

The Interconnection between Artificial Intelligence and the Right to Privacy

الترباط بين الذكاء الاصطناعي والحق في الخصوصية

Phd. Fayçal iglouli

*faculte of law and political sciences university of
Tizi-ouzou Globalization and National Law
Laboratory (Algeria)
Faycal.iglouli@ummto.dz*

**Received
Apr – 02 - 2026**

Pr. Elkahina irzil⁽¹⁾

*faculte of law and political sciences university of
Tizi-ouzou (Algeria)
Elkahina.irzil@ummto.dz*

**Accepted
Sep – 22 - 2026**

**Published
Oct – 31 - 2026**

Abstract:

Amid the technological and scientific revolution sweeping the global arena, various techniques and technologies have emerged that can only be described as representing unprecedented development across all social, economic, and even security levels. Among the techniques currently captivating attention and research is artificial intelligence technology, considered a highly prominent breakthrough due to its role in creating substitutes for humans in programming, research, and potentially even making crucial decisions in certain fields. These were originally human productions but have been transformed into machines called robots, programmed in ways unimaginable to the human mind. In this context, several issues have been raised, particularly from a legal perspective, concerning the impact of artificial intelligence on the course of operations and information it processes, and the dangers it poses to preserving their confidentiality and privacy, given the consequences arising from the software it contains in this regard.

key words: Artificial intelligence, Right to Privacy, law, Compatibility.

الملخص :

في خضم الثور التكنولوجية والعلمية التي تعرفها الساحة العالمية تم ظهور فنيات وتقنيات أقل ما يقال عنها أنها تمثل تطورا لا مثيل له على جميع الأصعدة الاجتماعية والاقتصادية وحتى الأمنية. ومن بين الفنيات التي تحظى حاليا بالانشغال والبحوث هي فنية الذكاء الاصطناعي باعتباره طفرة فنية عالية الظهور بالنظر إلى ما تعمل فيه في إيجاد بديل للإنسان في البرمجة والبحث وربما حتى اتخاذ القرارات الحاسمة في مجالات معينة بالأصل هي من إنتاج الإنسان لكن تم تحويلها إلى آلات تسمى بالبربوتات مبرمجة برمجة لا يتصورها العقل. في خضم ذلك أثيرت عدّة إشكالات خاصة من الناحية القانونية في مسألة تأثيرها على مسار الأعمال والمعلومات التي يسيرها الذكاء الاصطناعي وخطورتها عليها في مسألة الحفاظ على سرّيتها وخصوصيتها بحكم الآثار الناجمة عن البرمجيات التي يحتويها الذكاء الاصطناعي في هذا الأمر.

الكلمات المفتاحية: الذكاء الاصطناعي - الحق في الخصوصية - القانون - التناسب.

⁽¹⁾ Corresponding author: Pr. Elkahina irzil,

e-mail: naimairzil@yahoo.fr

Introduction:

Humanity is currently witnessing an unprecedented scientific and technological revolution that has transformed the methods and tools used across all sectors—whether social, economic, or security-related—by seeking solutions to the various challenges that might impede the flow of activities and interactions between societies.

This entails creating alternatives to physical interactions and replacing them with high-quality technical and technological processes. It involves developing machines and equipment—born of human ingenuity—to operate in place of the human being; essentially, it means finding a substitute for the physical human and replacing them with a "virtual human" in the form of machines that function and think on their behalf.

It involves creating a new technology—designed by humans to replace them—known as artificial intelligence, based on specific concepts and rules that follow a path aimed at achieving certain objectives, depending on the intended application.

In this regard it is appropriate to ask to what extent does the right to privacy constitute an objective limit restricting the right to use artificial intelligence?

To answer this question, it is necessary to clarify the relationship between artificial intelligence and the right to privacy (Section I), then highlight the impact of using artificial intelligence on the right to privacy (Section II).

Section I:

The Relationship between Artificial Intelligence and the Right to Privacy

Artificial intelligence is currently considered an important part of human life due to its numerous uses from which there can be no retreat. This expresses the position of this artificial intelligence in assisting humans in obtaining what they desire in terms of methods and tools for managing and controlling their affairs in diverse and varied fields.

Since this artificial intelligence has far-reaching dimensions and an unparalleled impact on people's lives, this raises the issue of its relationship with the right to privacy. Here we say that this relationship appears in considering artificial intelligence as a repository for various information specific to humans (A) and thus as a container for every human right to privacy (B).

