

Artificial Intelligence and the Right to the Protection of Private Life: A Formidable Challenge

DJAFOUR Islam

Associate Professor (Class A).

Faculty of Law and Political Sciences , Mouloud Mammeri University -Tizi-ouzou Algeria

E-mail: islam.djafour@ummto.dz

Received: 13/02/2026 ; Accepted: 05/08/2026 ; Published: 06/09/2026

Abstract:

Artificial intelligence (AI) can both benefit individuals and threaten their rights. Its impact largely depends on the purposes for which it is used. This dual nature highlights the role of law in addressing the challenges posed by artificial intelligence technologies in an increasingly borderless world.

Keywords: Artificial Intelligence (AI); Private Life; Personal Data; Precautionary Principle; Freedom of Innovation.

INTRODUCTION

Individuals today live in a risk-laden digital environment that threatens their fundamental rights. In recent years, this reality has been increasingly shaped by artificial intelligence (AI). In this environment, individuals face challenges that did not previously exist.

The role of law is to keep pace with developments in society while ensuring the protection of recognized human rights. Against this background, the law has sought to address the challenges created by artificial intelligence. Developments in this field have placed private life under increasing threat, as privacy is no longer under the exclusive control of the individual concerned. This is attributable to the indiscriminate use of personal data and to differences in the concept of private life arising from various subjective and objective factors.

AI applications reveal a complex relationship between artificial intelligence and private life. They have also narrowed the scope of private life. To prevent its further erosion, the existing situation must be regulated by law. This raises the question of how the right to private life can be protected against the risks posed by AI technologies.

Section One: Conceptual Approach to Artificial Intelligence (AI)

The historical roots of AI can be traced to mathematics in ancient civilizations before its evolution into its contemporary form. Its use has become widespread in society despite the ambiguity surrounding its legal nature (Subsection One). Given the risks associated with AI, the precautionary principle and the need to balance innovation with legal protection must also be taken into account (Subsection Two).

Subsection One: The Evolution of Artificial Intelligence and the Ambiguity of Its Legal Nature

AI technologies have developed rapidly in recent years, requiring law to keep pace with and accommodate these developments. However, law has not been able to do so fully because the legal nature of AI has not yet been precisely determined.

First: Artificial Intelligence (AI) as a Modern Tool with Ancient Historical Roots:

AI may appear to be a modern field, yet its intellectual foundations can be traced back to antiquity. In ancient Greece, the mathematician Euclid studied “algorithms,” also referred to as “programming code,” on which AI technology depends. AI therefore has deep roots in mathematics, although the modern concept emerged much later.¹

A variety of experiments laid the foundations of AI. In the thirteenth century, Ramon Llull created a machine known as the “Great Art” to determine whether a proposition was valid. In the seventeenth and eighteenth centuries, Descartes and Vaucanson developed machines known as “automata” that imitated the human form. Although these experiments were early precursors, modern AI is closely associated with computer science.

A major turning point occurred during the Second World War with the design of the first “Mark I” computer. The theoretical foundations of the modern concept of AI were then established in 1950, while the term “AI” was coined in 1956. Its modern development is closely associated with Alan Turing, who published the research paper “Computing Machinery and Intelligence”.²

One strand of scholarship defines AI as the scientific and technical field encompassing methods, theories, and techniques aimed at creating machines capable of simulating human intelligence.³ Another describes it as a science and technology grounded in a number of disciplines, including computer science, mathematics, biology, philosophy, and engineering, and directed toward developing computer functions that emulate human intelligence.⁴ Other scholars view AI as large-scale information assets characterized by high velocity, variety, and cost, requiring innovative forms of information processing and enhanced insight to support appropriate decision-making.⁵

The European Union has defined AI systems as software developed using one or more techniques and approaches that can achieve a given set of human-defined objectives or generate outputs such as content, predictions, recommendations, or decisions that influence the environments with which they interact.⁶ At an abstract and simplified level, an AI system can be described through three principal capabilities: perception and reasoning, decision-making, and execution. This description is sufficient to introduce and understand most of the technologies on which such systems are based.⁷

Second: The Legal Nature of Artificial Intelligence (AI):

The rapid development of AI has generated extensive legal debate concerning its legal nature and status within contemporary legislative systems. This debate has intensified because of AI’s advanced capacities for analysis, processing, and quasi-autonomous decision-making. Determining its legal nature is particularly important because it affects the scope of legal liability and the associated

¹ Clémentine Pouzet, *Les modes de régulation de l’intelligence artificielle par le droit européen*, Master 2 thesis, Droit européen et droits de l’homme, Université Jean Moulin Lyon 3, 2020, p. 10.

