 8 of the European Convention on Human Rights (1950) adopted nearly identical wording without significant modification.

International efforts specifically dedicated to data protection were reflected in the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, issued by the Organisation for Economic Co-operation and Development (OECD) in 1980¹⁸.

The Organization for Economic Cooperation and Development (OECD) influenced the adoption of Convention No. 108, issued in Europe in 1981, which pursued the same objectives as the OECD. This convention focuses on protecting natural persons from the risks arising from the automated processing of personal data. It is the first binding international convention in this field, unlike the OECD’s non-binding guidelines¹⁹.

¹⁸ Sadouk El-Mahdi and Mansri Mariem, “Legislative Efforts to Protect Personal Data in the Digital Environment”, *Marafteh Journal for Legal and Political Studies*, Vol. 1, No. 1, 2021, p. 13.

¹⁹ The International Covenant on Civil and Political Rights (New York, December 16, 1966), to which Algeria acceded under Presidential Decree No. 67/89 dated May 16, 1989, published in the *Official Journal* on May 17, 1989, No. 20.

All these efforts aim to strengthen the application of principles ensuring the protection of personal data and individuals' private lives within the framework of digital information systems, medical data, statistics, marketing, social security, employment, communications, the banking sector, as well as criminal information and data in particular²⁰.

The Economic and Social Commission for Western Asia (ESCWA), established by Resolution No. 1818 of the Economic and Social Council in 1973, has also shown interest in cyber legislation since 2007. This resulted in the publication of a study entitled "Model Legislations"²¹.

The Arab Convention on Combating Information Technology Offences was concluded in Egypt on December 25, 2010. This convention followed the path of international and regional organizations concerned with protecting individuals' privacy rights. It aims to strengthen cooperation among Arab states in exchanging information, technologies, and expertise necessary to combat such crimes that threaten their security and the safety of their societies and citizens²².

For over thirty years, the European Union took pride in having issued the only convention of its kind in this field. However, the African Union adopted the Convention on Cybersecurity and Personal Data Protection during the 23rd African Union Summit held in *Malabo* on June 27, 2014. This convention represents one of the most recent and significant efforts in this area, reflecting the African Union's progress in establishing a solid legal framework to protect fundamental human rights²³.

It is also worth noting the important role played by the International Criminal Police Organization (INTERPOL) in combating cybercrime, which is a transnational offense spreading criminal activity across multiple countries. INTERPOL has focused its efforts particularly on combating the sexual exploitation of children via the Internet. The organization serves as a security liaison between police authorities worldwide by issuing green notices and establishing specialized task forces composed of experts and investigators. It also regularly conducts specialized training sessions for law enforcement personnel²⁴.

²⁰ Sadouk El Mahdi and Mansri Mariem, *op. cit.*, p. 13.

²¹ UN General Assembly Resolution No. 44/132 of December 1989, Human Rights Committee Resolution No. 42/1990 of March 6, 1990, and Economic and Social Council Resolution No. 38/1990 of May 25, 1990, all entitled "*Guidelines for the Regulation of Computerized Personal Data Files*." (Sadouk El Mahdi and Mansri Mariem, *op. cit.*, p. 14.)

²² Abdallah Chaibani and Widad Ben Salem, "The Right to Information Privacy in Light of Artificial Intelligence", *Journal of Legal and Economic Studies*, Vol. 6, No. 3, 2023, p. 465.

²³ Sadouk El Mahdi and Mansri Mariem, *op. cit.*, p. 13.

²⁴ Karima Bouflaka, "The Safety of the Child in the International Digital Environment: What Risks and What Solutions? – An Analytical Study of International Legislative Texts on the

Subsection 2: Legal Protection under National Legislation

Referring to national laws, it becomes clear that the Algerian legislator has made several amendments — both constitutional and legal — regarding personal data, as cybercrime has become increasingly prevalent, making it necessary to introduce updated legislation capable of addressing this evolving threat.

