Protection of personal Data in the Era of Artificial Intelligence

Received: 25/03/2025; Accepted: **17/07/2025**

Djamila HARKATI*

University of Constantine 1, Algeria. harkatidjamila@gmail.com

Abstract

This research paper highlights the challenges faced by legal frameworks in protecting personal data in the context of artificial intelligence. The study examines the most significant risks to data owners, acknowledging that it is nearly impossible to enumerate all potential harms due to the continuous technological advancements in AI systems. Additionally, we explore the key mechanisms established by legislators to mitigate these risks, focusing on both legislative protection and the available technical safeguards for personal data. However, these measures require further adjustments to keep pace with rapid technological developments, particularly given the widespread adoption of artificial intelligence.

Keywords

Personal data;
Artificial Intelligence;
AI ethics ;
Intelligent profiling ;
GDPR .

حماية البيانات الشخصية في ظل الذكاء الاصطناعي

ملخص

سلطنا الضوء من خلال هذه الورقة البحثية على التحديات التي تواجه القانون في مجال حماية البيانات الشخصية في ظل الذكاء الاصطناعي حيث تناولنا بالدراسة أهم الأضرار التي يتعرض لها صاحب المعلومات والتي وجدنا أنه من غير الممكن حصرها جميعا بسبب التطور التكنولوجي المتزايد لأنظمة الذكاء الاصطناعي ،كما تعرضنا بالدراسة إلى أهم الطرق التي كرسها المشرع من أجل مواجهة هذه الأضرار ويتعلق الأمر بالتكريس التشريعي للحماية وكذلك الحماية التقنية المتوفرة لهذه البيانات ومع ذلك فإن هذه الطرق تحتاج إلى تعديل لمواكبة مختلف هذه التطورات خاصة في ظل الانتشار الواسع لاستخدام الذكاء الإصطناعي.

الكلمات المفتاحية

بيانات شخصية؛
ذكاء اصطناعي؛
أخلاقيات الذكاء الاصطناعي؛
تشخيص ذكي؛
النظام الأوروبي لحماية البيانات.

* *Corresponding author.E-mail: harkatidjamila@gmail.com*

Doi:

E-ISSN: 2588-2007 ---Journal homepage: *http://revue.umc.edu.dz/index.php/h*

I- Introduction :

The Artificial intelligence has witnessed rapid development and widespread adoption, becoming an integral part of our daily lives and extensively utilized across various fields. It has garnered significant attention from individuals and institutions alike. Despite the numerous advantages of this powerful technology, its widespread use raises several critical concerns, foremost among them being the protection of rights and freedoms in the age of artificial intelligence. Many fundamental rights have begun to be affected, including the right to information, the right to communication, the right to equality, freedom of opinion and expression, privacy, intellectual property, and others within the digital environment.

Among the most affected rights in the era of artificial intelligence is the right to personal data protection (Battiikh, 2024, pp. 21-22). Individuals may suffer harm to their personal data during automated processing or intelligent diagnosis. This diagnosis is conducted through AI algorithms that analyze data to construct individual profiles or assess conditions with a high degree of accuracy. Intelligent diagnostics are employed in various fields, including security, finance, marketing, social media, and other online platforms (Al-Bazouni, 2023, p. 158).

The emergence of AI applications necessitates serious consideration of their unprecedented impacts, given their autonomous decision-making capabilities. These developments call for legal intervention and proactive measures to address unforeseen and unpredictable risks associated with such technologies. Some countries have already initiated serious efforts to regulate artificial intelligence effectively (Ammar Karim Al-Fatlawi, 2022, p. 08).

Advanced nations have collectively pursued the expansion of AI technologies across all sectors, prompting legislators at both national and international levels to contemplate the enactment of appropriate legal frameworks and preventive measures governing AI technologies. This proactive approach aims to mitigate the potential negative consequences of these advancements. Consequently, the world now requires a set of legal and ethical regulations for artificial intelligence that mandate the design of AI systems with mechanisms and controls to ensure continuous monitoring and management of their outcomes throughout their lifecycle. These regulations must guarantee ongoing compliance with privacy and security standards.