A) Artificial Intelligence as a Source for Storing Privacy-Related Information:

The introduction of the idea of using artificial intelligence through devices and machines for the first time occurred in 1950 by Alan Turing, through operating machines and training them to control information and then make decisions independently¹. As for the term "artificial intelligence," it was coined by John McCarthy and Marvin Lee Minsky in 1956 through their lecture at Dartmouth².

However, the stabilization of its applications and characteristics began to manifest in the 1990s, the 2000s, and particularly in 2011 through the work of specialized agencies in this framework via their extensive activity in using artificial intelligence³. Efforts

focused on developing theories and algorithms allowing the machine or device to control information by having this machine learn neural simulation in the human body.

The concepts proposed for artificial intelligence by specialists and scholars vary, but they all agree on one meaning: considering artificial intelligence as a branch of computer science concerned with machines capable of solving types of problems to which humans resort using their intelligence⁴. That is, studying how to direct the computer to perform tasks that humans do better. These concepts also agree that artificial intelligence is the study and design of intelligent agents, where the intelligent agent comprehends a certain environment and takes actions to maximize its success in achieving its task or its team's task⁵.

According to these meanings, artificial intelligence is considered a valid repository for information, its use, and making decisions regarding it, which originates from the physical human. Thus, artificial intelligence serves as a substitute for the physical human - speaking of the robotic human in the form of a machine, device, or robot that senses and interacts with the environment intelligently, enabling it to operate in a wide range of fields including industry, medicine, and various services such as banks, insurance, communications, and others. That is, making the machine the one that plans, infers, communicates, and collaborates with humans and other machines.

In application, artificial intelligence includes the following:

- Containing a set of data: This is a collection of digital information expressing a set of facts and relationships in the physical and virtual world, where these facts are textual, audio, or visual. These data are the raw material provided to any computer system; they are analyzable and processable inputs. The proliferation of these data has been fueled by extensive internet use, the spread of digital media, and individuals sharing information via social media⁶.

In this context, these massive data have become in need of management, use, and employment through innovative techniques, including artificial intelligence as an added value via automated analysis to process them quickly without specialist intervention.

- Containing a set of algorithms: Algorithms are a set of rules defining how to solve a specific problem or perform a specific task, directed at managing the behavior of computers and robots in artificial intelligence.

Thus, algorithms form a means to analyze and process massive data, making their results clear, accurate, and confirmed. The more abundant the data, the more precise and organized the algorithmic processing. Hence, artificial intelligence's role emerges as a magnet for all data, considered two integrated factors.

B) Artificial Intelligence's ability to understand Privacy-Related Information:

Based on the above, we conclude the position of artificial intelligence in absorbing data linked to various stored information and then employing it in one way or another.

Artificial intelligence revolves around collecting and processing all information related to human privacy. This concerns information about a person's life, family, work,

and general surroundings. Meaning that privacy centers on preserving the confidentiality of information and data stored in databases across various digital platforms, which serve as sources for artificial intelligence uses and include personal information related to family, professional, financial transactions, and others.

We note here that the term "personal data" is legally defined in some legislations, including the Egyptian Law No. 151 of 2022 and the Algerian legislator under Law No. 18-07, considering it personal data relating to a specific natural person or one identifiable directly or indirectly by linking it to other data such as name, voice, image, digital identifier, and even psychological, health, economic, cultural, and social identity⁷.

The privacy of these data belonging to persons appears through sharing them with others - whether individuals or institutions - in the digital space, allowing them to become subjects of violation and theft from diverse sources when using artificial intelligence.

Based on this, information stored in the digital space has become a crucial matter requiring preservation of its confidentiality and thus consideration of its privacy. It must be processed by protecting it from violations that may affect it, through committing to the privacy of data recorded via the digital space without disclosing or encroaching upon it.

Therefore, storing data in the digital space is an issue requiring consideration when using artificial intelligence, as data collected by it demands security to avoid unauthorized access and thus breaching those data. Hence, transparency must be adopted, privacy respected, and data handled responsibly - meaning using ethical standards when employing information contained in artificial intelligence technology.

Based on this, we say that artificial intelligence is a means to collect data of various types, including privacies related to humans. However, using those data may pose a danger to their security due to illegitimate use. Accordingly, special security for those data must be provided through adopting a secure information system, especially if sensitive like personal information and conversation records.

