



ARTIFICIAL INTELLIGENCE: A NEW CHALLENGE TO THE RIGHT TO DIGITAL PRIVACY

Sarah KHOUALEF *

University of AinTemouchent - Algeria
sarah.khoualef@univ-temouchent.edu.dz

Send Article Date: 06-06-2026

Date of acceptance of the article: 18-08-2026

Abstract:

The right to digital privacy is an extension of the right to privacy, and constitutes one of the rights of human personality protected by law. However, the widespread use of artificial intelligence across various fields has resulted in multiple violations of this right, particularly in the absence of specific legal frameworks regulating artificial intelligence applications and their use of individuals' personal data. This situation calls for strengthening the protection of the right to digital privacy and urging developers of artificial intelligence application to adhere to a set of ethical principles that ensure the protection of individuals and their data.

Keywords: digital privacy; artificial intelligence (AI); personal data protection; AI ethics; legal regulation.

Introduction:

The technological revolution has profoundly transformed our lives, as evidenced by the widespread use of various technological and scientific applications based on artificial intelligence, such as smart phones, self-driving vehicles, drones, robots, and others. Despite the considerable benefits this technology offers, it has raised numerous issues and concerns regarding human rights, particularly individual privacy. This is because such applications can only function effectively when supplied with individuals' personal data. The more data they obtain, the better they perform.

These data fall within the scope of the right to digital privacy, which constitutes an inseparable component of the broader right to privacy-one of the most fundamental human rights. Even before the

* Sarah KHOUALEF.

advent of the internet and artificial intelligence, the right to privacy was enshrined in the 1948 Universal Declaration of Human Rights, which represents the first international legal instrument recognizing this right, followed by the 1966 International Covenant on Civil and Political Rights under Article 17. As modern technologies evolved and the concept of digital privacy emerged as a new dimension of the right to privacy, several international conventions recognized and protected it in its contemporary form, including Convention No. 108 of the Council of Europe and the 2001 Budapest Convention on Cybercrime.

This study aims to examine the right to digital privacy and the extent to which artificial intelligence affects it, as well as to explore proposals that may contribute to protecting this right from AI-induced violations and the ethical principles that developers of AI applications and systems must adhere to.

In light of the concerns raised by artificial intelligence regarding the right to digital privacy, the central research questions of this study are as follows: How does artificial intelligence negatively impact the right to digital privacy? and what are the possible means to mitigate this impact?

To address these questions, this study adopts an analytical approach aimed at defining the concept of digital privacy and analyzing artificial intelligence in order to determine the nature and extent of its impact on this right.

The study is divided into two main sections: the first addresses the concept of the right to digital privacy, while the second examines the risks posed by artificial intelligence to digital privacy and the mechanisms for mitigating them.

1- The Concept of the Right to Digital Privacy:

The right to privacy is considered one of the most fundamental rights associated with individuals' lives, particularly with the human existence and personality, as it constitutes one of the primary manifestations of inherent human dignity. An individual cannot live solely on material interests; rather, life requires rights that are inherently and inextricably linked to the person. The individual has the right to exercise their personal rights without interference from others by any means, which constitutes the essence of the right to privacy. As for the right to digital privacy, it represents an inseparable



component of the right to privacy. Therefore, this section addresses, we will address the definition of the right to digital privacy in the first subsection, while in the second subsection, this study examines the subject matter and legal basis of the right to digital privacy.

1.1- The Definition and Subject Matter of the Right to Digital Privacy

The right to digital privacy constitutes one of the most significant legal development in response to the rapid expansion of digital technologies and the widespread processing of personal data. This right aims to ensure the protection of individuals' private lives in the digital environment by regulating the collection, use, and disclosure of personal information. In this context, the present section is divided into two main parts: the first examines the Definition of the Right to Digital Privacy, while the second addresses The Subject Matter of this Right.

1.1.1- Definition of the Right to Digital Privacy:

Digital rights are an extension of human rights in the age of the internet. The right to digital privacy refers to an individual's ability to control access to their personal information, its use, and its protection when using the internet. The right to digital privacy also enables individuals to remain anonymous online by safeguarding personal information such as names, addresses, email accounts, credit card details, and other sensitive digital data(Tiwari, 2024, p. 195).