A- Legal Protection of Personal Data under General Laws:

Here, we highlight both constitutional protection and the Criminal Code, as follows:

1- Legal protection under the Algerian Constitution:

The Algerian legislator enshrined the protection of personal data in Article 77 of the 2016 Constitution, which states: “Everyone shall exercise all their freedoms within respect for the rights recognized to others in the Constitution, in particular respect for the right to honor and the inviolability of private life”²⁵.

Previously, the legislator had recognized citizens’ right to privacy and the protection thereof. In the 2016 constitutional amendment, the legislator kept pace with technological progress, particularly in the digital sphere, and explicitly addressed the protection of personal data. This was done through Article 46, which establishes that such rights are inviolable and that any violation thereof shall be punishable by law. The 2020 constitutional amendment reaffirmed these principles under Article 47.

2- Legal protection under the Criminal Code:

The Algerian legislator incorporated cybercrime into the 2004 amendment of the Criminal Code, creating a special section under Chapter Seven bis titled “Offenses against Automated Data Processing Systems” (Articles 394 bis to 394 bis 7).

Although this section does not specifically address personal data, Article 394 bis 2 stipulates that:

Protection of Children from Inappropriate Digital Content”, *Journal of Media Legislation*, Vol. 10, No. 14, p. 55.

²⁵ This was also confirmed by Article 39 of the 1996 Constitution, which stated that: “The inviolability of a citizen’s private life and honor shall not be violated, and the confidentiality of correspondence and private communications in all their forms is guaranteed by law.”

“Anyone who collects or trades in information related to an information system — including personal data — for the purpose of intimidation shall be punished”²⁶.

This applies to both natural and legal persons, meaning that any infringement of their rights entails legal liability and punishment under the Criminal Code, particularly the penalties set forth in Article 18 bis, which include fines, dissolution of the legal entity, and confiscation, in addition to the financial penalties provided for in Article 18 bis 2.

B- Legal Protection of Personal Data under Special Laws:

Several special laws have been introduced to address cybercrime in Algerian legislation. Although Algeria lagged behind other countries that were pioneers in enacting data protection laws — such as the United States (1974) and France (1978) — Arab countries later followed suit: Tunisia (2004), Morocco (2009), and Kuwait (2014)²⁷.

1-Protection of privacy under Law No. 09-04:

The Algerian legislator enacted Law No. 09-04 on special rules for the prevention and fight against offenses related to information and communication technologies. This law requires service providers to preserve data related to users’ privacy²⁸.

Article 11 obliges mobile and Internet service providers to collect and retain all information necessary to identify the source and location of a communication, under penalty of criminal sanctions.

It is evident that this law aims to facilitate the tracking of offenders, particularly in serious crimes such as terrorism. While it allows for technical arrangements to monitor electronic communications, it does not authorize violations of individuals’ personal data. To prevent abuse, the legislator established legal safeguards²⁹ limiting cases where electronic surveillance is permitted, as listed exhaustively in Article 4 of Law No. 09-04, namely:

- To prevent acts classified as terrorism, sabotage, or crimes threatening state security.

²⁶ See Articles 394 bis and the following of Law No. 19-15 of December 30, 2015, amending and supplementing Ordinance No. 66-156 of June 8, 1966, which contains the Penal Code, *Official Journal* of December 30, 2015, No. 71.

²⁷ Sadouk El Mahdi and Mansri Mariem, *op.cit.*, p. 16.

²⁸ Law No. 04-09 of August 5, 2009, on special rules for the prevention and fight against crimes related to information and communication technology, *Official Journal* of August 16, 2009, No. 47.

²⁹ Sadouk El Mahdi and Mansri Mariem, *op. cit.*, p. 16; Mezouz Dalila, *op. cit.*, p. 136.

- When there is information suggesting a potential attack on an information system that may endanger public order, national defense, state institutions, or the national economy.
- For the purposes of judicial investigations and inquiries when it is difficult to achieve results without electronic surveillance.
- Within the framework of implementing mutual legal assistance in criminal matters.