² Clémentine Pouzet, *op. cit.*, p. 11.

³ Bo-hu Li, Bao-cun Hou, Wen-tao Yu, Xiao-bing Lu, and Chun-wei Yang, “Applications of artificial intelligence in intelligent manufacturing: a review,” *Frontiers of Information Technology and Electronic Engineering*, Vol. 18, No. 1, 2017, p. 89.

⁴ Mohamed Fathi Mohamed Ibrahim, “Legislative Regulation of Artificial Intelligence Applications,” *Journal of Legal and Economic Research*, No. 71, September 2022, p. 1031.

⁵ Gabriele Buchholtz, *Artificial Intelligence and Legal Tech: Challenges to the Rule of Law*, Springer Nature Switzerland AG, 2020, 2018, p. 177.

⁶ European Commission High-Level Expert Group on Artificial Intelligence, *A Definition of AI: Main Capabilities and Scientific Disciplines*, Brussels, 18 December 2018, p. 1, available at: ec.europa.eu/futurium/en/system/files/ged/ai_helg_definition_of_ai_18-december_1.pdf

⁷ *Ibid.*, p. 5.

rights and obligations. This requires consideration of whether AI should be treated merely as a technical tool under human control or as a distinct legal entity capable of producing certain legal effects independently.

In this context, several doctrinal approaches have sought to define the legal nature of AI. The first regards AI as an advanced technical tool that neither acquires legal personality nor possesses legal independence. Under this view, AI remains a means of production or operation comparable to traditional machinery. The legal consequences arising from its use are therefore attributed to the natural or legal person who designed, programmed, operated, or supervised it. Proponents of this approach argue that traditional legal rules, particularly those governing tort and vicarious liability, are sufficient to address harm arising from the use of AI systems. Accordingly, there is no need to create a new legal status or recognize an independent legal personality for AI.⁸

Moreover, recognizing AI as a legal entity would ordinarily require registration and the attribution of characteristics such as a name, domicile, and nationality. A legal entity acts through the persons who represent it. AI, however, cannot act as a representative of human beings because it lacks consciousness and legal capacity.⁹

A study commissioned by the European Parliament advanced the view that AI could constitute a new and distinct legal entity known as “electronic personality,” analogous to legal personality. This view is particularly relevant because legal capacity derives from the law itself. Accordingly, the acts of such an entity would require detailed and appropriate legislation.

The European Parliament proposed creating a special legal personality for robots, particularly the most advanced and autonomous ones. Under this approach, they could be treated as electronic persons responsible for harm caused to third parties and potentially subject to a dedicated insurance regime. A practical example cited in support of this proposal is the partial recognition of electronic personality for robots in the State of Nevada, United States. There, robots have been granted certain powers associated with legal persons, made subject to registration in a special register, and allocated a financial patrimony for insurance purposes to cover harm caused to third parties.¹⁰

In considering the ethical implications of AI, legal personality should not be justified solely by reference to AI’s intrinsic characteristics. A future basis for such recognition may instead arise when technological development makes AI operations impossible to predict. AI systems whose actions remain predictable can be governed by detailed liability rules. As AI becomes more autonomous, the scope of the applicable liability framework may expand accordingly. Ultimately, such a framework may develop through the attribution of legal personality.¹¹

Subsection Two: Principles Governing the Use and Development of Artificial Intelligence (AI)

Law regulates all areas of life, including AI. Its use and development should therefore be governed by two fundamental legal principles: the precautionary principle and the principle of balance.

⁸ Hamdi Ahmed Saad Ahmed, "The Legal Nature of Artificial Intelligence," paper presented at the Fourth International Conference held at the Faculty of Sharia and Law in Tanta, entitled "The Sharia and Legal Characterization of Contemporary Developments and Its Impact on Achieving Societal Security," 11-12 August 2021, p. 248 et seq.

⁹ Salaheddine Neffad, "La nature juridique de l'Intelligence Artificielle," *Revue des contentieux d'affaires*, No. 98, 2025, p. 334.

¹⁰ Rabai Ibrahim, "The Legal Nature of Artificial Intelligence," *Al-Ustadh Al-Bahith Journal for Legal and Political Studies*, Vol. 10, No. 1, June 2025, p. 550.