The right to digital privacy is a modern and dynamic right, as it entails the establishment of a system of checks and balances to protect individuals during the processing of their personal data, ensuring that such processing remains lawful. Furthermore, such processing must comply with the essential components of personal data protection, particularly independent oversight and respect for the rights of the data subject. For example, when an employer records information relating to employees' names and the salaries paid to them, the mere recording of this information cannot be regarded as a violation of the right to digital privacy. However, if the employer transfers the employees' personal information to third parties without their consent and without informing them, this constitutes an interference with private life. In all cases, employers must comply with data protection

rules, as the recording of employee data constitutes a form of data processing(Giakoumopoulos& Christos, 2018, p. 20).

The emergence of the right to digital privacy is closely associated with concerns about the risks arising from the collecting and processing individuals' data for undeclared or unlawful purposes, as well as the misuse of such data or its transfer to other entities, particular emphasis is placed on the rights of the data subjects and the extent of their control over it. Consequently, attention was directed toward the protection of data related to individuals against the risks posed by the use of automated data processing systems as early as 1960s, as one of the earliest issues raised concerning information technology and its subjection to legal regulation(Janane, 2010, p. 18).

The credit for introducing the concept of digital privacy for the first time is attributed to two American authors: Alan Westin, in his book "Privacy and Freedom", and Arthur Miller, in his book "The Assault on Privacy". According to the jurist Alan Westin, information privacy (i.e., digital privacy) is defined as "the right of individuals to determine when, how, and to what extent information about them is communicated to others," whereas Miller defines it as "the ability of individuals to control the flow of information relating to them"(Sheibani & Ben Salem, 2023, p. 462).

Therefore, it can be stated that the right to digital privacy guarantees the security of individuals' personal data and information exchanged via the internet, ensuring that it is not unlawfully exploited or processed without the data subject's consent. This information includes not only identifying data such as names, photographs, date of birth, and passport number, but also behavioral data, preferences, interests, and the confidentiality of personal communications.

2.1.1- The Subject Matter of the Right to Digital Privacy:

The subject matter of the right to digital privacy is personal data, as defined in Law No. 18/07 on the protection of natural persons in relation to the processing of personal data(Algeria 18/07, 2018), specifically in Article 3, under the term "personal data," which provides as follows:

"Any information, regardless of its medium, relating to an identified or identifiable natural person-hereinafter referred to as 'the data subject'-directly or indirectly, particularly by reference to an



identification number or to one or more factors specific to their physical, physiological, genetic, biometric, psychological, economic, cultural, or social identity.”

From this definition, can be identified that there are two types of personal data:

A- Personally Identifiable data, which itself is subdivided into two categories:

- Alphabetical, numerical, or symbolic data, such as passwords that allow or prevent access to a personal computer, a workplace database, email accounts, data required to complete electronic commercial transactions, or to log into a forum or a personal account on a website.

- biometric identification data, such as fingerprint scans, iris scans, voiceprints, palm geometry, handwriting samples, facial recognition data, etc.

B- Sensitive Personal Data, which relates to anything concerning racial or ethnic origin, political opinions, religious or other beliefs, as well as personal data concerning health, sexual life, or criminal records. These data are stored by public and private institutions in the form of databases or on network servers. Databases maintained by various organizations are a major source of such data, as are media contents published on social media platforms and data collected and analyzed by investigative and intelligence agencies.

As for the right to privacy, it entails the prohibition of collecting personal data, as defined in the aforementioned article, without the data subject's consent, or the using such data for unlawful purposes. This data collection is carried out through multiple mechanisms, including:

A- Collecting personal data via sales channels and selling them to third parties, or building a digital profile of the person by monitoring and tracking their behavior on the internet and displaying commercial or political advertisements tailored to the individual's interests to induce them into contracts or achieve certain objectives. This is done through cookies or what is known as “tracking files,” which collect information for advertising purposes without the user's consent, and is considered a violation of the right to digital privacy. This is precisely what occurred when a group of individuals filed a

lawsuit against Facebook, claiming it had used cookies and various plug-ins to track and store information regarding users' visits to third-party websites and then sold this data to advertisers. Facebook was found liable and was ordered to pay USD 90 million to settle 21 lawsuits)Espace_réservé(1(Al-Shamsi, 2022, p. 42).

