

Risks of Artificial Intelligence to Personal Data Protection: A Study Based on the Perceptions of Algerian Citizens

Nawal HIRECH*

Oran graduate school of economics, Algeria

hirech.nawel250@gmail.com

Received: 08/04/2026

Accepted: 25/04/2026

Published: 05/06/2026

Abstract:

This study analyzes the factors influencing perceptions of risks associated with artificial intelligence (AI) regarding personal data in Algeria. An empirical survey was conducted among 120 Algerian citizens (purposive sample, young users with higher education). The results show that the perception of AI risks for personal data is significantly linked to the level of knowledge about AI ($p=0.037$) and the variety of uses of AI-based technologies ($p=0.041$). The study reveals a privacy paradox: concern does not systematically trigger individual protection practices ($p=0.125$), but generates a strong demand for legal regulation ($p=0.004$). Furthermore, while knowledge of Law n°18-07 does not influence fear, awareness of the ANPDP (National Authority for the Protection of Personal Data) is the cornerstone of the sense of institutional security ($p<0.001$). These findings underscore the importance of enhancing the visibility of supervisory authorities to ensure a smooth digital transition in Algeria.

Key Words: Artificial intelligence, personal data, digital risks, legal framework, public perception, Algeria.

JEL Classification : O33, L86, K24, D83

* Corresponding author: HIRECH Nawal (*hirech.nawel250@gmail.com*)

Introduction

Artificial intelligence (AI) is no longer limited to a research discipline confined to computer science laboratories; it has now established itself as a foundational technology at the heart of contemporary societal transformations. From a foundational perspective, McCarthy (2007) defines it as an engineering discipline dedicated to the design of intelligent machines capable of replicating certain human cognitive functions. The development of these systems relies on the intensive use of data, which is mobilized as an essential resource for optimizing algorithmic performance. This evolution is part of a trend that Zuboff (2019) describes as “surveillance capitalism,” characterized by the systematic collection and monetization of personal data.

However, this increased capacity for information processing is accompanied by growing concerns about privacy. While human error has historically been a major source of data breaches, the unique characteristics of AI systems introduce additional vulnerabilities, which complicate the mechanisms for protecting individuals and heighten uncertainty regarding the use of their personal

information. In response to these challenges, institutional responses have gradually taken shape. Following trends observed at the international level, the Algerian government adopted Law No. 18-07, supported by the National Authority for the Protection of Personal Data (ANPDP), to regulate the processing of personal data. Nevertheless, beyond the legal framework, the question of public perception of this digital transition remains central.

Amid this technological and legal transformation, our research focuses on the following central question: **How do Algerian citizens perceive the risks associated with the use of artificial intelligence in relation to their personal data, and what factors influence this perception?**

To address this issue, four working hypotheses were formulated

- H1: *The level of knowledge about artificial intelligence significantly influences perceptions of risks related to personal data protection.*
- H2: *The variety of uses for AI-based technologies influences Algerian citizens' perception of risks.*
- H3: *Knowledge of the Algerian legal framework regarding personal data protection reduces the perception of risks associated with AI.*
- H4: *The perception of risks associated with AI positively influences support for strict regulations limiting the use of personal data.*

This study aims to compare the theoretical reality of AI risks and legal frameworks with users' subjective perceptions. Following an in-depth presentation of the conceptual and legal framework in the first section (Literature Review), we will outline our research methodology and present an analysis of the data collected from a sample of 120 Algerian citizens (Empirical Study). The study primarily focused on a young population (71.7% of the sample) with a higher level of education (92.5%, including students and graduates), as this group is considered to be the most exposed to the challenges posed by AI. The statistical analysis of the data, conducted using SPSS (v. 27.0.1), relied on correlations (Pearson and Spearman) and linear regressions to validate our hypotheses and propose avenues for more transparent data governance in Algeria.

I. Literature Review

1. The conceptual evolution of Artificial Intelligence

Artificial intelligence is a complex field that draws on several disciplines beyond computer science, such as philosophy, statistics, mathematics, psychology, neurology, biology, and linguistics (Russel & Novig, 2020).

Since the 1950s, the concept of artificial intelligence has begun to take shape, particularly through the work of mathematician Alan Turing, who wondered whether a machine could one day think. To test this hypothesis, he created the Turing test in 1950, which assesses a machine's intelligence based on its ability to mimic human conversation and, by extension, human behavior. The term "Artificial intelligence," abbreviated as AI, was first introduced in 1956 by John McCarthy¹ (Turing Award, 1971) during the "Dartmouth Summer Research

Project on Artificial Intelligence” conference. Years later, in 2007, he defined it as “the science and engineering of making intelligent machines.” (McCarthy, 2007, p. 1). Unlike Turing, McCarthy does not make machine intelligence contingent on their ability to faithfully reproduce human behavior. His definition allows us to consider as intelligent systems whose modes of reasoning and action differ fundamentally from those of humans, while remaining effective in achieving defined objectives. Drawing on a logical-mathematical tradition (formal logic, decision theory, analytical philosophy), McCarthy argues that AI is programmed using symbols, rules, and formal logic in order to reason correctly to solve abstract problems (independent of the real world²) and draw valid conclusions from formalized knowledge. Thus, McCarthy emphasizes the necessity of human control over systems that use AI.