2-Protection of Privacy under Law 15/12:

The Algerian legislator enacted Law 15/12 on the protection of children³⁰, recognizing that children are particularly vulnerable to online risks due to their frequent use of social media platforms and other online applications. Coupled with a lack of awareness about digital risks, this exposure subjects many children worldwide to attempts at harassment, manipulation, exploitation, and even threats to their lives through various means. These include influencing the child's culture and values instilled from an early age, exposing them to violent content and training them in its practice (even virtually), and sexual harassment, whether direct (involving blackmail or coercion) or indirect (exposing children to pornographic images or content).

This situation highlights the urgent need to protect children from undesirable content. In 2020, records were broken, with more than 21.7 million reports of suspected child sexual exploitation submitted to the CyberTipline of the National Center for Missing & Exploited Children (NCMEC). This represents the largest number of reports received in a single year, of which 21.4 million came from electronic service providers³¹.

In Algeria, national estimates indicate around 2,000 cases of sexual assault annually, particularly against children, with 90% occurring in family settings or local residential environments³².

3-Protection of Privacy under Law 18/07:

Law 18/07 includes specific rules for preventing and combating crimes related to information and communication technologies. This law addresses shortcomings present in E-Commerce Law 18/05, which did not explicitly regulate personal data and its protection.

Article 2 of Law 18/07 stipulates that the processing of personal data, regardless of its source or form, must respect human dignity, private life, and public freedoms, without infringing upon the reputation and honor of individuals³³.

³⁰ Law No. 15/12 of July 15, 2015, on the Protection of the Child, *Official Journal* of July 19, 2015, No. 39.

³¹ Karima Boufalaka, *op. cit.*, p. 5.

³² <https://alarab.co.uk/%D8%AA%D8%B5%D8%A7%D8%B9%D8%AF-%D9%85%D9%82%D9%84%D9%82-%D9> accessed on 27-07-2025.

Article 7 explicitly requires the express consent of the data subject for access to and processing of their personal data. In the case of minors, consent must be obtained in accordance with general legal rules, and the data subject may withdraw this consent at any time. See Article 7 of the same Law 18/07, which regulates the requirement of the data subject's explicit consent for the collection and processing of personal data, including provisions for minors and the right to withdraw consent at any time³⁴.

To ensure comprehensive protection of personal data, the National Authority for the Protection of Personal Data was established in accordance with Article 22 of Law 18/07. This article also stipulates that the Authority enjoys independence, meaning it has the freedom to determine its internal regulations without interference from any external entity. The primary responsibilities of the National Authority include ensuring that the processing of personal data complies with the provisions of the law. Among its duties are:

- Granting licenses and receiving declarations related to the processing of personal data.
- Informing data subjects and data controllers of their rights and obligations.
- Providing advice to individuals and entities that process personal data or conduct experiments or activities that may result in such processing.
- Authorizing the transfer of personal data abroad under the conditions stipulated in the law.
- Ordering necessary changes to protect processed personal data.

Section II: Challenges in the Legal Framework for Protecting Personal Data under Artificial Intelligence

Despite the existence of international, Arab, and national legal provisions, all aim at one goal: protecting personal data from AI applications that have permeated both the public and private lives of individuals. However, a critical challenge remains, including in Algeria, regarding whether these legal texts are sufficient to safeguard individuals' privacy. This section highlights this concern as follows:

Subsection 1: Risks Threatening Personal Data under AI Applications

Numerous risks endanger individuals' privacy, especially with the widespread use of social media and AI applications, which penetrate personal life and make individuals vulnerable to violations at any moment. The following subsection identifies the main risks.

³³ See Article 2 of Law 18/07 on *the Protection of Natural Persons in the Processing of Personal Data*, op.cit..

³⁴ See Article 7 of the same Law.

A-Risks Related to the Collection of Personal Data:

The process of collecting data is essential for carrying out processing operations that ideally should be free from risks of violating privacy. However, government agencies or private entities often collect detailed data about their users, which can lead to misuse of stored data, especially since these entities frequently connect devices via public networks to facilitate the exchange of personal data³⁵.