B- Collecting personal data through “web bugs”, which are invisible elements embedded within email pages and websites. These components transmit information about user activity on a website, such as copying or downloading pages. They can also detect the timing of when a user opens their email or whether the message has been forwarded to others. These elements are also used to analyze web pages. Although they are usually not harmful and are not classified as viruses, their danger lies in the type of information they collect.

C- Personal data is also collected through what is known as “spyware”, which covertly monitors user activity in ways that are difficult to detect. Spyware can record passwords, access computer files, and transfer them from the user's device to a third party without their consent. It can be used for cyber extortion, whereby sensitive personal data is used as leverage in exchange for financial compensation(Al-Shamsi, 2022, p. 42).

2.1- The Scope of the Right to Digital Privacy and the Position of the Algerian Legislator

The right to digital privacy lies between two contradictory poles: on the one hand, the individual's right to private life, and on the other, the necessity imposed upon states and governments to ensure a minimum threshold of security and to curb crimes committed via the internet. This will be explored in Part One, titled “The Scope of the Right to Digital Privacy”. In Part Two, we will examine the extent to which the Algerian legislator recognizes and adopts the right to digital privacy, under the heading “The Position of the Algerian Legislator on the Right to Digital Privacy”.

1.2.1- The Scope of the Right to Digital Privacy:

The right to digital privacy is subject to a set of necessities that help delineate its scope, including the following:

A -The necessity of coordinating between the individual's right to digital privacy and the state's right of access to such data for the purpose of ensuring better organization of social life. It should be



noted that this, in principle, does not constitute a violation of private life, except in cases where personal data are used for purposes that contradict the safeguarding and respect of such privacy(Khdouja, 2017, p. 148).

B- The necessity of reconciling the individual's right not to disclose any data related to their privacy with their interest in voluntarily disclosing such information to derive benefits. As long as the disclosure is made voluntarily, it does not conflict with the right to digital privacy except when such voluntarily disclosed data are exploited for purposes that violate individual dignity and breach private life(Belassel Bint Nabi Yasmine, 2021, p. 11).

C- The necessity of balancing the positive and negative effects resulting from the emergence of information systems, which serve as mechanisms for collecting and processing personal data related to private life in the context of organizing electronic interactions. Due to the high efficiency and virtually unlimited capacity of these information systems in analyzing and retrieving data electronically, most countries and institutions have moved toward establishing databases that support these processes. However, this has also led to a rapid awareness of the dangers posed by information technologies to privacy. The core concern lies in the indefinite storage and easy retrieval of such data, which may compromise individuals' private life. Additionally, the risk of data generated by electronic transactions being leaked, hacked, extracted, or misused transforms this technological advancement from a positive tool into a threat to the stability and confidentiality of private life(Fayed, 2008, p. 48).

Since the subject matter of the right to digital privacy is personal data, which serve as a source of private and sensitive information, its scope is wide and multifaceted. Personal data are present across numerous domains and information systems, particularly in the databases and digital systems of institutions and administrative bodies, such as medical records, court case files, and employee lists. The right to digital privacy also extends to communications and communication and transmission networks over the internet(Khdouja, 2017, p. 149).

2.2.1- The Position of the Algerian Legislator on the Right to Digital Privacy:

The Algerian legislator has not remained passive in the face of the ongoing transformations in information technology and the criminal activities associated with it. Rather, a set of legal texts has been enacted within the Constitution, organic and fundamental laws, and the Penal Code aimed at recognizing and protecting the right to digital privacy.