Russell and Novig (2020) argue that the reason there is no consensus on the definition of AI stems from the fact that each definition reflects a distinct disciplinary tradition and different research objectives. That is why they propose a typology of artificial intelligence structured around four conceptual combinations, distinguishing approaches centered on human imitation from those based on rationality, as summarized in the following table.

Table 1: «Classification of AI definitions according to Russell and Norvig»

Axe	Definition of AI	Scientific objective	Research discipline	Limitations according to Russell and Norvig
Thinking Humanly	a machine's ability to replicate the mechanisms of human thought, such as reasoning, memory, and learning.	to replicate the mental mechanisms underlying human thought	Neuroscience Cognitive Psychology Cognitive Science	Human cognition is often irrational, biased, and inconsistent.
Acting Humanly	Ability to mimic human behavior.	Human-like behavior so realistic that it blurs the line between human interactions and those of a system	Philosophy of Mind linguistics Human Computer Interaction(Computer Science, Cognitive Science, and Design)	A system can be intelligent without resembling a human (e.g., search engines)
Thinking Rationally	To draw logically sound conclusions from given premises.	Ensuring formally valid reasoning	Mathematics Analytic philosophy	Rationality presupposes complete and certain information, which is rarely available. Logical reasoning is not suited to reality.
Acting Rationally	AI is an agent capable of choosing the optimal action to achieve its goals	Maximize performance and decision-making efficiency	Computer Science Operations Research Economics Data Science	Heavy reliance on data, risks of bias, lack of transparency, and privacy violations

Source: Prepared by the author based on the explanations provided by Russell and Norvig in (Russell & Norvig, 2020, pp. 20, 21, 22)

This typology highlights an evolution in approaches to artificial intelligence, shifting from the replication of human behavior to a logic of rational optimization, an approach that is now dominant in contemporary AI systems due to its alignment with economic principles of performance, optimization, and data exploitation. Russell and Norvig clearly favor the “Act Rationally” approach to defining AI, as they state that “*Artificial Intelligence is the study of agents that receive percepts from the environment and perform actions*” (Russell & Norvig, 2020, p. 55). For these authors, an intelligent system is an agent capable of perceiving the environment, acting autonomously, and maximizing its performance to achieve defined goals (Russell & Norvig, 2020, p. 56).

In addition to the ability to think and act rationally, Yann LeCun adds the capacity for learning and representation. Indeed, Yann LeCun, winner of the 2018 Turing Award, believes that human or artificial intelligence is “*the ability to learn models of the world that can be used to predict the consequences of actions*” (LeCun, 2022, p. 3). This definition emphasizes that intelligence is not limited to solving problems or following pre-established rules: it involves constructing internal models of the world, which enable one to predict, generalize, and adapt one’s behavior to new situations. Thus, learning becomes central, as it allows the agent—whether human or machine—to continuously update its representations and improve its decision-making in complex and dynamic environments.

Thus, AI has no universal definition and remains a multidimensional concept that depends on the chosen analytical framework. This diversity of definitions demonstrates that AI is complex and encompasses various technologies capable of learning, understanding language, perceiving the environment, and making decisions autonomously.

2. Risks to Personal Data Posed by AI:

AI relies on data to learn and improve. As a result, the risks to personal data are not a side effect of artificial intelligence, but a direct consequence of its conceptual and operational foundations.

Indeed, according to Shoshana Zuboff (2019), AI cannot be viewed as a data-processing technology; rather, it is a central mechanism of surveillance capitalism, which collects and processes data—particularly personal data—and channels it toward the creation of economic value through prediction and behavioral modification (Zuboff, 2019, p. 42). AI is therefore not neutral; it serves economic interests. The risks associated with its use can extend to surveillance and control.

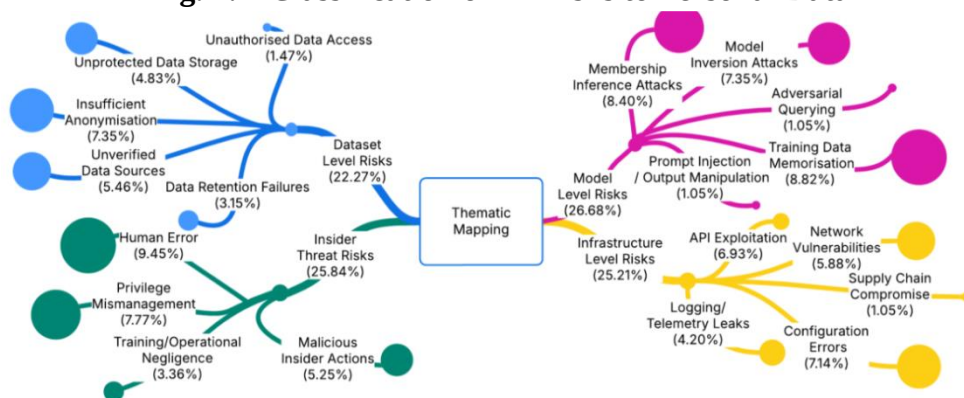
Artificial intelligence encompasses a broad range of computational techniques, among which machine learning and deep learning play a central role in contemporary applications. Although these subfields differ in their technical implementation methods, they share a common characteristic: the large-scale processing of personal data to identify patterns, make predictions, and automate decisions. These techniques are primarily encountered through concrete applications widely used by the general public, such as chatbots, recommendation systems, social media platforms, and geolocation services.