There is no doubt that the technological development that relies on artificial intelligence has given the personal lives of individuals a character that did not exist before. Despite the positives that this development offers, on the other hand, the user's privacy may be exposed to some potential risks. The right to protect personal data processed automatically has received great importance due to the infringement of the privacy of individuals' private lives,

The significance of this topic lies in highlighting the risks to personal data arising from intelligent diagnostics and the use of artificial intelligence systems. It also seeks to identify the legal challenges in protecting personal data and explore effective measures to mitigate these risks and safeguard this fundamental right.

The objectives of the study are to define artificial intelligence and clarify the principles on which it is based, as well as define private data and state its types, highlight the risks of artificial intelligence on private data, in addition to examining the necessity of devoting legal accountability to artificial intelligence systems.

This study raises the following key question:

To what extent has the Algerian legislator addressed the harms resulting from the processing of personal data in the context of artificial intelligence?

To answer this question, this research paper is divided into two main subtitles:

- First Subtitle: Challenges to the Protection of Personal Data in the Age of Artificial Intelligence
- Second Subtitle: Methods for Protecting Personal Data in the Context of Artificial Intelligence

I.1. First Subtitle: Challenges to the Protection of Personal Data in the Age of Artificial Intelligence

Despite the numerous advantages that artificial intelligence applications offer in serving humanity, they also present significant risks, particularly concerning the violation of individual privacy. Privacy is a fundamental human right, recognized by international conventions and enshrined in national legal frameworks. In the digital environment, the right to privacy holds particular significance, encompassing both readily available information and data that can be obtained about an individual, their life, and personal affairs.

The protection of such personal information and data in the context of artificial intelligence faces numerous challenges. Before addressing these challenges, it is essential to first define the concept of artificial intelligence.

1.1 Artificial Intelligence Between Inconsistent Legal Recognition and Widespread Adoption

The concept of artificial intelligence has been widely used in the media in a rather superficial manner, often to describe any form of analytical computing (Najm, 2024, p. 22). As a result, there is no universally agreed-upon definition, and scholarly efforts to define AI have varied considerably. This ambiguity stems from longstanding differences in defining intelligence itself, as well as disagreements over what constitutes artificial intelligence. Consequently, despite numerous attempts to establish a clear definition, AI remains a concept that is, to this day, somewhat elusive (Al-Bazouni, 2023, p. 22).

Some argue that it is difficult to establish a comprehensive definition of artificial intelligence due to its evolving nature as a newly developed system. The complexity of AI, its diverse applications, methods of data processing (Battiikh, 2024, p. 39), and various approaches make it challenging to fully encompass all its dimensions. However, given the widespread adoption of artificial intelligence and the potential risks associated with its use, it has become imperative to establish legal frameworks that define AI clearly. Additionally, there is a growing need for a well-structured ethical and legal framework to regulate its functioning, ensuring that AI does not become a source of harm or a threat to human rights and freedoms.

In this context, many countries and regional unions have taken an interest in enacting specialized legislation on artificial intelligence, recognizing that advancements in AI technologies must be accompanied by parallel legal and ethical developments. The European Union, for instance, issued several recommendations in 2017 regarding civil law rules applicable to AI technologies. In 2019, it also published a set of guidelines outlining the principles that governments and companies should adhere to when developing AI applications. Additionally, in 2018, the European Parliament proposed that EU member states establish legislation addressing the legal aspects of AI development and use. The EU has also introduced supplementary regulations to the General Data Protection Regulation (GDPR) to further safeguard personal data in the context of AI applications (Mansour, 2024, p. 29).

Despite these efforts, some countries have yet to introduce specific AI legislation, leading to ongoing legal debates among experts in the field. These discussions raise fundamental questions regarding the definition of AI, its various forms, ethical considerations, and the legal implications associated with its use. Given the complexity of AI technology, continuous expert support is essential, and legal scholars must acquire a fundamental understanding of the technical aspects they aim to regulate. Therefore, achieving an effective balance between technological progress and legal frameworks remains a critical necessity.

Many scholars have attempted to define artificial intelligence, despite the challenges posed by its novelty and the lack of a universally accepted definition. AI is a broad term encompassing a range of advanced technologies that have emerged over recent decades, making it difficult to formulate a single, comprehensive, and universally applicable definition. The perception of AI varies among researchers depending on their field of expertise (Al-Bazouni, 2023, p. 26).