All previous constitutions, including the current Constitution of 2020, have recognized the right to privacy and considered it an inviolable constitutional right. The 1963 (Constitution, 1963), Constitution established the principle of protecting human dignity and protecting it from any physical or moral assault, and enshrined the inadmissibility of violating elements of this right, such as the inviolability of the home and personal correspondence. Similarly, the 1976 (Ordinance, 1976) Constitution explicitly recognized the inadmissibility of violating the sanctity of citizens' private lives and ensured the confidentiality of communications and correspondence. The 1996 (Decree, No. 96/438, 1996), Constitution went further than merely recognizing the right to privacy as an absolute constitutional right; it considered it one of the obligations that individuals must observe when exercising other rights, requiring them to preserve privacy and confidentiality.

The Algerian legislator reaffirmed this commitment to the right to privacy through the 2020 (Decree, 20/442, 2020) constitutional amendment, particularly in Article 47, which stipulates the need to protect natural persons in the processing of their personal data and considers such protection a fundamental right. In Article 81 further affirms that everyone has the right to exercise their freedoms, provided that this is done in a manner that respects the rights recognized for others in the Constitution including the right to privacy.

Furthermore, the Algerian legislator recognized the right to digital privacy within criminal law by granting it special protection under Law No. 04/15, amending the Penal Code (04/15, 2004). This law dedicated a specific section entitled "Offenses against Automated Data Processing Systems". Additionally, Law No. 09/04, which sets



out specific rules for the prevention of and the fight against crimes related to information and communication technologies, was enacted to introduce investigative procedures consistent with the nature of cybercrime(09/04, 2009).

In 2016, as part of efforts to harmonize Algeria's legal framework with international legal developments, especially those related to combating terrorism, which has itself evolved rapidly, the Algerian legislator amended the Penal Code under Law No. 16/02(16/02, 2016). This law introduced three new articles: Articles 87 bis 11, 87 bis 12, and Article 394 bis, aimed at criminalizing terrorist crimes that rely on information and communication technologies.

2- the risks posed by artificial intelligence to digital privacy and the mechanisms for mitigating them:

Artificial intelligence has become an integral part of daily life. as it is now used in a wide range of tools, from smartphones and social media platforms to self-driving cars and smart home devices. Despite the immense benefits it provides, it also poses significant risks to the right to digital privacy. With the increasing use of AI in data collecting and analysis, individuals have become more vulnerable to breaches and violations, as AI technologies rely on processing vast quantities of data to function efficiently. Accordingly, this section seeks to examine the impact of artificial intelligence on the right to digital privacy in Subsection One, while Subsection Two will explore the challenges of protecting this right in light of AI-related violations.

1.2- How Artificial Intelligence Affects the Right to Digital Privacy:

The individual's right to digital privacy has become increasingly vulnerable to interference and infringement, particularly in light of the expanding use of artificial intelligence applications, which has subjected this right to multiple and diverse risks. This development has necessitated the adoption of protective mechanisms and regulatory measures aimed at mitigating such violations. Accordingly, this section is structured into two subsections: the first examines the impact of the inherent characteristics of artificial intelligence on the right to digital privacy, while the second analyzes the manifestations

of the impact of artificial intelligence systems on the exercise of this right.

2.1.2- The Impact of AI Characteristics on the Right to Digital Privacy:

Artificial intelligence functions by developing machines and applications capable of replacing human intelligence through algorithms or mathematical models that analyze vast amounts of data to support decision-making and solve highly complex problems. The examples of such applications are numerous and diverse including voice assistants on smartphones, conversational agents such as ChatGPT, facial recognition systems, self-driving vehicles, and more. All of these applications can only achieve their intended functions by processing individuals' digital data, such as voice data, images, and textual content. Therefore, it has become impossible to speak of artificial intelligence without simultaneously addressing personal data(Hulin, 2023).

These capabilities have intensified concerns regarding privacy. The ability of this technology to infer sensitive information, such as individuals' locations, preferences, and habits, poses a significant risk when such data are disclosed or distributed without legal authorization or consent. Additionally, artificial intelligence contributes to threats related to personal data, including identity theft and unwarranted surveillance. These violations typically occur through the collection of digital personal data, most commonly via cookies and IP addresses—without the explicit consent of user(Al-Ashqar, 2025, p. 8).