Grace Billiris, Asif Gill, and Madhushi Bandara (2025) conducted a systematic review of 45 studies published between 2020 and 2025 to identify the main risks to personal data privacy associated with AI. The researchers identified 19 risks, which they organized into four broad categories:

- *Risks related to the data itself*: poor anonymization, improper collection, incomplete or erroneous data.
- *Risks related to AI models*: the models' ability to retain or infer sensitive information from the data.
- *Infrastructure risks*: Technical systems (servers, pipelines) may be misconfigured or hacked.
- *Human-related risks*: Errors or misconduct by individuals (employees, users) can lead to data breaches.

This study revealed that the risks are distributed almost equally across the four categories (22.26%, 26.67%, 25.20%, and 25.87%, respectively) (Billiris et al., 2025, p. 5). However, among the 19 identified risks, human error accounts for 9.45%, followed by intentional memorization models (8.82%) and membership inference attacks (8.40%), as shown in the following figure.

Fig. 1: « Classification of AI Risks to Personal Data »



Source : (Billiris & al, 2025, p 05).

Thus, human error is the greatest risk when using AI. Another study confirms this finding. IBM Security's «Cost of a Data Breach Report 2025» states that, across 16 countries in various regions of the world, human error accounts for 27% of data breaches across all industries. One of the most glaring examples of human error is that of “Shadow AI”. This error occurs when employees enter confidential personal data into a public AI system for professional purposes (such as writing a report or summary). This action can lead to a data breach, as the AI may regurgitate the entered data to other users during subsequent sessions. The company will also lose track of the data. Hence the importance of training and monitoring individuals who have access to personal data. Employees should avoid free AI tools and use the secure tools provided by the company.

The study by Grace Billiris, Asif Gill, and Madhushi Bandara also demonstrates that the intentional memory typically found in generative AI (ChatGPT, Gemini, Claude, etc.), social media, recommendation AI, and healthcare AI intentionally stores personal data through overfitting and storage capacity. Taking generative AI as an example, if a very specific email address has been leaked on a forum, it can be reproduced verbatim with just a few prompts. Even though this risk isn't as high for social media and recommendation models, the fact remains that specific recommendations (health status, political views, etc.) can reveal the nature of your current concerns to anyone looking at the screen. Messaging AI also stores email addresses, phone numbers, and even short chat threads. All it takes is for another user to type the beginning of a sentence, a number, or an email address to retrieve the desired data.

As for the risk of membership inference attacks, it can be explained as follows. Overfitting in AI creates familiarity with data that has already been seen or processed. An attacker knows that the AI behaves differently with data it is familiar with versus data it is processing for the first time. If the AI answers the attacker's questions with certainty, the attacker can deduce that the data has indeed undergone specific processing. The central issue that amplifies the risks of AI regarding personal data lies in the difficulty of "unlearning" the data once it has been processed by the AI. In other words, even though deleting personal data entered into an AI system is technically possible through radical methods such as retraining (deleting the data from the source and then retraining the model from scratch), these methods cannot be applied to LLM (Large Language Models) such as GPT-4 and Cloud, which use billions of connections to process data. This data is not stored in a specific location; it is dispersed across these billions of connections, making the deletion of data (1) technically difficult because it will affect the model's quality and (2) economically impossible because this retraining process will cost billions of dollars and take several months. If just 0.1% of users of these AI models request the deletion of their data, the company that created the model would go bankrupt within a few days. (EDPB, 2025, p. 05). Other solutions have recently emerged to mitigate the risks associated with LLM³ models, which should already be scaled down to reduce retraining costs, but which should also incorporate algorithms that mitigate these risks—such as "Guardrails" filtering algorithms, which are software layers that moderate inputs and outputs to prevent data leaks. (IAPP, 2024, pp. 50–51). Personal data breaches caused by the use of AI have a significant economic impact. According to the IBM Cost of a Data Breach 2025 report, the average cost of data breaches in the United States reached 10.22 million dollars in 2025. A legal framework should be coupled with governance practices to regulate AI systems and reduce the risks associated with their use on personal data.