John McCarthy, a computer scientist credited with coining the term "artificial intelligence" in 1956, defined it as "the science and engineering of making intelligent machines or a branch of computer science that aims to create intelligent systems" (Mansour, 2024, p. 36).

Blay Whitby described AI as "the study of behavior in humans, animals, and machines, as well as an attempt to find ways to incorporate such behavior into industrial machines" (Whitby, 2008, p. 15).

Waterman defined AI as "a branch of computer science concerned with developing intelligent computer programs."

Russell characterized AI as "a system whose expected utility is the highest achievable by any system operating under the same computational constraints."

Meanwhile, Scheldt defined artificial intelligence as "a system that exhibits behavior similar to human behavior when faced with a comparable problem" (Ammar Karim Al-Fatlawi, 2022, p. 22).

Others define artificial intelligence as "a branch of computer science focused on creating machines that can function and interact in a manner similar to human intelligence. AI is closely linked to research on the human mind" (Ammar Karim Al-Fatlawi, 2022, p. 20).

At its most basic level ,AI is a system that can learn how to learn .Humans write initial algorithms for a system that enables the computer to subsequently write its own algorithms ,without additional human oversight or interaction .This process allows continuously learn from ,and solve new problems within ,an ever-changing environment ,based on its continuing collection of data . (Humerick, 2018, p. 393)

Some scholars approach the definition by breaking down the term into its two components: "artificial" and "intelligence." The concept of intelligence has been subject to varying definitions by psychologists, philosophers, and sociologists. Some define intelligence as the ability to comprehend, reason, and think critically (Al-Bazouni, 2023, p. 20), while others view it as a mental adaptation to new circumstances or as a state of equilibrium sought by all motor and sensory adaptations, as well as all adaptive interactions between an organism and its environment (Ammar Karim Al-Fatlawi, 2022, p. 20).

The second term, "artificial," refers to something that is man-made or not naturally occurring.

From the above discussion, it becomes evident that artificial intelligence encompasses multiple definitions, all of which converge on the idea that AI is a broad term referring to applications capable of performing complex tasks that traditionally required human intervention. AI involves the development of methods that enable computers to acquire intellectual abilities comparable to those of humans, such as learning and responding to stimuli, while also incorporating autonomy and awareness.

While AI applications have created significant opportunities for advancing humanity, they have also introduced potential risks, both tangible and intangible, particularly concerning human rights. Although concerns over technological risks existed prior to the digital revolution, artificial intelligence has introduced new challenges across political, economic, and cultural domains. These challenges are further intensified by AI’s cross-border nature and the concentration of its capabilities in the hands of a few dominant entities. Consequently, there is a pressing need for legislative intervention at both national and international levels to safeguard human rights and prohibit AI applications that conflict with established human rights protection laws (Najm, 2024, p. 64).

1.2 The Impact of Artificial Intelligence on Digital Personal Data

The rapid advancement of artificial intelligence across various sectors has led to the emergence of numerous challenges, necessitating effective solutions and enhancing data protection mechanisms. Before discussing the impact of AI on information privacy, it is essential to define this concept and examine the legal safeguards established for its protection.

1.2.1 Digital Personal Data – Concept and Categories

The widespread integration of artificial intelligence into nearly all aspects of daily life has resulted in individuals generating vast amounts of data on a continuous basis. Given that traditional data management methods are insufficient to handle the exponential growth of big data, researchers in the field have developed data-mining techniques utilizing AI technologies. Personal data constitutes a substantial portion of the big data produced by individuals on a daily basis (Al-Bazouni, 2023, p. 150).

Before examining the legal protections afforded to personal data, it is necessary to first define the concept of personal data as outlined in Algerian legislation and in comparative legal frameworks.

A. Definition of Personal Data

The concept of personal data privacy first emerged in academic discourse in the late 1960s through the works of two American authors. The first, Alan Westin, introduced the idea in his book *Privacy and Freedom*, where he defined information privacy as the right of individuals to determine when and how their personal information is accessed by others. The second, Arthur Miller, discussed the concept in his book *The Assault on Privacy*, in which he stated that information privacy entails the right of individuals to decide when, how, and to what extent others may access their personal information (Battiikh, 2024, p. 60).