According to the above data, persons have the right to preserve their private lives, and it is their right to prevent others from accessing their personal data without prior permission. The right to privacy in the digital space is an inseparable part of human private life, considered a fundamental right and freedom guaranteed by law.

Among artificial intelligence techniques that may violate the right to privacy, we mention ChatGPT technology, as it involves direct and indirect processing through posing questions without stipulating preservation of confidentiality for declared personal data⁸. If these data include trade or industrial secrets, they may be exploited by another market competitor. Personal data also form the backbone of artificial intelligence uses, sometimes employed as a means for advertising and promotion by institutions and companies to market products and services, such as telecommunications, banks, insurance, transport, and others.

Moreover, declaring such data by persons is sometimes a preliminary and mandatory procedure, like data required on social media sites, varying from one site to another, allowing those sites to retain them. This later enables feeding them via artificial

intelligence as fuel for the latter, as they are processed in terms of collection, recording, and storage using any electronic medium⁹.

Section II:

The Impact of using Artificial Intelligence on the Right to Privacy

Given the existing link between artificial intelligence and information/data privacy mentioned above, there are significant emerging effects that can be summarized as considering artificial intelligence a source of violation to the right to privacy (A) and thus the necessity to protect the right to privacy from artificial intelligence use (B).

A) Artificial Intelligence as a Source of Infringement on the Right to Privacy:

Since various data recorded in databases in the digital space enable using diverse artificial intelligence applications, conversely, this means those applications may threaten those personal data, hence considering them a source of violation to what is called the right to privacy.

The right to privacy means the right of various persons who recorded their information in the digital space to protect their information and data declared via various digital internet means from piracy and theft forms in the framework of data protection or personal information. Remembering that the right to privacy is constitutionally protected, inherent to the natural person as a general principle.

Privacy of information divides into two aspects:

- Information privacy: Includes rules governing collection and management of private data like identity card information, financial data, medical and government records, requiring protection under personal data protection framework.
- Communications privacy: Concerns correspondence and communications via phone, email, social media sites, and others.
- Bodily privacy: That is, information linked to individuals' bodies like medical examinations, drug tests, and others. The Algerian legislator designated them in Article 3 of Law No. 18-07 as genetic data and mental/physical condition of the natural person, also including them among sensitive data closely tied to the human person.

The privacy harmed by artificial intelligence is digital privacy, considered part of private life. Within the United Nations framework, a 2018 report on the right to privacy in the digital age stated that the right to privacy means recognizing individuals' right to a space for self-development based on interaction and freedom principles, or their right to a private sphere expanding for interaction or non-interaction with others without state intervention or intrusive excess by other individuals without recourse.

What highlights harm to the right to privacy from artificial intelligence techniques includes the following manifestations:

A - Various personal data are sometimes used for spying on persons or exploitation for commercial purposes or performing harmful, illegal acts for institutions and companies. Not to mention errors that may mar artificial intelligence use when employing

smart technology, for example in contracting. Also when using personal data belonging to persons via artificial intelligence techniques without their permission or license.

B - Using artificial intelligence as a means to violate persons' bank and financial accounts via internet, smartphones, and ATMs to execute banking operations, improve and facilitate banking services, potentially allowing theft of data specific to those operations. Artificial intelligence systems may be vulnerable to cyber threats, including attacks, data theft, and algorithmic biases, requiring strong cybersecurity measures to protect sensitive financial information and maintain customer trust.

C - Using ChatGPT artificial intelligence technology to pose questions about specific personal data enables violation and theft of that data.

D - In self-driving vehicles operating on GPS system, continuous uninterrupted internet use makes their information systems vulnerable to piracy, despite being a good service providing comfort and safety to facilitate transport movement.

E - Also self-driving vehicles in maritime transport. Using artificial intelligence techniques in maritime transport has reduced the human element's role in the contemporary system through relying on electronic navigation methods, automated positions, and electronic transmission/reception systems operating via precise data analysis and sensors. This ranks among the most important developments in maritime navigation. Artificial intelligence operates according to mechanisms not matching known error and negligence concepts, requiring development of a new legal theory considering these systems' privacy and providing sufficient protection to the harmed without overlooking technology complexities¹⁰.