3. Legal Framework for AI Related to Personal Data Protection:

Artificial intelligence is now a major focus of data governance. Indeed, Jobin, Ienca, and Vayena⁴ (2019) show that international ethical guidelines on AI converge toward a set of dominant principles, including transparency, fairness, accountability, security, and privacy. These principles, developed primarily by the OECD, aim to promote AI as a driver of productivity. The legal framework addressing the risks of AI related to personal data appears to be a central global issue. This is because it must serve both as a regulatory constraint and as a support for the creation of an open and secure data ecosystem. Algeria's legal framework on personal data protection and AI-related risks is still in the early stages of development, but it can be analyzed in light of international standards.

3.1. European Union:

The European Union is a leader in the legal framework for AI systems, through the General Data Protection Regulation (GDPR) and the AI Act (Regulation (EU) 2024/1689). The GDPR has served as the legal foundation for personal data protection in the European Union since 2018 and fully applies to automated processing based on artificial intelligence, particularly with regard to profiling and automated decision-making. This regulation enshrines fundamental principles such as lawfulness, transparency, data minimization, and the accountability of data controllers, while expanding the rights of data subjects (access, rectification, erasure, portability). Its extraterritorial scope and strengthened penalty regime (up to 4% of global revenue) make it a major benchmark in data governance. This framework is supplemented by the AI Act (EU Regulation 2024/1689), which introduces specific regulations for artificial intelligence based on a risk-based approach. The AI Act is the most comprehensive law of its kind in the world; it was adopted in June 2024 and entered into force on August 1, 2024. This law classifies AI into four risk categories and assigns obligations based on the level of risk (European Parliament & Council, 2024).

- Unacceptable risk (banned since 2025): Certain AI systems infringe upon fundamental rights, such as the social scoring of citizens or the exploitation of children or people with disabilities. These AI systems are strictly prohibited
- High risk (currently in use): These are AI systems that can directly affect rights, alter economic opportunities, and reduce personal safety. These systems are used in healthcare, human resources, access to credit and social benefits, education, etc. This AI is permitted but must be strictly regulated: human oversight, robustness testing, and data traceability.
- Limited risk (transparency requirement): Systems that generate text, voice, or images, as well as chatbots and conversational assistants, are required to clearly inform the user that they are interacting with AI.
- Zero risk (unrestricted use): These are AI systems used in everyday life, such as recommendation AI, spam filters, video games, etc. This type of AI does not require any obligations because the risk is practically zero.

Together with the GDPR, the AI Act forms a coherent and strengthened legal framework. While the GDPR protects data, the AI Act ensures the governance of AI systems and thus protects personal data against unfair use and algorithmic discrimination (such as in the screening of resumes during recruitment). It also limits biometric surveillance, mandates transparency, and imposes heavy penalties for any attempt to violate its requirements.

3.2. The United States:

In the United States, personal data protection is based on a sector-specific and fragmented legal framework. There is no federal law similar to the GDPR; however, legislation such as HIPAA for healthcare, GLBA for financial services, and COPPA for children's data—supplemented by the central role of the Federal Trade Commission (FTC)—punishes unfair or deceptive practices related to the use of data and AI systems. Furthermore, several states have adopted cross-sectoral data protection laws, notably the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), which introduce rights similar to those of the GDPR and apply to certain uses of AI. On the non-binding front, soft law instruments shape risk governance, such as the NIST AI Risk Management Framework (2023) and the Blueprint for an AI Bill of Rights published by the White House (2022), which emphasize privacy protection, bias mitigation, and algorithmic transparency. The current debate centers on the federal government's ability to override (more protective) state laws to promote national innovation. In 2026, the balance remains precarious, forcing researchers and companies to adopt the highest standard (California/Colorado) to ensure compliance across the entire country (FTC, 2026).

4. Algeria :

In Algeria, AI is not subject to any specific legal framework. To date, there is no law or national strategy specifically addressing AI. The risks it poses to personal data are addressed by Law No. 18-07 of June 10, 2018, on the protection of personal data and regulated by the National Authority for the Protection of Personal Data (ANPDP), established by the same law and launched in 2022 (CMS Expert Guide, 2022) This law applies to all automated (and non-automated) processing, including that based on AI systems. By adhering to the three fundamental principles of personal data protection (confidentiality, integrity, and availability of data), this law:

- Grants data subjects the right to access and rectify their personal data, as well as the right to object to data processing or to withdraw consent during processing.
- Requires data controllers to appoint a Data Protection Officer (DPO) who must (1) notify the ANPDP or request authorization (for sensitive data) for data processing, (2) obtain prior consent from data subjects for processing, (3) explain the purpose of the processing to data subjects and the ANPDP, (4) ensure the confidentiality and security of the data, particularly if the data controller engages a processor (in which case they must inform the

ANPDP and the data subjects), They must also enter into a strict contract with the processor to ensure data security and confidentiality), (5) minimize data use, (6) report personal data incidents to the ANPDP and the data subjects.

Law No. 18-07 is supplemented by Law No. 09-04 of 2009 on the prevention and combating of offenses related to information and communication technologies. This law focuses on the security of systems and data. Indeed, AI systems, particularly chatbots and recommendation systems, can serve as vectors for personal data breaches by facilitating unauthorized access, disclosure, or manipulation of data, which justifies the application of the criminal provisions set forth in Law No. 09-04 of 2009.