¹¹ Karolina Ziemianin, "Civil legal personality of artificial intelligence: Future or utopia," *Internet Policy Review*, Vol. 10, No. 2, 2021, p. 10.

First - The Precautionary Principle:

Major internet companies that employ AI technologies have become dominant market actors, exercising substantial control through monopolistic practices. More seriously, they possess vast repositories of users' personal data. This situation raises two distinct concerns: how such data are used and the political implications of platforms' capacity to influence individuals' beliefs and awareness. AI may also affect individuals' futures and life choices through identification, classification, and judgment by opaque algorithms. In this context, delaying the establishment of regulatory frameworks for AI would serve primarily the interests of these major companies, without necessarily promoting greater innovation or fair competition. Instead, it could pave the way for the dominance of technology giants to such an extent that they can shape human behavior and influence individual choices.¹²

Against this background, the precautionary principle assumes particular importance in AI regulation. Under this principle, public authorities may intervene when the occurrence of harm is uncertain but its potential effects are serious and irreversible. Such intervention allows authorities to assess risks and adopt appropriate temporary measures. Potential harm may have severe and irreversible consequences for human rights even when its occurrence remains uncertain. Incorporating the precautionary principle into AI regulation can therefore enable public authorities to prevent or mitigate ethical and social risks.

The multidimensional nature of AI technologies has generated a range of challenges requiring regulatory oversight. The opacity of algorithms raises fundamental issues of accountability and transparency because it can make it difficult to determine how decisions are reached. This creates a need for guidelines requiring algorithmic interpretability and explainability. The protection of fundamental rights is also a major concern, as AI technologies may infringe privacy and freedom of expression. Regulatory frameworks are therefore necessary to safeguard these rights. The risks associated with AI are not merely theoretical. They have tangible real-world implications, ranging from biased decision-making to catastrophic large-scale failures. Regulatory oversight is therefore essential to assess and mitigate these risks. It should be supported by robust mechanisms for monitoring compliance and imposing appropriate sanctions for violations.¹³

The application of the precautionary principle depends on the absence of scientific certainty. This may concern either the lack of scientific evidence regarding the risks posed to third parties by AI technologies or the absence of an established causal relationship between the activity and the resulting harm. In such circumstances, proactive measures should be adopted to reduce potential risks. The precautionary principle is therefore particularly important where scientific certainty concerning AI technologies is lacking. Even when risks remain unproven and merely potential, such uncertainty may justify the adoption of necessary measures to address unpredictable errors.¹⁴

¹² Adriana Ricardo da Costa Schier, Cristina Borges Ribad Maksym, and Vitoria Dionisio Mota, "The urgency of regulating and promoting artificial intelligence in the light of precautionary principle and sustainable development," *International Journal of Digital Law*, No. 3, 2021, p. 141.

¹³ Nathalie de Marcellis-Warin, Frédéric Marty, and Thierry Warin, "Réglementer l'intelligence artificielle sur la base des risques: Perspectives économiques et éthiques," *Revue économique*, Vol. 76, No. 1, January 2025, p. 102.

¹⁴ Idabir Yamina and Kessi Zahira, "The Precautionary Principle: A New Approach to Liability Arising from Damage Caused by Artificial Intelligence Systems," *Al-Ijtihad Journal for Legal and Economic Studies*, Vol. 14, No. 1, 2025, p. 251.

Second - The Principle of Balancing Freedom of Innovation and Legal Protection:

This principle is also known as the principle of proportionality. It originated in German administrative law and gradually developed into a fundamental principle of public law, expanding in both substantive scope and geographical application.

This principle can also be understood through the concept of rationality. In law, rationality generally reflects moderation and appropriateness while rejecting excessive measures. This reflects the close relationship between rationality and proportionality. Balance, in this sense, serves to identify the boundary between what is permissible and what is prohibited.¹⁵

A further challenge is to ensure that legitimate scientific innovation is not unduly restricted as AI continues to develop globally. Regulation should not impose restrictions that obstruct technological progress. Instead, AI should be regulated through a careful balance between innovation and legal protection. Regulatory measures should not exceed what is strictly necessary to protect the international community from potential harm. This position has also been advanced in international scholarship, which maintains that restrictions on modern technologies should be reasonable, necessary, and justified.