Personal data is often collected without individuals' knowledge through modern technological tools on the Internet, such as cookies, which commercial companies use for advertising their services and products. Despite their many benefits, cookies are one of the most effective tools for tracking individuals and revealing personal data, which can be misused for illegal purposes. An even more dangerous method involves information-gathering systems, such as tracking and capturing software, which enable users to collect a large amount of sensitive information and process it at high speed³⁶.

B-Risks Arising from the Digitalization of Personal Data:

The digitalization of data exposes it to viruses and cyber threats, allowing users to access computer networks and store data and software on the Internet, with flexible access from any time or place. The main risk lies in the transfer and circulation of stored data across the Internet, coupled with the use of intelligent algorithms that can reveal information the user did not intend to disclose. This raises serious concerns about the security of personal data³⁷.

C-Risks Related to Data Flow over the Internet:

This risk involves viruses, which are harmful programs created by specialists familiar with computer systems. These programs are inserted into software to delete or damage existing information on disks for unauthorized purposes, including:

- **Worms (WORM):** Programs that replicate themselves from one computer to another via the Internet, embedding themselves as files on targeted disks to disable or erase them. Their true purpose may be to replicate within the active memory of computers to monitor, delete, or locate vulnerabilities and then spread to other digital devices³⁸.
- **Computer Viruses:** Programs intentionally designed to attach to other software. They activate when the host programs run, reproducing themselves using computer hardware and software without the owner's

³⁵ Heba Ramadan Ragab, *op. cit.*, p. 428.

³⁶ Heba Ramadan Ragab, *op. cit.*, p. 428; Mezouz Dalila, *op. cit.*, p. 129.

³⁷ Ahmed Ben Masoud, "Crimes Affecting Automated Data Processing Systems in Algerian Legislation", *Journal of Law and Humanities*, Vol. 10, No. 01, University of Djelfa, February 2017, p. 284.

³⁸ Mezouz Dalila, *op. cit.*, p. 131.

knowledge. These viruses can spread rapidly, erase memory, and disable systems even after being removed³⁹.

- **Trojan Horses**⁴⁰: Programs that appear useful to the user but hide an illicit purpose or instructions that execute harmful and unexpected tasks when run⁴¹.
- **Spam Emails (SPAM)**: Also known as intrusive emails, these are unsolicited promotional messages sent to a person's inbox, often intended to disrupt normal operations or manipulate data.

E-Risks Arising from Hacking:

Hacking occurs when a computer is illegally accessed, its programs copied without authorization, often through password theft or electromagnetic waves. The primary objectives typically include stealing trade secrets or marketing information to manipulate public institutions or steal funds⁴².

Accordingly, it becomes evident from the above that there is a purpose behind the dissemination of such applications and the insufficient regulation surrounding them, which fails to adequately protect individuals' personal data. These data are exploited by commercial and economic companies, especially when they are on digital platforms, facilitating the operations of companies such as Facebook, Instagram, and Google. These companies analyze users' personal information to interact with them in a highly personalized manner, tailored to each individual's preferences, affiliations, and age. Additionally, search engines are manipulated to identify consumer needs, as most companies and organizations now use artificial intelligence (AI) systems that interact with clients who believe they are communicating with service providers, whereas, in reality, they are dealing with intelligent systems that fulfill their requests instantly.

Subsection 2: Warnings Regarding the Use of AI Applications and Guidelines for Their Use

The global development, particularly the increasing adoption and demand for AI applications across all fields, has prompted many experts and international figures to issue numerous warnings about the potential risks of AI, especially regarding the infringement of individuals' privacy. For instance, Elon

³⁹ Ahmed Ben Masoud, *op. cit.*, p. 282.

⁴⁰ Trojans are generally spread by some form of social engineering. For example, a user may be duped into executing an email attachment disguised to appear innocuous (e.g., a routine form to be filled in), or into clicking on a fake advertisement on the Internet. Although their payload can be anything, many modern forms act as a backdoor, contacting a controller who can then have unauthorized access to the affected device.[3] Ransomware attacks are often carried out using a trojan. [https://en.wikipedia.org/wiki/Trojan_horse_\(computing\)](https://en.wikipedia.org/wiki/Trojan_horse_(computing)). Accessed on 31/07/2025 at 18:41.