This framework, which focuses primarily on automated data processing, remains limited, however, when it comes to the specific challenges posed by AI.

II. Empirical Study :

1. Presentation of the Sample and Sociodemographic Profile :

The study was conducted with a sample of 120 respondents residing in Algeria. Data collection took place via an online questionnaire distributed during 2026. The sampling was non-probabilistic by reasoned choice, targeting regular or occasional users of artificial intelligence-based technologies. The most represented age groups are 18–25 years old (43.33%), 26–35 years old (28.33%), and 36–44 years old (16.66%). 92.5% of respondents have a higher education degree. This targeting ensures an adequate understanding of the issues related to AI.

2. Measurement Instrument :

The research instrument is a structured questionnaire divided into six sections:

- **Level of AI Knowledge:** Consisting of an ordinal question (5-point Likert scale) on self-assessment of AI knowledge (AI_Knowledge_Level), and dichotomous questions (Yes/No) whose sum forms the variable Actual_AI_Knowledge_Score, designed to verify the level of AI knowledge reported by users (verification of the subjective level against the actual level).
- **Exposure to AI:** measured by the variable Score_variety_AI, which represents the variety of AI-based technologies used by respondents. It is calculated as the sum of the following variables (dichotomous questions: Yes/No): use of social media, use of generative AI, use of recommendation engines, use of search engines, use of location-based apps, use of financial apps, use of online government services, and use of facial recognition services.
- **Perception of AI risks regarding personal data:** represented by the variable Score_perception_risks, calculated as the arithmetic mean of the four items on the scale that assess users' fears regarding: data leaks,

- surveillance, unauthorized collection, and sharing of personal data without consent. (Dichotomous questions: Yes/No).
- **Knowledge of the legal framework governing personal data protection:** measured using a rating-scale question asking respondents to self-assess their level of knowledge regarding personal data protection, recorded in the variable *Connaissance_Cadre_juridique_PDP* (PDP: Personal Data Protection). This self-reported level of knowledge is verified by a dichotomous (Yes/No) question regarding their awareness of the existence of the ANPDP.
 - **Attitude toward regulations limiting the use of personal data:** The variable *Regulations_Limiting_PD_use* is derived from an ordinal question (5 point Likert scale) asking whether respondents are very supportive, supportive, somewhat supportive, unsupportive, or very unsupportive of strict regulations limiting the use of personal data by AI, knowing that this will affect application performance.
 - **Protective behavior:** assessed by the *Protection_Practices_Score* variable. This composite score is based on the sum of four specific actions: adjusting privacy settings, limiting the sharing of personal data, using a VPN, and using secondary email addresses for unofficial services, as determined by dichotomous questions (Yes/No).

The reliability of the scales is confirmed by a Cronbach's alpha of 0.706, indicating good internal consistency.

The data were analyzed using IBM SPSS Statistics software (version 27.0.1). We used descriptive statistics (frequencies, means), tests for comparing means (t-test for independent samples), and correlation analyses (Pearson's and Spearman's correlations, as well as linear regressions) to test our hypotheses.

3. Hypothesis Testing

3.1. Testing the First Hypothesis

First Hypothesis: *The level of knowledge about artificial intelligence significantly influences perceptions of risks related to personal data protection.*

To validate the reported level of knowledge, we performed a Spearman correlation test between the variable *AI_Knowledge_Level* and the variable *Actual_AI_Knowledge_Score*. The relationship between these two variables shows a trend toward significance ($\rho=0.175$ and $p=0.056$) Although slightly above the critical threshold of 0.05, this result suggests an overall consistency between respondents' self-assessments and their objective knowledge.

To test our first hypothesis, we performed a Pearson correlation test between the variable *Risk_Perception_Score* and the variable *AI_Knowledge_Level*. The results are presented in the following table.

Table. 2: «Pearson's correlation between Risk_Perception_Score and AI_Knowledge_Level»

Pearson Correlation			
		AI_Knowledge_Level	Risk_Perception_Score
AI_Knowledge_Level	Pearson Correlation	1	0,191*
	Sig. (two-tailed)		0,037
	N	120	120
Risk_Perception_Score	Pearson Correlation	0,191*	1
	Sig. (two-tailed)	0,037	
	N	120	120

*. The correlation is significant at the 0.05 level (two-tailed).

Source: SPSS V27

Pearson's correlation analysis confirms the existence of a statistically significant link between the level of knowledge about AI and the overall perception of risks ($r = 0.191$; $p = 0.037$). This correlation demonstrates that awareness of the challenges posed by AI increases with the level of familiarity perceived by the individual.

To reinforce this result, we performed a linear regression test between AI_Knowledge_Level (independent variable) and Risk_Perception_Score (dependent variable).