Several researchers have proposed a practical model for applying this principle through the concept of a conditional treaty on AI. Such a treaty would not seek to prohibit the development of intelligent technologies altogether. Rather, it would establish technical criteria for distinguishing high-risk systems from those whose development may be permitted. Under this model, states would retain the freedom to innovate.¹⁶

Technology develops rapidly, whereas law is characterized by slow adaptation and updating, a disparity that has disrupted the balance between law and AI. To avoid the potential problems arising from this situation, legal professionals and legislators must deepen their engagement and collaborate in order to keep pace with modern developments. At the same time, technologists and innovators must be aware of legal rules and operate within their framework so that they can use their knowledge and skills in the service of humanity.¹⁷

All of this raises a fundamental question as to whether the loss of life caused by AI can be proportionate to a legitimate aim. Even where the development of AI pursues legitimate societal objectives, such as scientific research or national defense, it must be recognized that such objectives cannot under any circumstances be justified if unintended consequences result in humanity losing control over this technology and ultimately lead to its extinction. The inherent disproportionality of such an outcome reinforces the need to balance freedom of innovation with law.¹⁸

Clear rules have therefore become necessary to protect human rights without obstructing innovation. It is important to recognize that AI systems learn from existing data, which may contain biases arising during the design of opaque algorithms. This can make it difficult to identify the party

¹⁵ Antoine Guilmain, "Sur les traces du principe de proportionnalité: une esquisse généalogique," *Revue de droit de McGill*, Vol. 61, No. 1, 2015, pp. 114-115.

¹⁶ Kim Kaivanto, "The Precautionary Principle and the Innovation Principle: Incompatible Guides for AI Innovation Governance?," *arXiv preprint*, 1 May 2025, pp. 1-12, available at: <https://arxiv.org/abs/2505.02846>

¹⁷ Donna Ibrahim Halal, *Artificial Intelligence: Defining Criminal Law*, Dar Bilal, Beirut, 2022, p. 250.

¹⁸ Bryan Druzin, Anatole Boute, and Michael Ramsden, "Confronting Catastrophic Risk: The International Obligation to Regulate Artificial Intelligence," *Michigan Journal of International Law*, Vol. 46, No. 2, 2025, p. 209.

responsible for biased or discriminatory decisions. Legal frameworks therefore seek to regulate the use of AI in a manner that safeguards fundamental rights and democratic values.¹⁹

Section Two: The Difficulty of Protecting Private Life in the Digital World

AI has created a reality that was previously unknown, particularly in relation to the right to privacy, because of the close interrelationship between private life and AI (Subsection One). The protection of private life, however, encounters complex legal obstacles (Subsection Two).

Subsection One: The Necessity of Protecting Private Life

Individuals possess a range of rights relating to their privacy that must be protected in both the physical and digital worlds.

First - The Relationship Between Private Life and Artificial Intelligence (AI):

Private life is a flexible and evolving concept with no fixed boundaries. Its scope varies not only across societies and states but also among individuals, depending on factors such as age and the level of protection considered appropriate for different aspects of personal life. This complexity also reflects differences among societies in balancing privacy against competing values. The scope of the right to private life therefore depends on a society's conception of individual life. It is not fixed but shaped by the social circumstances in which individuals live.²⁰

The relationship between AI and the right to private life may be understood as an interconnected legal relationship with both positive and negative dimensions. AI technologies can collect, process, and exploit vast quantities of personal data, thereby placing individual privacy at risk.

Surveillance and monitoring are among the most significant privacy concerns associated with AI. Advanced software can learn from vast quantities of information, including individuals' communications, internet browsing records, actions, and conduct. Such practices may constitute an infringement of the right to private life.²¹

Data extraction conflicts with several privacy principles recognized by law and reflected in professional codes of conduct. These include transparency in the collection and use of personal data, informing individuals about privacy policies, and disclosing the third parties that receive their data. They also require appropriate safeguards to ensure data protection. Individuals should have the right to access, correct, and delete their data. Personal data should be retained only for as long as necessary to achieve the stated purposes, then securely disposed of and protected against unauthorized access. In practice, however, third parties may collect data without notice, consent, adequate safeguards, or a specified purpose. Such practices show little meaningful regard for individuals' private lives.²²

The need to regulate the automated processing of personal data in order to protect the right to private life is therefore evident. The French legislature was among the first to address this issue through the Law of 6 January 1978, which established fundamental principles governing this field.