⁴¹ Mezouz Dalila, *op. cit.*, p. 132.

⁴² Ibid., p. 132.

Musk, Bill Gates, and Stephen Hawking issued an open letter in 2015 on AI, warning of potential threats to privacy arising from its applications⁴³.

On September 15, 2021, in Geneva, the United Nations High Commissioner for Human Rights, Michelle Bachelet, emphasized the urgent need to halt the sale and use of AI systems that pose serious risks to human rights until appropriate safeguards are in place. She also called for a ban on AI applications that cannot operate in accordance with international human rights law. She stated: "AI may serve as a force for good, helping societies overcome some of the most pressing challenges of our time. However, AI technologies may also have negative, even catastrophic, consequences if deployed without sufficient consideration of their impact on human rights"⁴⁴.

These steady changes naturally raise serious ethical concerns stemming from the potential inherent in artificial intelligence systems to instill bias, exacerbate climate change, threaten human rights, and much more. The risks resulting from artificial intelligence have already begun to escalate with the development of these systems. Existing inequalities further harm already marginalized groups. The Recommendation on the Ethics of Artificial Intelligence.

UNESCO prepared a first-of-its-kind global normative document on the ethics of artificial intelligence, the "Recommendation on the Ethics of Artificial Intelligence," in November 2021, which was adopted by all 193 Member States. The defense of human rights and human dignity is a fundamental pillar of the Recommendation, based on the promotion of the core principles of transparency and equity, while constantly emphasizing the need for human oversight of AI systems. This Recommendation is exceptionally implementable due to its broad policy scope, enabling policymakers to translate core values and principles into action while respecting data governance, the environment and ecological considerations, gender, education and research, health and social welfare, and many other aspects of life⁴⁵.

At the Arab regional level, an international conference was held on July 21, 2022, titled Challenges of Protecting the Right to Privacy in the Era of AI Development, organized under the auspices of the Arab Organization for Human Rights in partnership with the Supreme Permanent Committee for Human Rights. The conference addressed the impact of AI on the right to privacy and the consequences of its violation on the implementation of other

⁴³ Karl Manheim & Layric Kaplan, "Artificial Intelligence: Risks to Privacy and Democracy", *The Yale Journal of Law and Technology*, Vol. 21, No. 106, 2016, p 180.

⁴⁴ <https://www.ohchr.org/ar/press-releases/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet> ,accessed on Thursday, 2025/07/31

⁴⁵ Recommendation on the Ethics of Artificial Intelligence, Adopted on 23 November 2021, year of publication: 2022, <https://unesdoc.unesco.org/ark:/48223/pf0000381137>, accessed on 30L10L2025.

human rights. It also examined the responsibilities of states and private organizations in protecting individuals' data and privacy. The conference aimed to develop legislation and legal frameworks for data protection in the context of smart technologies and to strengthen human rights⁴⁶.

These and other warnings were issued to limit the widespread and dangerous use of AI applications, which today threaten our lives and personal data. The use of AI applications is fundamentally based on principles governing the processing of individuals' personal data. There are three core privacy principles in data collection, derived from the OECD Principles of the Organisation for Economic Co-operation and Development, which are:⁴⁷

- **Principle of Collection Limitation:** Smart technologies rely on the assimilation of vast amounts of data to train and develop algorithms. These data are often collected through smart devices, phones, web tracking, and other methods. In practice, individuals are often unaware of the volume of information collected about them or the methods of its collection. This creates a conflict between the principle of limiting personal data collection and the functionalities of smart technologies.
- **Principle of Purpose Limitation:** It must be ensured that collected information is used solely for the purpose for which it was gathered. In some cases, companies and organizations may use it for secondary purposes, provided this is done reasonably. They are therefore obligated to ensure the information is used properly and lawfully.
- **Purpose Specification:** Given the diverse uses of AI applications, specifying the purpose of data collection is crucial to safeguarding individuals' privacy and preventing misuse of their data. Excessive data collection beyond what is necessary undermines individuals' control over their information.