B) Protecting the Right to Privacy from Artificial Intelligence Use:

Given the above enumeration, we affirm that the right to privacy is exposed to violation via artificial intelligence techniques, prompting legislative and even international conventions intervention to confront this by establishing a legal framework. We note here that most such laws and international conventions focused on protecting personal data regardless of the space used - without specifically targeting artificial intelligence. However, the European legislation is the only one that enacted an AI law in 2024, including protection of personal data used by artificial intelligence¹¹.

Some legislations ensuring personal data protection can be mentioned as follows:

- The European Regulation No. 679 of 2016 on personal data protection and free circulation¹².

- The French legislation issued in 2018 on personal data protection¹³.

- The Egyptian legislation issued in 2020 on personal data protection, including digital privacy protection controls¹⁴. Additionally, enacting the Information Technology Crime Law No. 175 of 2018.

- The Algerian legislation in aforementioned Law No. 18-07, stipulating that the text's objective is protecting personal data, affirming that personal data processing must respect human dignity, private life, public freedoms, and not harm persons' rights, honor, or reputation.

What characterizes the content of those legislative texts includes the following elements:

A - Affirming that protecting the right to privacy must be within respecting human dignity, private life, public freedoms, and not harming persons' rights, honor, or reputation.

B - Stipulating that automated data processing is automatic but conditional on prior consent of data owner, considered among ethical considerations mandatory for handling personal data. The Algerian legislator stated this in Article 7 of Law No. 18-07, with the person able to withdraw consent anytime possible. The same position was adopted by the French legislator in Article 7 of the 2018 law, requiring data owner's consent before processing, informing him of processing procedures and purpose. Considering capacity rules regarding incapacity or absence, taking guardian or proxy opinion.

C - Legitimacy of personal data processing: The above legislations included necessity for personal data processing to be legitimate via informing data owner of processing, methods to be taken, and purpose. Informing the data owner with precise details on his data processing, otherwise illegitimate. Generally, data owner must be informed of:

- Identity of who processes his personal data.
- Purpose of personal data processing.
- To whom those personal data will be directed.
- Right to object and access data.

The Algerian legislator went further by requiring prior license from the National Personal Data Protection Authority before any data processing, prohibiting sensitive data processing for public interest reasons or necessity for regulatory/legal tasks of processor, or genetic data processing except within certain limits.

D - Specifying purpose of collecting/processing personal data: Most mentioned legislations affirmed this condition, emphasizing restricting data processing to the purpose for which collected. For example, if a person deals with an entity requesting specific data, processing occurs only to achieve that purpose - providing/receiving a service. If another purpose, processing illegitimate. Data collection purpose aims at applying transparency, expressed by informing the person whose data collected of everything happening to it.

E - Imposing strict obligations on personal data handlers: Some legislations, including Algerian, imposed a set of obligations on personal data processor for protection. Thus stipulating confidentiality in processing, committing to security/safety of declared data by owner. Also prohibiting processor from transferring personal data to foreign country without license from data protection authorities, ensuring destination state provides sufficient protection for private life, freedoms, rights regarding personal data processing.

F - Enacting penal provisions: Among other provisions for personal data protection are penal ones, criminalizing acts constituting breach during processing/use, including via artificial intelligence. Here legislations vary in criminalizing such acts, stipulating penalties ranging from fines to imprisonment. Including criminalizing non-compliance with legal data processing as above.

We note here those texts did not specifically criminalize acts using AI technology, e.g., remaining in smart electronic processing crime, despite practical cases like hacking social networks and user passwords via AI. Included under data processing provisions.

Also criminalized acts obstructing electronic data processing system flow, as mentioned legislations criminalize any act stopping, disrupting, halting, or intercepting information network operation. Likewise criminalizing acts linked to data processing without prior owner permission¹⁵. Egyptian legislator went further by prohibiting trading smart devices for data violation purposes.

Artificial Intelligence and Privacy Encryption Problem

Finally, we mention the content of the European AI law entering force in parts in 2025 and remainder in 2026. This law affirmed applying EU Regulation 2016 content mentioned above on personal data protection, also stipulating:

- Protecting fundamental rights, especially right to privacy.
- Affirming commitment to data security/safety.
- Affirming data governance application, adopting transparency in handling, fairness rules, non-discrimination in personal data handling.