The rapid development of AI technologies requires existing legislation to be reconsidered, as the issues they raise differ significantly from those posed by traditional algorithms. Traditional algorithms consisted of sequences of instructions designed to produce predetermined results from given inputs. By contrast, machine learning represents a qualitative shift because it moves beyond

¹⁹ Hicham El Yousfi and Sanaa Benabdallaoui, "Entre Innovations et Régulation: Les Défis Juridiques de l'Intelligence Artificielle," *Revue du Contrôle de la Comptabilité et de l'Audit*, Vol. 9, No. 3, 2025, p. 216.

²⁰ Ahmed Ibrahim Ahmed Attia Khalil, "Legal Protection of Private Life in the Face of Artificial Intelligence Technologies," *The Legal Journal*, No. 7, 2024, p. 2642.

²¹ M. D. Danish Raza, B. Nagendra Prasad, Naziya Fathima K., and J. Ranjani, "Artificial Intelligence and Right to Privacy," *International Journal of Innovative Research in Technology*, Vol. 11, No. 11, April 2025, p. 5645.

²² Daniel J. Solove, "Artificial Intelligence and Privacy," *Florida Law Review*, January 2025, p. 24.

this deterministic model and can identify the processes required to reach a result. This capacity for self-learning increases the algorithm's independence from its programmer. Rather than specifying the sequence of operations followed by a traditional algorithm, the programmer now trains the system.²³

Second - Personal Data Processing and Use Must Be Subject to the General Principles of Law:

Under general principles of law, relationships between persons, regardless of their nature, are based on consent. The same principle should apply to the processing and use of personal data through AI technologies.

Consent must be unambiguous, clear, and not open to interpretation. It may neither be presumed nor inferred merely from the data subject's silence or failure to act. Consent is explicit when it involves a positive expression of will that clearly conveys the data subject's intention and can be understood by the data controller. The Court of Justice of the European Union has affirmed this position, holding that silence or inactivity does not constitute consent and requiring a positive act or actual conduct by the data subject. Accordingly, any indication or statement, whether oral, written, or electronic, may constitute unambiguous consent, provided that the options have not been preselected and reflect a conscious and informed choice.²⁴

In addition, personal information must be collected for specified, explicit, and legitimate purposes and may not be processed in a manner incompatible with those purposes, including where processing is undertaken in the public interest or for scientific research.²⁵

The data being processed must be accurate and consistent with the purposes for which the processing is carried out, particularly where personal data are used to make decisions or draw conclusions concerning a data subject. This helps ensure that individuals are not discriminated against on the basis of sex, opinion, religion, or any other factor that may result in discrimination.

Personal data should be processed for the purpose of protecting legitimate interests, namely interests protected by law, such as safeguarding human rights and fundamental freedoms. An exception may be made for the processing of personal data for training purposes and the design of a computational model, provided that robust security and technical measures are adopted.²⁶

Law should be interpreted in a manner that gives priority to protecting the right to private life despite the importance of promoting innovation and commercial interests. These objectives should under no circumstances be pursued at the expense of fundamental rights, foremost among them the right to private life. Fundamental rights and commercial activities should therefore not be placed on an equal footing.

AI raises a range of challenges relating to the protection of private life. Existing laws, which focus on the collection, use, and disclosure of personal information, suffer from several shortcomings. As a result, the concept of personal data can be said to have overshadowed both the information-processing cycle and the protection of privacy in its broader sense. Most privacy concerns focus on

²³ Francis Donnat, "L'intelligence artificielle: un danger pour la vie privée?," *Pouvoirs*, Vol. 3, No. 170, 2019, p. 95.

²⁴ Claude Eliante Mbome, "Consentement et protection des données à caractère personnel: Les frontières du droit," *Revue Juridique et Politique en Afrique*, Vol. 2, No. 5, 2025, pp. 128-129.

²⁵ Nello Cristianini, "On the current paradigm in artificial intelligence," *The European Journal on Artificial Intelligence*, Vol. 27, No. 1, February 2014, pp. 37-43.

²⁶ Wafaa Helmy El-Saeed, "Artificial Intelligence Technology and Personal Data Protection," *Journal of Sharia and Law*, No. 43, April 2024, p. 1436.

individuals' personal information rather than privacy as a whole, thereby narrowing the scope of private life.²⁷

Subsection Two: Legal Obstacles to the Protection of Private Life

Law recognizes the individual's right to the protection of private life. However, complex legal obstacles make the effectiveness of that protection uncertain.