The privacy problem is further exacerbated by the fact that AI algorithms can only develop and evolve through the processing of vast quantities of personal and sensitive data, such as health information, biometric data, and online behavior patterns. The more abundant and higher-quality the data, the more accurate and effective these algorithms become in prediction, classification, and interaction(Akakpo & Akwasi Gyasi, 2025, p. 1). There is a marked contrast between the performance of artificial intelligence before the emergence of Big Data and after it. In the past, AI was characterized by slow learning and limited data-analysis capacity. The true revolution in AI began with the advent of Big Data, which marked a qualitative leap in the digital data landscape and significantly



enhanced the effectiveness of artificial intelligence(Saghai & Malika Madhkour, 2024, p. 526).

Multiple entities now seek to access individuals' personal data, ranging from application and service providers to advertising and marketing partners, and sometimes even governmental and security agencies. The situation becomes increasingly complex when privacy in the era of AI turns into a tradable commodity, exchanged among these entities. For instance, companies like Facebook, Google, and Instagram engage in the mining of user data through AI, analyzing it according to their needs to interact with users more accurately through highly targeted advertisements tailored to each individuals' data profile, group affiliation, age, and other characteristics(Spalevic & Vicentijevic, 2022, p. 56). The larger the volume of data, the greater the potential profit. These companies rely on multiple and highly advanced AI techniques embedded in computing devices and search engines. These systems process, analyze, store, and deliver data to users. For example, when a user searches a specific topic on a search engine, they may later encounter the same topics reappearing, this is because AI algorithms access user data such as previous interests and search behavior. Thus, it becomes evident that smart technologies fundamentally operate on sensing and processing data. A simple click on a search engine or browsing a particular site renders the individual a monitored and targeted subject stripped of a significant portion of their right to privacy(Saghai & Malika Madhkour, 2024, p. 528).

2.2- Manifestations of AI Systems' Impact on the Right to Digital Privacy

Artificial intelligence can contribute to several risks that violate the right to digital privacy, such as identity theft and unwarranted surveillance. Numerous concerns arise merely from considering how individuals' data are stored and used, where such data are stored, and who is granted access to them. Accordingly, the manifestations of the impact of AI systems on the right to digital privacy can be summarized as follows:

A- Cloud Computing:

Cloud computing is a technology that allows users to access computing resources via the internet, provided through data centers owned by specialized companies. It involves storing data and software

online, enabling users to access and use them flexibly at any time and from anywhere. Here lies the danger: once data are stored in the cloud, they are transmitted and circulated across the internet, and subjected to smart algorithms that may potentially extract information that the user never intended to disclose. This raises serious concerns regarding the security and protection of individuals' data (Sheibani & Ben Salem, 2023, p. 470).

B- Human Activity Tracking:

With the widespread presence of the internet rendering homes and cities “smart” and the use of robots for domestic assistance or surveillance, these technologies are directly connected to personal data. The same applies to smart applications on smartphones, as well as self-driving vehicles and drones that collect personal information. These devices contain processing units or embedded chips within internet-connected objects or robotic systems, which serve as storage for the data they capture: images, sounds, and actions. Consequently, governments or other entities may monitor individuals and exert unprecedented control, leading to a loss of privacy and the potential abuse of power by those who control these surveillance technologies. This misuse could extend to violations of human rights and other forms of oppression (Al-Ashqar, 2025, p. 9)

C- Hacking and Breaching Sensitive Personal Data:

Among the most sensitive personal data are banking details, which are highly susceptible to AI-based risks through fraudulent and sophisticated methods, such as identity theft and the acquisition of credit card and electronic payment credentials. Additionally, violations may occur concerning health-related information, which enjoys particular protection and must not be compromised or must not be infringed. Today, several robots are programmed to perform surgical operations, which require the storage of patients' health information in the robot's database. This data could be leaked—either by the person operating the robot or by the robot itself, since it has been programmed to perform the operation. Such actions represent another form of privacy violation through the use of artificial intelligence tools, specifically medical robots (Dalila & Wali, 2024, p. 822).