Many legal frameworks have sought to define personal data, with the Algerian legislator being among them. According to Article 3 of Law No. 18-07, personal data is defined as:

"Any information that may be directly or indirectly linked to a specific person, especially when it involves an identifying number or one or more characteristics unique to that person's physical, physiological, genetic, biometric, psychological, economic, cultural, or social identity (Article 03 of Law No. 18/07, 2018)*."*

Similarly, the French legislator defines personal data in Article 2 of Law No. 801 of 2004, which amended and supplemented Law No. 07 of 1978 on the protection of personal data, stating:

"Any information pertaining to a natural person or someone who can be directly or indirectly recognized by using their personal number or any other information unique to them is referred to as personal data. (Law No. 2004-801, 2004)*."*

The General Data Protection Regulation (GDPR) of 2016, which replaced the 1995 European Data Protection Directive, also provides a definition of personal data. According to Article 4 of the GDPR, personal data is defined as:

"Any information pertaining to a natural person who can be identified or identified, especially through the use of a personal identifier like their name, social security number, location information, online identifier, or one or more characteristics unique to their physical, physiological, genetic, mental, economic, cultural, or social identity (Paragraph 1 of Article 04, 2016)*."*

The Egyptian legislator has also defined personal data in Article 1 of Law No. 151 of 2020 on data protection. According to this law, personal data is:

"Any information pertaining to a real person who may be directly or indirectly recognized by connecting it to other information, such a picture, voice, identification number, online identifier, or information that establishes a person's social, cultural, psychological, or economic identity."

B. Categories of Personal Data

Based on the previously mentioned definitions, personal data can be classified into different categories:

- Identity-related data, which includes an individual's name, surname, voice, image, personal identification numbers, address, financial records, and biometric data.
- Data related to physical integrity and personal well-being, covering aspects that impact an individual's bodily safety and moral existence.
- Data concerning moral and ideological identity, which includes political, literary, union-related, philosophical, and even genetic information.
- Data held a hospital or doctor ,which could be a symbol that uniquely identifies a person

The Algerian legislator refers to this last category as "sensitive data."[(1)]

1.3 Risks of Intelligent Profiling and Automated Processing on Personal Data

Personal data sharing has become an important issue in public and private sectors of our society .However, data subjects are perceived to be always unwilling to share their data on security and privacy reasons .they apprehend that those data will be misused at the cost of their privacy jeopardizing their human rights. (Sheshadri Chatterjee, 2019, p. 21)

One of the most significant risks threatening personal information and data is its accessibility on the internet through information banks and sector-specific databases, which vary in their level of security and regulation. Personal data is particularly vulnerable to breaches, either through direct access to physical devices storing such information or indirect access via unauthorized intrusions. As a result, intelligent profiling has become a major threat to the privacy of personal information and data.

Before identifying these risks, it is essential to define the concept of intelligent profiling. In this regard, the General Data Protection Regulation (GDPR) defines profiling in Paragraph 4 of Article 4 as:

"Any type of automated personal data processing that uses personal data to assess certain aspects of a natural person, specifically to analyze or forecast traits related to that person's behavior, location, or movements, economic status, health, personal preferences, dependability, or performance at work."

This definition highlights that profiling consists of two key elements:

- Automated data processing
- Evaluation of an individual's personal aspects

These two components illustrate the core risks associated with intelligent profiling, as they enable large-scale data analysis and predictions that may significantly impact individual privacy.

The Algerian legislator has not provided a specific definition for intelligent profiling. However, Article 3 of Law No. 18-07 defines automated processing as:

"Operations carried out entirely or partially through automated means, such as data recording, the application of logical or mathematical processes to such data, its modification, deletion, extraction, or dissemination…"

This definition closely aligns with the one provided in Paragraph 3 of Article 4 of the General Data Protection Regulation (GDPR).

This implies that intelligent profiling is not merely a traditional method of processing personal data, nor is it limited to collecting and storing information. Rather, it involves creating a digital profile of an individual's characteristics through automated system analysis of available data. The objective of such profiling may be to serve either private or public interests)Al-Bazouni(152 صفحة ،2023 ،.