Table.3: «Linear regression analysis between risk perception and level of AI knowledge»

Summary of Models				ANOVA ^a					
R	R-deux	R-deux ajusté	Erreur standard de l'estimation	Somme des carrés	ddl	Carré moyen	F	Sig.	
0,191 ^a	0,036	0,028	0,82155	Régression	3,012	1	3,012	4,463	0,037 ^b
				de Student	79,644	118	0,675		
				Total	82,656	119			
a. Prédicteurs : (Constante), AI_Knowledge_Level				a. Variable dépendante : Risk_Perception_Score					
				b. Prédicteurs : (Constante), AI_Knowledge_Level					

Source : SPSS V.27

The level of knowledge about AI is a significant predictor of risk perception ($R^2 = 0.036$). Indeed, the analysis of variance (ANOVA) confirms that the regression model is significant ($F = 4.463$ and $p = 0.037$). These results confirm our first hypothesis. Thus, the more knowledge users have about AI, the higher their perception of AI-related risks.

3.2. Testing the second hypothesis

Second hypothesis: *The variety of uses for AI-based technologies influences Algerian citizens' perception of risks*

A Pearson correlation test was conducted between the variable Risk_Perception_Score and the variable AI_Variety_Score to determine whether there is a relationship between these two variables.

Table. 4: «Pearson's correlation test between risk_perception and AI_Variety_Score»

Pearson Correlation			
		Risk_Perception_score	AI_Variety_Score
Risk_Perception_score	Corrélation de Pearson	1	0,187*
	Sig. (bilatérale)		0,041
	N	120	120
AI_Varety_Score	Corrélation de Pearson	0,187*	1
	Sig. (bilatérale)	0,041	
	N	120	120

*. The correlation is significant at the 0.05 level (two-tailed).

Source: SPSS V.27

This result ($p=0.041$) confirms the existence of a positive correlation between risk perception and the variety of AI applications.

To further analyze this relationship, we conduct a simple linear regression test, using risk perception as the dependent variable and the variety of AI applications as the independent variable.

Table. 5: «Simple linear regression between perceptions of AI risks and the variety of AI uses»

Summary of Models				ANOVA ^a					
R	R-deux	R-deux ajusté	Erreur standard de l'estimation	Somme des carrés	ddl	Carré moyen	F	Sig.	
0,187 ^a	0,035	0,027	0,82214	Régression	2,898	1	2,898	4,288	0,041 ^b
				de Student	79,758	118	0,676		
				Total	82,656	119			

a. Prédicteurs : (Constante), AI_Variety_Score

a. Variable dépendante : Risk_Perception_Score

b. Prédicteurs : (Constante),AI_Variety_Score

Source : SPSS V.27

The variety of AI usage explains 3.5% of the variation in the perception of AI risks ($R^2 = 0.035$). The simple linear regression model is statistically significant ($F(1,118) = 4.288$ and $p = 0.041$). According to this model, the score for the variety of AI usage significantly predicts the perception of AI risks regarding personal data. In other words, the more citizens use AI-based technologies, the higher their perception of risk. Thus, we can confirm the second hypothesis.

3.3. Testing the third hypothesis :

Third hypothesis: ***Knowledge of the Algerian legal framework regarding personal data protection reduces the perception of risks associated with AI.***

Before testing this hypothesis, it is important to assess respondents' perceived knowledge of the legal framework for personal data protection.

A t-test for independent samples was conducted to compare respondents' perceived knowledge of data protection rules between those familiar with the ANPDP (Yes, N=40) and those unfamiliar with it (No, N=79). The results reveal a highly significant difference ($t(63.8) = -3.79$; $p < 0.001$). Respondents familiar with the ANPDP feel significantly more informed ($M = 3.37$; $SD = 1.11$) than those unaware of the existence of this authority ($M = 4.11$; $SD = 0.83$). The effect size, measured by Cohen's d ($d=0.80$), indicates a large effect. These data confirm that awareness of the regulatory authority (ANPDP) is a major indicator of users' sense of mastery of the legal framework.

To test our third hypothesis, we performed a Pearson correlation test between the variable `Score_perception_risks` and the variable `Knowledge_legal_framework_PDP`. The results are shown in the following table.

Table.6:«Pearson's correlation coefficient between Risk_Perception_score and Legal_Framework_Knowledge_PDP»

Correlations			
		Risk_Perception_score	Knowmedge_legal_framework_PDP
Risk_Perception_score	Corrélation de Pearson	1	-0,002
	Sig. (bilatérale)		0,984
	N	120	120
Knowmedge_legal_framework_PDP	Corrélation de Pearson	-0,002	1
	Sig. (bilatérale)	0,984	
	N	120	120

Source: SPSS

Pearson's correlation analysis shows a complete lack of a significant link between the sense of being informed about the legal framework for personal data protection and the overall perception of risks associated with AI ($r = -0.002$; $p = 0.984$). This result indicates that for the Algerian users in our sample, reported knowledge of legal rules has no influence, either positive or negative, on their level of concern regarding artificial intelligence. The third hypothesis is not confirmed. Although respondents who are familiar with the ANPDP feel better informed about the legal framework for personal data, the existence of this framework does not reduce their fear of AI.