1.2.2- Challenges to Protecting the Right to Digital Privacy Amid AI Violations:

Artificial intelligence (AI) technologies have engendered a complex and evolving environment fraught with unprecedented challenges concerning personal data protection and digital privacy. Unlike previous data-processing systems, modern AI extends far beyond basic classification or analytical tasks it now harnesses vast quantities of data for autonomous learning, the development of adaptive cognitive models, and the generation of predictive behaviors that often mimic or exceed human cognitive capacities (Sheibani & Ben Salem, 2023, p. 474). What exacerbates these challenges is the opacity and unpredictability of AI algorithms, many of which evolve autonomously and continuously. In fact, in numerous instances, even the original developers or system architects cannot explain, let alone control, the exact mechanisms behind the outcomes produced by their own algorithms. This "black box" nature of AI creates a considerable a legal and ethical gap.

As a result, ensuring digital privacy in this evolving landscape demands proactive, multi-tiered responses from individuals, institutions, and regulatory authorities. This section is divided into two parts: the first outlines key concerns regarding the widespread use of AI applications, while the second explores the ethical principles that should govern the design and deployment of AI technologies to safeguard the right to digital privacy.

A- Warnings Regarding the Expanding Use of AI Applications:

Protecting digital privacy from the growing risks associated with AI is not merely a technological issue—it is a fundamental human rights issue in the 21st century. The collection, processing, and monetization of personal data without adequate safeguards threaten the autonomy, dignity, and freedoms of individuals. Given the exponential growth of AI capabilities, a comprehensive, strategic, and anticipatory regulatory framework must be established—one that involves individuals, private sector entities, civil society, and state actors (El-Sadiq, 2023, p. 900). The following measures are central to such a framework:

- Balancing Utility and Protection: Individuals must be empowered to benefit from AI while maintaining control over their personal information. Digital literacy programs should promote best practices in privacy-aware behavior, such as using multi-factor authentication, encrypted communications, and exercising heightened caution when sharing personal details on untrusted platforms(Chinmay, 2025, p. 81).
- Establishing Robust Legal Protections: National legislation should be adopted or updated to specifically regulate the use of AI in personal data processing. Such laws must require clear, informed, and prior consent before any collection or use of sensitive data. Moreover, they must mandate strong encryption standards, data minimization, and privacy-by-design principles for developers and technology providers.
- Corporate Accountability and Transparency: technology companies and data controllers must be held legally accountable for the misuse or unauthorized transfer of user data. There must be enforceable obligations to disclose data practices transparently and to provide remedies to users in case of violations. Fines, sanctions, or suspension of operations should apply to entities that breach these responsibilities. Furthermore, companies should be required to demonstrate innovation in the development of tools and technologies that enhance user privacy(El-Sadiq, 2023, p. 900).
- Cross-border Data Governance and International Cooperation: Given that AI applications and associated data flows often transcend national boundaries, cooperation among governments, international organizations, and regulatory bodies is crucial. Harmonized standards—such as those in the EU’s General Data Protection Regulation (GDPR)—can serve as reference models for ensuring data sovereignty and cross-border protection of digital rights.
- Independent Oversight Mechanisms: Independent supervisory authorities must be empowered with the legal mandate, technical capacity, and institutional independence to monitor AI-related privacy violations, investigate breaches, and enforce data protection laws effectively(El-Sharif, 2021, p. 56).



2.2.2- Ethics of Using Artificial Intelligence Tools:

Artificial intelligence, though a product of human invention, is not ethically neutral. Its outcomes are heavily shaped by the values, biases, and choices embedded in its training data and system design. Therefore, ethical considerations must be deeply integrated into every stage of AI development—from data selection and algorithm design to deployment and real-world application(Saoud, 2023, p. 10).

Ethical frameworks serve not only to mitigate harm, but also to enhance trust in AI systems and promote their use for the social good. The following principles constitute the ethical foundation for responsible AI use:

- A- Integrity and Fairness: Developers and users of AI systems must take all necessary steps to prevent and mitigate bias, discrimination, and profiling in data and algorithms. Historical data often reflect systemic inequalities; uncorrected, these are reproduced and amplified by AI. Therefore, fairness audits and algorithmic impact assessments should be mandated, especially in high-risk sectors such as healthcare, finance, recruitment, and law enforcement.
- B- Privacy and Security: AI systems must be secure by design and compliant with data protection regulations. This includes implementing cyber security safeguards, access controls, auditable logs, and real-time monitoring to prevent unauthorized data breaches. Importantly, systems should offer user-controllable settings that allow individuals to manage the scope of data collection and processing((SDAIA), 2023, p. 12)
- C- Human-centricity: The principle of humanity dignity requires that AI be used in a just, transparent, and accountable manner, guided by human rights and cultural values. AI must be designed to enhance—not undermine—human well-being, autonomy, and agency. Systems should be explainable, interpretable, and reversible, especially in high-stakes contexts.
- D- Social and Environmental Benefit: AI should be directed toward advancing social justice and environmental sustainability. It must not accelerate existing harms or deepen inequalities. Instead, it should contribute to solving pressing societal challenges such as climate change, education access,

healthcare delivery, and public sector efficiency. Ethical AI governance must explicitly align with the UN Sustainable Development Goals (SDGs).

- E- Accountability and Responsibility: The principle of accountability requires that developers, designers, and users of AI systems bear ethical responsibility for foreseeable harms. Human oversight, good governance, and clear lines of liability must be established across the AI lifecycle. Stakeholders must be identifiable and reachable, ensuring that redress mechanisms are available to those harmed by AI decisions or operations. Additionally, transparency in system design and decision logic is essential to uphold public trust((SDAIA), 2023, p. 1)

Conclusion:

In conclusion, this study highlights that the widespread integration of artificial intelligence applications into daily life and their use across diverse domains have had a direct and increasing impact on individuals' right to digital privacy. This impact is primarily reflected in the collection and reuse of personal data and information for purposes beyond the individual's knowledge or consent. If left unregulated, the trajectory suggests that in the near future, individuals may lose any meaningful control over their personal privacy-particularly in light of mounting warnings calling for restrictions on AI technologies that violate human rights.

Accordingly, the unmonitored and unregulated use of artificial intelligence represents a significant threat to personal privacy. It facilitates the misuse of sensitive data, which could be exploited in the commission of crimes or lead to the emergence of autonomous entities that potentially displace human agency in sensitive decision-making domains.

Based on the analytical findings of this study, the following key conclusions were reached:

- The right to digital privacy is fundamentally the individual's right to protect their personal data and information exchanged over the internet, including images, videos, identifying features, and even behavioral data such as preferences, interests, and online patterns.
- The Algerian legislator, like many others globally, has addressed the right to digital privacy through a range of legal



instruments, including the Constitution, the Penal Code, and laws related to the prevention and punishment of information and communication technology-related crimes. These frameworks collectively aim to secure and protect this right from infringement.

- Artificial intelligence possesses the capacity to infringe upon digital privacy through the tools and devices it powers-tools that serve individuals' needs on one hand while simultaneously extracting and processing their personal data for unrelated or potentially harmful purposes on the other.
- The intensification of AI-related risks has led to a wave of proposals and policy initiatives, both at the individual and institutional levels, as well as among state actors. These initiatives are designed to enforce protection mechanisms for the right to digital privacy in the face of AI-driven threats.

Recommendations

Based on the findings of this study, several strategic and legal recommendations are proposed to strengthen the protection of digital privacy rights in the Algerian context:

- The Algerian state must reinforce its role in strengthening regulatory oversight and legal controls over violations of digital privacy rights, including the enactment of a specific legislative framework on artificial intelligence, addressing the associated risks and laying out clear regulations for its use and boundaries.
- The state must undertake robust legal measures to safeguard the rights of individuals, ensuring the integrity and security of personal data across all technological platforms.
- Public awareness must be raised regarding the dangers of sharing personal information whether on social media or digital platforms-to reduce the risk of unlawful data collection, profiling, and exploitation.

These recommendations underscore the urgent need to establish a balanced regulatory ecosystem-one that supports technological innovation while upholding fundamental rights. As AI continues to reshape the digital landscape, the preservation of human dignity and privacy must remain at the forefront of any legislative or technological development.