This raises serious concerns regarding violations of the right to personal privacy. The infringement on personal data can be defined as any unethical behavior related to the automated processing and transmission of personal data without the individual's authorization. It can also be understood as any unlawful act in which an electronic processing system is used as a tool for unauthorized data access or manipulation.

The most significant of these violations—whether intentional or unintentional—include the following:

1.3.1 Destruction or Disclosure of Personal Information and Data

The destruction of personal information or data is one of the most prevalent forms of privacy violations. Such breaches can occur either directly, through unauthorized access to the physical device storing the personal data, or indirectly, by remotely infiltrating the system using electronic means and malicious software (Al-Saadi, 2012, p. 78).

Similarly, the unauthorized disclosure of personal information and data represents one of the most serious threats to informational privacy. Under no circumstances should information obtained through profiling or automated processing be disclosed without authorization (Battiikh, 2024, p. 83). This principle is explicitly emphasized by the Algerian legislator, who stresses the necessity of maintaining the confidentiality and integrity of processed information (Chapter One of Title Five of Law No. 18/07, 2018).

1.3.2 Restriction or Transfer of Personal Information and Data

Restriction of information refers to preventing the data owner from accessing their personal information. In this case, the violation does not affect the content of the information itself but rather targets the system responsible for processing and granting access to the data. The Algerian legislator refers to this as "information blocking," defining it as making access to data impossible (Final Paragraph of Article 03 of Law No. 18-07, 2018).

On the other hand, data transfer involves relocating information from one place to another without retaining the original copy (Battiikh, 2024, p. 84).

1.3.3 Disruption of the Information System

This is considered the most severe form of personal data breaches, as it completely or partially prevents individuals from accessing their information. Such disruptions effectively block users from retrieving their data, regardless of its type.

Disrupting an information system can be achieved through manipulating or corrupting system data, damaging the server software, or compromising the program that enables access to the system. These actions render the system inoperative, preventing authorized users from accessing their data (Hamdan, 2021, p. 17).

I. 2. Second Subtitle: Methods for Protecting Personal Data in the Era of Artificial Intelligence

Various constitutions and legal frameworks have established safeguards to protect individuals' personal data from breaches, particularly in the digital environment, to ensure information privacy. This need for protection has become even more critical with the widespread use of artificial intelligence.

Personal data protection is ensured through two primary approaches:

- Legal Protection of Personal Data in the Context of Artificial Intelligence
- Technical Protection of Personal Data in the Context of Artificial Intelligence

2.1 Legal Protection of Personal Data in the Context of Artificial Intelligence

The unique characteristics of artificial intelligence, particularly its autonomy and ability to learn, have led many legal scholars to propose the establishment of special liability rules and the development of a comprehensive framework for holding AI systems accountable for any harm they may cause to individual rights and freedoms.

Furthermore, Article 42 of UNESCO's AI Ethics Guidelines states that AI systems must bear ethical and legal responsibility in accordance with national and international law (Article 42 of Ethics of Artificial Intelligence).

Before addressing legal liability, it is essential to first examine the protection of digital personal data as a foundational element of legal safeguards.

2.2 Legal Safeguarding of Digitally Processed Personal Data

The risks and violations that personal data may face in the context of artificial intelligence are numerous. As a result, all legal frameworks aim to establish robust protections for the privacy of personal data when it is processed or analyzed using automated and intelligent methods.

Privacy protection in this context refers to an individual's control over their personal data and information, enabling them to manage all such data, its digital processing, storage, and use in a manner that aligns with their personal goals while also respecting public morals and order (Battiikh, 2024, p. 62).

At the international level, Article 32 of UNESCO's AI Ethics Guidelines asserts that "the enjoyment of privacy is an essential right for preserving human dignity, defending independence, and protecting personal actions. Therefore, privacy should be respected, safeguarded, and promoted throughout the lifecycle of artificial intelligence systems."

Article 33 of the same guidelines further emphasizes the need for a "multilateral approach at the national or international level to establish suitable frameworks for data protection and implement appropriate mechanisms. These frameworks and mechanisms should be protected by judicial systems."