3.4. Testing the fourth hypothesis

Fourth hypothesis: *The perception of risks associated with AI positively influences support for strict regulations limiting the use of personal data.*

To test this hypothesis, a Pearson correlation test was conducted between the variable Risk_Perception_Score and the variable Regulations_Limiting_DP_Use.

Table.7: «Pearson correlation test between Risk_Perception_score and Regulations_Limiting_PD_Use»

Corrélations			
		Risk_Perception_sc ore	Regulation_Limiting_PD_ use
Risk_Perception_sc ore	Corrélation de Pearson	1	0,264**
	Sig. (bilatérale)		0,004
	N	120	120
Regulation_Limitin g_PD_use	Corrélation de Pearson	0,264**	1
	Sig. (bilatérale)	0,004	
	N	120	120

** . The correlation is significant at the 0.01 level (two-tailed).

Source: SPSS V.27

Pearson's correlation analysis ($r=0.264$; $p=0.004$) reveals a positive and highly significant relationship between the overall perception of risks associated with AI and a favorable attitude toward regulations limiting the use of personal data. This result supports the idea that Algerian users' concerns are not merely passive feelings, but rather translate into an explicit desire for legal oversight.

To further analyze the link between attitudes toward regulation and users' concerns, a simple linear regression was performed.

Table.8: «Simple linear regression between Risk_Perception_Score and Regulations_Limiting_PD_use»

Summary of Models				ANOVA ^a				
R	R- deux	R- deux ajusté	Erreur standard de l'estimation	Somme des carrés	ddl	Carré moyen	F	Sig.
0,264 ^a	0,070	0,062	0,80732	Régression	5,749	1	5,749	8,820
				de	76,908	118	0,652	0,004 ^b
				Student				
				Total	82,656	119		

a. Prédicteurs : (Constante),
Regulation_Limiting_PD_use_DP

a. Variable dépendante: Risk_Perception_score
b. Prédicteurs : (Constante),
Regulation_Limiting_PD_use_DP

Source : SPSS V.27

The model is highly significant ($F(1,118)=8.820$; $p=0.004$) and indicates that the desire to limit the use of personal data by AI explains 7% of the variance in overall risk perception ($R^2=0.070$). These results confirm that the perception of

technological risk among Algerians in our sample is intrinsically linked to a need for legal safeguards. It is noteworthy that respondents are willing to accept a decrease in the performance of AI applications in exchange for greater protection of their privacy. These results demonstrate that data security has become a top priority, taking precedence over technological efficiency. Thus, the fourth hypothesis is confirmed.

3.5 Analysis of Protective Behaviors

For this study, it is of interest to determine whether users' concerns or their sense of expertise translate into the actual implementation of self-protection strategies. Thus, we need to conduct a Pearson correlation test between the variable Risk_Perception_score and the variable Protection_Practices_Score, and another Pearson correlation test between AI_Knowledge_Level and Protection_Practices_Score

Table. 9: «Pearson's correlation test between Risk_Perception_score and Protection_Practices_Score»

Correlations			
		Protection_Practices_Score	Risk_Perception_score
Protection_Practices_Score	Corrélation de Pearson	1	-0,141
	Sig. (bilatérale)		0,125
	N	120	120
Score_Perception_risques	Corrélation de Pearson	-0,141	1
	Sig. (bilatérale)	0,125	
	N	120	120

Source: SPSS V.27

Table. 10: «Pearson correlation test between AI_Knowledge_Level and Protection_Practices_Score»

Corrélations			
		AI_Knowledge_Level	Protection_Practices_Score
AI_Knowledge_Level	Corrélation de Pearson	1	-0,191*
	Sig. (bilatérale)		0,037
	N	120	120
Protection_Practices_Score	Corrélation de Pearson	-0,191*	1
	Sig. (bilatérale)	0,037	
	N	120	120

*. The correlation is significant at the 0.05 level (two-tailed).

Source: SPSS V.27

The data analysis reveals a clear distinction between the influence of knowledge and that of anxiety on safety behaviors.

On the one hand, a significant correlation is observed between the reported level of knowledge and the Protection_Practices_Score ($r = -0.191$; $p = 0.037$). This

result indicates that a sense of technical expertise promotes the adoption of concrete measures: the more competent users consider themselves to be, the more they use tools to protect themselves.

On the other hand, no significant link was established between risk perception and the implementation of these practices ($r = -0.14$; $p = 0.125$). This finding highlights a “privacy paradox” within our sample: although users express genuine fears regarding AI, this concern does not translate into active self-protection. It therefore appears that technical know-how (having sufficient knowledge about AI) is a more powerful driver of action than mere awareness of the danger when it comes to encouraging digital caution.

4. Discussion of the results:

This study demonstrates that perceptions of AI-related risks in Algeria are shaped by practical experience and a sense of expertise. Our results confirm that the variety of technologies used ($p = 0.041$) and the level of knowledge about AI ($p = 0.037$) significantly influence perceptions of danger. This sense of expertise serves as a concrete lever for action: it promotes the adoption of protective practices ($p=0.037$), whereas concern alone fails to change individual behaviors ($p=0.125$).