Conclusion:

Through the topic of artificial intelligence and the right to privacy, we reach a basic conclusion: the inseparability between the two systems despite mutual impact, especially AI's impact on privacy right. Here we affirm that the right to privacy has merged into AI techniques, as humanity entirely has become an open market and transparent wall where all data/information available without required solid fence/protection.

Specialists state AI has become a fertile space for spying and disclosing all human secrets across fields due to massive information/data flow on internet channels, despite attempts to set limits - this on one hand.

On the other, we affirm legislations' strictness in intervening to reduce AI damages to privacy right via laws protecting personal data within provisions ranging from imposing obligations on data processors to penal provisions via criminalizing privacy-breaching acts.

However, despite these legislative attempts to reduce negative effects of AI techniques on privacy right path, deficiencies can be noted as follows:

Firstly: Those legal texts lack specific provisions on AI; all general protecting personal data generally, except 2024 European legislation entering force 2025.

Secondly: Variation in personal data-regulating provisions across legislators; some succeeded in detailed rules for regulating/protecting like French, Egyptian, European; others remain distant like Algerian.

Thirdly: Some legislations, including Algerian, lack systems preserving personal data security/safety like encryption. Organized systems deficient given piracy/violation ease.

Based on these deficiencies, we propose the following suggestions:

- 1 - Necessity to enact specific texts regulating AI complementing personal data protection texts by legislations including Algerian, akin to European.
- 2 - Amending personal data protection laws linking also to AI system. Establishing secure/safe systems like encryption etc.
- 3 - Adopting transparency/data governance as systems ensuring fair/legitimate AI use.
- 4 - Training high-level staff in AI techniques to handle various personal data processing. Alerting persons/institutions/companies to AI dangers on data via seminars/sensitization meetings.

Bibliography:

¹- CANNARSA Michel, PIOTRAUT Jean-Luc et al., *Droit des affaires et intelligence artificielle, Diagnostic et perspectives*, Editions mare & martin, Paris, 2023, p. 11.

²- Ibid.

³- Ahmed Mohammed Brak, "Artificial Intelligence and Digital Privacy Right Legal Challenges and Prospects of AI ", *Journal of Legal and Economic Sciences*, Vol. 66, No. 3, 2024, p. 11

⁴- Quoted from: Maazouz Dalila, "Wali Nadia, AI Risks to Digital Privacy and Protection Mechanisms: Legal Challenges and Prospects of AI ", *Journal of Legal and Social Sciences*, Vol. 09, No. 3, 2024, p. 821.

⁵- Abdel Wahab Mohammed Abdel Wahab El-Saddah, *Legal Aspects of AI*, University Publications House, Alexandria, 2025, P. 11.

⁶- Saghi Mariam, Mazkour Malika, "AI and Privacy Problem", *Rawafid Journal for Studies and Scientific Research in Social and Human Sciences*, Vol. 8, No. 2, 2024, p. 524.

⁷- Law No. 18-07 dated June 10, 2018, relating to the protection of natural persons in the field of processing of personal data, *Official Gazette* No. 34 issued on June 10, 2018.

⁸- Ahmed Mohammed Brak, *Op.cit*, P. 11.

⁹- Heba Ramadan Rajab, "Legal Protection of Personal Data in Digital Technology Era: Legal Challenges and Prospects of AI ", *Journal of Legal and Economic Sciences*, Vol. 66, No. 3, 2024, p. 437 et seq.

¹⁰- Al-Qawsi, Hamam, "Sufficiency of General Civil Liability Rules in Compensating AI Damages", *Sharia and Law Journal*, No. 85, 2022, p. 227.

¹¹- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Regulation) (Text with EEA relevance)

PE/24/2024/REV/1, OJ L, 2024/1689, 12.7.2024 <http://data.europa.eu/eli/reg/2024/1689/oj>

¹²- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

¹³- Law No. 2018-493 of 20 June 2018 on the protection of personal data, Official Journal No. 0141 of 21 June 2018, <https://www.legifrance.gouv.fr/eli/loi/2018/6/20/2018-493/jo/texte>

¹⁴- Law No. 151 of 2020 relating to the issuance of the Personal Data Protection Law, Official Gazette No. 28 issued on July 15, 2020.

¹⁵- Samih Abdel Wahid Al-Tehami, "Controls on Personal Data Processing: Comparative Study between French and Kuwaiti Law", *Kuwaiti Global Law Faculty Journal*, p. 411.