Article 34 outlines that "algorithmic systems require sufficient evaluation of their privacy impacts, taking into account both societal and ethical considerations. An innovative approach should be adopted to ensure privacy is respected throughout the design process of such systems" (Najm, 2024, p. 80).

The Algerian legislator has also enshrined these protections through its Constitution and laws.

2.2.1 Enshrinement of Protection in the Constitution

The Algerian Constitution explicitly safeguards the privacy of personal data, recognizing it as a fundamental right. Article 47, Paragraph 4 of the 2020 Constitutional Amendment states:

"The protection of individuals during the processing of personal data is a fundamental right."

2.2.2 Enshrinement of Protection in the Laws

The Algerian legislator has also taken significant steps to protect digitally processed personal data through various laws, notably Law 18/07 concerning the protection of natural persons in the context of personal data processing. This law outlines a series of measures and procedures to protect individuals during the processing of their personal data, along with a set of penalties for those who violate these provisions.

Additionally, Law 04/15, amending and supplementing the Penal Code, includes provisions criminalizing offenses related to the manipulation of automated data processing systems. These offenses include crimes such as unauthorized access to or remaining within information systems, attacks on the operation of automated data processing systems, and destruction of information (Law No. 04/15, 2004).

2.3 The Extent of Enshrining Legal Responsibility for Artificial Intelligence Systems

Legal responsibility refers to an individual's obligation to bear legal consequences, either civilly, if they fail to fulfill their duties or violate an obligation causing harm to another, or criminally, if they commit a crime punishable by law. The involvement of artificial intelligence in various aspects of life has created fertile ground for establishing responsibility for the emerging entities it creates. Thus, AI systems must be subject to liability rules, whether civil or criminal.

The legal need is what makes the legislator seek to enact new laws that keep pace with the development taking place in society, and this legal need appears with the emergence of artificial intelligence technologies in many fields and their association with some crimes. For example, in the field of transportation, self-driving cars have appeared, as they operate using artificial intelligence technology because they deal with the car's data and collect data from the surrounding environment and process the data and issue orders after analyzing this data. There are also other crimes and errors committed using artificial intelligence technology in the field of e-commerce, in the field of health and in the military field, in addition to crimes committed on personal data, as they differ from traditional programs that operate within the framework of pre-determined instructions or in a predictable linear manner, while smart programs operate in an unexpected independent manner according to what the surrounding environment dictates and make their decisions without referring to their users.

The issue of establishing legal responsibility for artificial intelligence has sparked significant doctrinal debate, particularly concerning the identification of the person responsible for the damages caused by AI systems. In response, scholars have sought to develop a modern framework for legal accountability, starting with the recognition of legal personality for these systems.

While some legal scholars oppose granting legal personality to AI systems, another faction of French legal scholars argues that autonomous robots could be regarded as electronic persons with specific rights and obligations, including the responsibility to repair any damage caused to others. According to this view, AI systems could be recognized as electronic persons capable of making independent decisions. Advocates of this perspective compare recognizing AI systems as legal persons to the recognition of legal personality for corporations. While legal personality for corporations is a mere legal fiction, the same could apply to intelligent robots, which could be acknowledged as having rights and obligations under this approach (Najm, 2024, p. 87).

From a legal perspective, although laws do not yet recognize artificial intelligence as a legal person, the European Parliament has granted AI a legal status that brings it closer to the concept of legal personality. In this regard, the European Parliament issued a set of recommendations in 2017 concerning civil law rules related to robots, in which it recognized the electronic legal personality of AI systems. The recommendations included the creation of a special registry for intelligent robots where all relevant information about them would be recorded. Additionally, they proposed the establishment of a civil liability system for damages caused to third parties by AI systems, along with an insurance system to cover potential risks associated with AI activities (European Parliament, 2017).

To establish civil and criminal liability for artificial intelligence systems, some scholars have proposed the adoption of a comprehensive liability system that combines several frameworks, allowing for a shared approach to determining responsibility. This can be achieved through individual liability, where responsibility for the damage caused by AI is attributed to a specific person based on their authority or control over the system. This follows a standard similar to the custody principle in general law, where liability is assigned to the party with the effective authority over the AI system. For example, the party responsible for programming the system or modifying its operational data may be held liable, as well as the individual with the authority to initiate the system's operation. This extends to both the developer and the user of the system.