First: The Absence of a Unified and Precise International Legal Characterization of Personal Data:

The United Nations (UN) recognized the danger of leaving the regulation of AI to the individual initiatives of states or major technology companies. It therefore launched initiatives aimed at achieving international consensus on minimum legal safeguards. These efforts culminated in 2024 with the adoption of the "Pact for the Future" through General Assembly Resolution No. 79/1²⁸, which affirmed the need to address responsibly the potential risks of technology that may adversely affect the enjoyment of human rights.²⁹

The approach adopted by the UN undoubtedly extends to the right to the protection of private life. Nevertheless, the absence of a unified legal characterization of personal data remains a principal obstacle to the effective protection of that right. The international community still lacks a binding definition establishing the legal nature of personal data and determining whether they should be regarded as a human right or an economic interest. This uncertainty has produced divergence among national, regional, and international legal frameworks.

These differing approaches have resulted in significant variation in the legal characterization of personal data across legal instruments. The European Union treats the protection of personal data as an inalienable fundamental right, requires the individual's explicit consent to data processing, and imposes strict restrictions on transfers to countries that do not provide adequate protection.³⁰ By contrast, the United States follows a sectoral approach to the protection of personal data privacy. It has no comprehensive legislation or general principles guaranteeing the privacy and protection of personal data; at the federal level, legislation primarily protects data within specific sectoral contexts.³¹ This reflects a broader difference in legal approach: the EU treats data protection as a fundamental right, whereas the United States largely approaches it through sector-specific regulation.³²

European Convention No. 108 of 1981 was among the first international legal instruments to address digital privacy and seeks to ensure a balance between the free cross-border flow of data and the protection of individuals' private life.³³ Its principal purpose is to secure respect for the rights and fundamental freedoms of every natural person, particularly the right to privacy, with regard to the

²⁷ Noémie Blouin, La protection du droit à la vie privée à l'ère de l'intelligence artificielle, Master's thesis in Information Technology Law, Université de Montréal, Faculty of Law, 2023, pp. 109-110.

²⁸ United Nations, Pact for the Future, General Assembly Resolution No. 79/1, adopted at the 79th session, agenda item 123, 22 September 2024.

²⁹ See paragraph 50 of Resolution No. 79/1.

³⁰ Jean-Philippe Walter, "Le Conseil de l'Europe et la protection des données," *Annuaire international de justice constitutionnelle*, No. 35-2019, 2020, pp. 599-601.

³¹ Shawn Marie Boyne, "Data Protection in the United States," *The American Journal of Comparative Law*, Vol. 66, July 2018, p. 299.

³² James B. Rule, "La protection des données personnelles aux Etats-Unis: La réaction à la directive Européenne," *Revue française d'administration publique*, No. 89, January-March 1999, pp. 95-104.

³³ Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, European Treaty Series No. 108, available at: rm.coe.int/1680078b39

automated processing of personal data concerning that person.³⁴ However, it neither determined the legal nature of such data nor provided a precise definition of them.

International conventions have likewise failed to establish a unified concept of personal data. The 2001 Budapest Convention on Cybercrime did not provide a specific and clear definition. Instead, it focused on the criminalization of cyber conduct and on measures, including criminal-law provisions, that states undertake to adopt jointly to combat cybercrime, particularly by preventing offenses against the confidentiality and integrity of data.³⁵

Through Resolution No. 68/167 on the right to privacy in the digital age³⁶, the UN General Assembly affirmed the right of all individuals to the protection of their private life, the prohibition of arbitrary interference with their privacy, and their right to legal protection.³⁷ It also affirmed that the rights enjoyed by individuals in the physical world must likewise be protected in the digital world, including the right to privacy.³⁸ Mere access to or covert surveillance of individuals' private data interferes with their right to privacy.³⁹ Despite the considerable importance of the Resolution in recognizing the protection of private life as a right, it did not precisely determine the legal nature of personal data.

National laws differ in their characterization of personal data, and legislation governing the protection of such data likewise varies. This further complicates the implementation of uniform global policies for protecting private life, particularly because some states lack robust legislation, making effective cross-border protection difficult to guarantee.⁴⁰

Second: The Conflict Between the Right to the Protection of Private Life and the Right of Access to Information:

The entitlement to safeguard one's private life encounters numerous obstacles, as the safeguarding of personal data might clash with the right to information access, acknowledged at both constitutional and international tiers. In a general context, freedom of information pertains to the entitlement to access information possessed by governmental entities upon request.⁴¹

Article 19 of the Universal Declaration of Human Rights acknowledges the entitlement to freedom of opinion and expression, encompassing the liberty to pursue, obtain, and disseminate information and ideas⁽⁴²⁾. Article 10 of the European Convention on Human Rights similarly acknowledges the right to freedom of expression, encompassing the liberty to develop opinions and to access and disseminate information without interference from governmental authorities.