The Algerian legislator, like others, has sought to protect individuals' data by imposing certain administrative and criminal penalties aimed at mitigating violations of privacy or personal data rights. These include:

- **Administrative Measures:** The Algerian legislator granted the National Authority for the Protection of Personal Data the power to take administrative actions against data controllers in case of legal violations. The range of administrative measures includes warnings, reprimands, temporary withdrawal of prior declarations or authorizations for up to one year, permanent withdrawal, and fines⁴⁸.

⁴⁶ <https://www.youm7.com> , accessed on Thursday 31-07-2025 at 15:11.

⁴⁷ Abdallah Chaibani, Widad Ben Salem, *op. cit.*, pp. 275–276.

⁴⁸ Article 46 of Law 18/07 on the protection of natural persons in the processing of personal data, as previously mentioned.

Decisions of the National Authority in this regard are subject to appeal before the Council of State according to legal procedures. Under Law 18/07, fines may reach 500,000 DZD for each data controller who: refuses, without legitimate reason, the rights to information, access, correction, or objection as provided by Law 18/07; or fails to make legally required notifications. The National Authority may also employ oversight agents to investigate violations of personal data, under the supervision of the public prosecutor, alongside judicial police officers⁴⁹.

- **Criminal Measures:** The National Authority is empowered to conduct investigations, inspect sites where processing occurs (excluding residential premises), and authorize other oversight agents, in addition to police officers, to carry out investigations under the supervision of the public prosecutor. Law 18/07 prescribes penalties for violations ranging from two months to five years of imprisonment, with fines from 20,000 DZD to 1,000,000 DZD, depending on the nature of the violation committed by the data controller, subcontractor, or any other person breaching the law. For legal entities, violations are referred to the Penal Code⁵⁰.

Conclusion

In conclusion, the study of personal data protection in the context of artificial intelligence (AI) applications shows that, while technological development offers many advantages, it also carries numerous negative consequences. These adverse effects are evident daily through social media platforms and even through the use of AI applications, which have become tools that facilitate searches on search engines and provide information at unprecedented speeds. This efficiency is largely due to these applications having access to individuals' data and understanding their needs, enabling them to deliver results almost instantly.

From the above analysis, several key findings can be summarized as follows:

- **Digital Illiteracy:** Individuals are absorbed by social media and by creating accounts on various platforms, as well as by using AI applications that simplify personal and professional tasks, often without considering that their personal data may be compromised, in addition to lacking knowledge about how to protect it.
- **Law 18/07:** Although relatively recent, this law was enacted somewhat late compared to the risks and threats faced by individuals' digital data. While it provides protection for personal data, it still requires amendments to ensure comprehensive protection for natural persons.

⁴⁹ Article 50 of the same Law.

⁵⁰ See articles 54, 69 of the same Law.

- **Technical Infrastructure:** There is a need to establish suitable technical frameworks to guarantee the rights of data subjects by providing effective and advanced protective programs, particularly in digital environments.
- **Awareness Raising:** It is essential to promote public awareness about the risks associated with AI applications, which have become integral to both professional and personal life.
- **Autonomy of the National Authority:** Full independence should be granted to the National Authority for the Protection of Personal Data to allow it to exercise its powers freely, implement appropriate safeguards, and take timely actions without awaiting approval from subordinate entities.

Additionally, several recommendations should be considered in the near future:

- **Updating Law 18/07:** The law concerning the protection of natural persons in the processing of personal data should be updated to explicitly include the protection of data transmitted through various communication channels in digital transactions.
- **Civil Society Engagement:** The state should intensify efforts to involve civil society in achieving and implementing effective protection of individuals' data in the digital environment.
- **Strict AI Regulations:** The state should establish strict regulations governing the use of AI applications.