Additionally, collective liability for AI developers has been proposed, based on an idea introduced by American scholar David Vladeck. This system aims to hold a group of parties who have contributed to the creation of the AI entity jointly and severally liable for its actions, promoting shared accountability among all involved in the development and deployment of AI systems (Al-Bazouni, 2023, p. 289).

As for criminal liability, what is currently prevalent in jurisprudence is that the representative of the legal person or the person who committed these crimes from among the employees of the legal person are criminally liable for their crimes even if they committed them for the benefit of the legal person for whom they work. However, in the event that the criminal behavior is committed by the artificial intelligence itself without a programming error of manufacture or intervention from another party, and through modern technologies that enable the artificial intelligence to think and issue independent decisions, it alone is responsible. There is no doubt that the natural person who committed these crimes in the name of a legal person or for its account and benefit is responsible according to the general rules stipulated in the Penal Code.

3. Technical Protection of Personal Data in the Context of Artificial Intelligence

These protective measures can be summarized as encryption and processing data in a lawful and transparent manner.

3.1 Encryption System

Encryption refers to the process of concealing confidential information in a way that ensures it remains incomprehensible to unauthorized individuals. By using encryption, data is securely stored on computers or transmitted over insecure channels, such as the internet. While encryption does not entirely prevent unauthorized access, it ensures that the content remains unreadable to those without the proper decryption keys. Therefore, encryption is one of the simplest and most essential methods to prevent the theft or unauthorized reading of computer system information (Najm, 2024, p. 80).

3.2 Processing Personal Data in a Lawful and Transparent Manner

The European Data Protection Regulation has established a set of guidelines for the processing of personal data. These include ensuring that the processing is limited to ordinary data rather than sensitive data. It also requires obtaining the explicit consent of the individual whose data is being processed, and adherence to the original purpose for which the processing was conducted.

Moreover, the data collection, analysis, profiling, and implementation stages must be performed with accuracy. The retention of data should only occur for the time necessary to achieve the specified purposes of the processing. Any retention beyond this period is permissible only for archiving purposes, in the public interest, or for scientific research (Al-Bazouni, 2023, p. 160).

A set of rules pertaining to the automated processing of personal data has been created by the Algerian parliament. These include, firstly, the requirement for explicit consent from the individual concerned as a general rule. However, there are exceptions to this requirement when the processing is necessary, such as in cases involving the protection of the individual's life or vital interests, the fulfillment of a legal obligation, when the individual is a party to a contract, or for the achievement of public interest.

In the absence of these exceptions, obtaining the individual's consent is a necessary step before processing data (Article 7 of Law No. 18-07, 2018). Furthermore, the party responsible for processing the data must provide a prior declaration confirming their commitment to process the data in accordance with legal rules (Article 13 of Law No. 18-07, 2018).

In order to safeguard people' privacy, the lawmaker mandates that prior permission be obtained from the National Authority for the Protection of Personal Data in cases where the processing may compromise the protection of personal privacy or the individual's basic rights and freedoms (Article 17 of Law No. 18-07, 2018)

IV-Conclusion:

The protection of personal data is one of the most important rights and freedoms recognized by national legislations due to its practical and personal significance, especially in the era of digitization and artificial intelligence. Most laws aim to address the violations that personal data may face, which negatively affect the data owner, violate their privacy, or lead to material losses.

In this research paper, we examined the main risks to personal data in the context of artificial intelligence and attempted to highlight the protection granted by legislations, particularly the Algerian legislator, in safeguarding personal data under intelligent profiling. In this research paper, we have studied the most important damages that personal data can be exposed to in light of artificial intelligence. We also tried to shed light on the protection approved by legislation, especially the Algerian legislator, to protect personal data in light of smart diagnosis. Before that, we studied the concept of artificial intelligence, where we explained that it went through historical stages that led to its development and reaching the peak of development, which led to the necessity of legal intervention. We also discussed the concept of personal data and its various types.