Moreover, Article 19 of the International Covenant on Civil and Political Rights stipulates that the right to freedom of expression encompasses the liberty to pursue, obtain, and disseminate

³⁴ See Article 1 of the Convention.

³⁵ Roberto Angrisani, "Données personnelles et surveillance massives: quelle protection face aux ingérences des autorités publiques?," *Revue québécoise de droit international*, Special Issue, 2020, p. 116.

³⁶ United Nations, The Right to Privacy in the Digital Age, General Assembly Resolution No. 68/167, adopted at the 68th session, agenda item 69(b), 70th plenary meeting, 18 December 2013.

³⁷ See paragraph 1 of Resolution No. 68/167.

³⁸ See paragraph 3 of Resolution No. 68/167.

³⁹ Falahi Soumia and Meziane Mohamed El Amine, "The Right to Privacy in Light of the Development of Artificial Intelligence Technologies," *Journal of Human Rights and Public Freedoms*, Vol. 10, No. 2, 2025, p. 353.

⁴⁰ Rahmani Imane and Lattar Zine El Abidine, "Protection of Personal Data in the Digital Age," *Tabna Journal for Academic Scientific Studies*, Vol. 8, No. 2, 2025, p. 415.

⁴¹ Zaabat Taher, *The Citizen's Right to Access Information*, Master's thesis, Kasdi Merbah University Ouargla, Faculty of Law, 2014, p. 7.

⁴² Pierre Trudel, "Réflexion pour une approche critique de la notion de droit à l'information en droit international," *Les Cahiers de droit*, Vol. 23, No. 4, 1982, p. 853.

information and ideas of every nature without regard to borders.⁴³ Article 13 of the 1969 American Convention on Human Rights acknowledges the entitlement of every individual to freedom of thought and speech, encompassing the associated rights to pursue, obtain, and disseminate information and ideas of various forms. Article 9 of the 1981 African Charter on Human and Peoples' Rights acknowledges the entitlement of every person to access information.⁴⁴

As a result, conflicts have emerged between the right to privacy and the right to information due to the utilization of sophisticated technologies for data collection, whether by governmental entities or private individuals. These tensions encompass the state's authority to acquire information regarding individuals' matters in connection with the right to personal privacy, alongside the clash between individuals' entitlement to private life and the liberty to disseminate information.

The entitlement to safeguard personal information may also clash with the doctrine of transparent justice. Implementing that approach might necessitate the judiciary to restrict the safeguarding of personal information. The dissemination of legal rulings may facilitate the spread of information on individuals' safety, thereby jeopardizing the safeguarding of personal privacy.

Attaining equilibrium between the right to privacy and the right to information necessitates an acceptable benchmark, as privacy inherently restricts access to information.⁴⁵

CONCLUSION

Law has been slow to regulate the development and use of AI, weakening the protection afforded to the right to private life. This delay is attributable to several factors, foremost among them the rapid pace of AI development and innovation.

Differences among national, regional, and international standards governing AI have also prevented agreement on what constitutes lawful and unlawful conduct. This is particularly evident in relation to the use of personal data, the protection of their confidentiality, and the prohibition of their circulation without prior authorization.

Effective enforcement mechanisms are essential to ensuring respect for private life. The judiciary must therefore fulfill its role when individuals' privacy is violated in a world without borders. Otherwise, the limited safeguards currently in place will fail to achieve the purpose for which they were legally established.

⁴³ Hafsa Koubibi, "The Right of Access to Information: A Comparative Legal Study," *Journal of Communication and Journalism*, Vol. 8, No. 1, 2021, p. 66.

⁴⁴ Aaron Olaniyi Salau, "The right of access to information and national security in the African regional human rights system," *African Human Rights Law Journal*, Vol. 17, 2017, p. 373.

⁴⁵ Jendali Warida, "Protection of Personal Data under Algerian Legislation and International Instruments: Between Guarantees and Challenges," *Academic Journal of Legal and Political Research*, Vol. 6, No. 1, 2022, p. 1432 et seq.