The analysis also highlights the importance of the institutional framework. Although theoretical knowledge of Law 18-07, particularly its provisions on prior consent and the purpose of processing, does not directly influence the perception of risks ($p=0.984$), public awareness of the ANPDP emerges as the central pillar of the sense of legal certainty. This expectation of protection, rooted in the fundamental rights of access and objection guaranteed by the legislature, translates into a significant desire for regulation ($p=0.004$). Users thus demonstrate a clear trade-off, prioritizing the confidentiality and integrity of their data over technological performance. These results demonstrate that the perception of risks associated with AI goes beyond the mere existence of legal texts; the latter alone appears insufficient to allay the fears of young users. Consequently, the role of the ANPDP is crucial, not only to ensure the enforcement of the law but also to ensure its dissemination to the general public.

Conclusion

In conclusion, perceptions of AI-related risks in Algeria are shaped by practical experience and the need for institutional security among young people with higher education. The study demonstrates that familiarity through use and the visibility of regulatory authorities, such as the ANPDP, are the true pillars of digital trust. Enhancing the ANPDP’s visibility and transforming everyday digital experiences into genuine legal expertise appear to be the essential drivers of a smooth digital transition.

Bibliographic References :

- ANPDP (2025) Délibération n ° 01 qui définissent le Délégué à la Protection des Données, ses activités et comment le désigner » sur <https://anpdp.dz/ar/storage/2025/12/DELIBERATION-1.pdf>
- Billiris, G., Gill, A., & Bandara, M. (2025). Privacy in the Age of AI: A Taxonomy of Data Risks. *Journal of Data and Information Quality*. In file:///C:/Users/Splendid/Downloads/Privacy_in_the_Age_of_AI_A_Taxonomy_of_Data_Risks.pdf
- CMS Expert Guide. (2022). *Data protection and cybersecurity laws: Algeria*. CMS Law. In <https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/algeria2>
- European Data Protection Board. (2025). *AI: Complex algorithms and effective data protection supervision – Effective implementation of data subjects' rights*. In https://www.edpb.europa.eu/system/files/2025-01/d2-ai-effective-implementation-of-data-subjects-rights_en.pdf
- McCarthy, J. (2007). *What is artificial intelligence?* Stanford University. In <http://jmc.stanford.edu/articles/whatisai/whatisai.pdf>
- IBM Security. (2025). *Cost of a data breach report 2025*. <https://www.ibm.com/reports/data-breach>
- International Association of Privacy Professionals. (2024). *AI governance in practice report 2024*. IAPP. in https://assets.contentstack.io/v3/assets/bltd4dd5b2d705252bc/blt99a18c62ab0b92a7/ai_governance_in_practice_report_2024.pdf
- European Parliament & Council. (2024). *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Official Journal of the European Union, L 1689, July 12, 2024
- Jobin, A., Ienca, M., & Vayena, E. (2019). ***The global landscape of AI ethics guidelines***. *Nature Machine Intelligence*, 1(9), 389–399. In file:///C:/Users/Splendid/Downloads/Jobinetal.-2019-ThegloballandscapeofAIethicsguidelines.pdf
- Russell, S., & Norvig, P. (2020). *Artificial Intelligence: A Modern Approach* (4th ed.). Pearson. In http://lib.ysu.am/disciplines_bk/efdd4d1d4c2087fe1cbe03d9ced67f34.pdf
- Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs. From file:///C:/Users/Splendid/Downloads/Zuboff,%20Shoshana.The%20Age%20of%20Surveillance%20Capitalism.2019.pdf
- Federal Trade Commission. (2026). *Algorithmic accountability and data provenance in autonomous systems: Enforcement report 2025-2026*. U.S. Government Publishing Office. In <https://www.congress.gov/bill/119th-congress/house-bill/5511/text> LeCun, Yann (2022). *A Path Towards*

Autonomous Machine Intelligence (version 0.9.2), OpenReview, 2022. In <https://openreview.net/pdf?id=BZ5a1r-kVsf>

¹ John McCarthy (1927–2011) was an American computer scientist and mathematician considered to be the leading pioneer of artificial intelligence; he developed several algorithms and programming languages that played a major role in AI programming during his time.

² McCarthy assumes that AI operates on concepts rather than images, sounds, and raw data from the real world. He considers issues related to the physical world and perception to be secondary, since machines must first solve all kinds of intellectual problems.

³ Large Language Models (LLMs) are artificial intelligence systems trained on very large text corpora to capture statistical patterns in language. Their learning mechanism, based on the aggregation and interdependence of data, means that information cannot be isolated. This transforms unlearning into a problem of irreversibility and adjustment costs, rather than a simple operation of information deletion.

⁴ Jobin, Ienca, and Vayena (2019) examined 84 documents (guidelines, statements, reports) from international organizations, governments, companies, universities, and professional associations. They used a mapping method to identify the themes of their research.