References:

1- Books

- Giakoumopoulos & Christos, B. G. (2018). *Handbook on European Data Protection Law*. Luxembourg: European Union Agency for Fundamental Rights and Council of Europe. Luxembourg.
- Janane, Al-Arabi. (2010). *Processing of Personal Data: Legal Protection in Moroccan and Comparative Legislation*. Al-Matba'awa Al-Waraqa Al-Qanuniya. Marrakesh.
- Osama. Fayed. (2008). *Criminal Protection of Private Life and Information Banks: A Comparative Study in French and American Civil Law According to the Latest Legislative Amendments*. Dar Al-Nahda Al-Arabiya. Egypt.

2- Master's Thesis :

- Al-Shamsi, R. G. (2022). *Protection of Digital Privacy in Artificial Intelligence Applications: A Comparative Analytical Study (Master's Thesis)*. United Arab Emirates University.

3- Articles :

- Al-Ashqar, A. (2025). Digital Privacy in the Age of Artificial Intelligence: A Reading of Jordanian and Palestinian Legislation. *Al-Quds Open University Journal for Human and Social Research*, 07(66).8.
- Belassel. Bint Nabi Yasmine. (2021). The Right to Digital Privacy. *Journal of Future Legal and Political Studies*, 05(01).
- Akakpo, A., & Akwasi Gyasi, E. (2025). Artificial intelligence and the future of information Privacy: Expert Viewpoint. *Journal of Global Information Management*, 33(01). 1.
- Chinmay. (2025). Privacy in the age of artificial intelligence. *NUJS Journal of regulatory studies*, 09(04).81.
- Dalila, M., & Wali, N. (2024). Risks of Artificial Intelligence to Digital Privacy and Protection Mechanisms. *Journal of Legal and Social Sciences*, 9(3), 822.
- El-Sadiq, A. R.-S. (2023). The Impact of Artificial Intelligence on Values and Human Rights. *Benha Journal for Human Sciences*, 04(02).
- El-Sharif, M. A. (2021). Protection of Personal Data in International Arab Law. *Journal of Economic and Social Research, Algeria*, 37(02).56.
- Khdouja, Dahbi. (2017). The Right to Privacy in Confrontation with Cyber-Attacks: A Comparative Study. *Journal of the Researcher Professor for Legal and Political Studies*, 01(08), 148.
- palevic, Z., & Vicentijevic, K. (2022). GDPR and challenges of personal DATA protection. *The European Journal of Applied Economics*, 19(01).56.
- Sheibani, A., & Ben Salem, W. (2023). The Right to Information Privacy in Light of Artificial Intelligence. *Journal of Legal and Economic Studies*, 06(02), 462.
- Saghai, M., & Malika Madhkour, M. (2024). Artificial Intelligence and the Privacy Problem. *Rawafid Journal*, 08(02). 526.



- Saoud, W. (2023). Artificial Intelligence and the Challenges of Ethical Practice. Nama' Journal for Economy and Trade, 07(02). 10.
- Tiwari, Rajan. (2024). Digital Privacy and data protection in the age of surveillance. international journal of law, 04(02), P195.

4- Site web:

- Hulin, A. S. (2023, 04 25). Artificial Intelligence Data Sharing and Human Rights. Récupérés sur University of Sherbrooke: <https://www.usherbooke.ca/actualites/nouvelles/dztails/50160>

5- Reports:

- (SDAIA). (2023). *Principles of AI Ethics*. First Edition. Saudi Data and Artificial Intelligence Authority. Saudi Arabian.

6- LegalText (Law/Decree...)

- Algeria. (1963). Constitution of 1963. Official Gazette (64).
- Algeria. (1976). Ordinance 76/97 concerning the Constitution of the People's Democratic Republic of Algeria. Official Gazette.
- Algeria. (1996) Decree No. 96/438. Official Gazette(76).
- Algeria. (2020) Presidential Decree 20/442. Official Gazette(82).
- Algeria. (2004). L. N 04/15 containing the Penal Code. Official Gazette No(71).
- Algeria. (2009). L. N 09/04containing the special rules for the prevention and combating of crimes related to information and communication technologies. Official Gazette(47).
- Algeria. (2018). L. N.18/07 concerning the Protection of Natural Persons in the Processing of Personal Data. Official Gazette (34).