We have concluded with the following results:

- The widespread use of artificial intelligence technologies in various areas of life has led to many positives, but it has also caused many harms, especially to rights and freedoms
- Personal data that is automatically identified is vulnerable to tampering.
- The Algerian legislator has enshrined the protection of automated personal data processing.
- There is difficulty in identifying all the violations that personal data may face due to their diversity, driven by technological advancements and the emergence of newly developed artificial intelligence systems.
- The challenge of establishing legal responsibility for artificial intelligence systems regarding the harm caused to the owner of this personal data.

Therefore, we propose the following:

- Amend Law 18/07, which concerns the protection of natural persons during personal data processing, to include intelligent profiling of information and to enshrine legal responsibility rules for artificial intelligence systems.
- Implement a highly professional and secure encryption system that is difficult to breach.
- Establish a national ethical charter that outlines the rules, principles, and ethics of using artificial intelligence.

Referrals and References:

[1]. Article 03 of Law No. 18/07The Protection of Natural Persons During the Processing of Personal Data*Official Gazette 34* Algerian Government

[2]. Article 13 of Law No. 18-07The Protection of Natural Persons During the Processing of Personal Data*Official Gazette* AlgeriaAlgerian government

[3]. Article 17 of Law No. 18-07The Protection of Natural Persons During the Processing of Personal Data*Official Gazette* AlgeriaAlgerian government

[4]. Article 42 of Ethics of Artificial IntelligenceEthics of Artificial Intelligence

[5]. Article 7 of Law No. 18-07The Protection of Natural Persons During the Processing of Personal Data*Official Gazette* AlgeriaAlgerian government

[6]. Chapter One of Title Five of Law No. 18/07The Protection of Natural Persons During the Processing of Personal Data*Official Gazette* AlgeriaAlgerian government

[7]. *Civil Liability for Complex Artificial Intelligence Technology: A Comparative Study*2022AlexandriaDroub Al-Ma'rifa for Publishing and Distribution

[8]. Criminal Models of Attacks on Personal Data2021*Journal of Legal and Economic Research*

[9]. *Ethics of Artificial Intelligence in Light of the United Nations (UNESCO) Recommendations*2024AlexandriaEgyptDar Al-Fikr Al-Jamei

[10]. European ParliamentRecommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))European UnionEuropean Parliament

[11]. Final Paragraph of Article 03 of Law No. 18-07The Protection of Natural Persons During the Processing of Personal Data*Official Gazette* Algerian government

[12]. Humerick, M. (2018, march 5). Taking AI personally ;How the E.U Must learn to Balance the Interests of Personal Data privacy and Artificial Intelligence. *Santa Clara High Technology Law Journal , 34* (4), pp. 393-418.

[13]. Law No. 04/15The Penal Code*Official Gazette 71* AlgeriaAlgerian government

[14]. Law No. 2004-801the Protection of Natural Persons with Regard to the Processing of Personal Data, Amending Law No. 78-17 of January 6, 1978, on Information Technology.

[15]. *Legal Protection of Information Privacy*2024CairoDar Al-Nahda Al-Arabiya

[16]. Paragraph 1 of Article 042016The General Data Protection Regulation (GDPR)European UnionOfficial Journal of the European Union

[17]. Sheshadri Chatterjee, N. S. (2019, mars 15). personal data sharing and legal issues of human rights in the era of artificial intelligence;Moderating effect of government regulation. *international Journal of Electronic Government Research (IJEGR)* , pp. 21-36.

[18]. *Substantive Criminal Protection from Acts of Artificial Intelligence Technology*2024AlexandriaDar Al-Matbouat Al-Jameia

[19]. *The Crime of Destroying Computer Programs and Information in Kuwaiti and Comparative Legislation*2012Dar Al-Nahda Al-Arabiya

[20]. *The Impact of Artificial Intelligence on the Theory of Rights*2023LebanonArab Institution for Books

[21]. Whitby, B. (2008). *Artificial Intelligence: A Beginner's Guide.* Cairo: Dar Al-Farouk for Cultural Investments.

Note:

[1]. Article 03 of Law 18-07 defines sensitive data as follows:"any operation or set of operations performed on personal data, whether by automated or non-automated means, such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, use, disclosure by transmission or publication, erasure, or any other form of processing."