

Journal of legal and social studies

Issn: 2507-7333

Eissn: 2676-1742

Protection of Digital Privacy Between the International Reference and the Global Governance of Artificial Intelligence

Benguettat Khadidja*

Abdelhamid Ibn Badis University Mostaganem (Algeria),

Khadidja.benguettat@univ-mosta.dz

International Law for Development Laboratory

Date of send: 01/03/2026	date of acceptance: 01/05/2026	Date of Publication: 01/06/2026
--------------------------	--------------------------------	---------------------------------

***Corresponding author**

Abstract :

The world today faces growing challenges in protecting the right to privacy due to the rapid development of artificial intelligence technologies and their extensive use of personal data. This article aims to examine the international legal framework governing the protection of this right in the digital environment by analyzing its recognition within global conventions and reviewing the main human rights standards regulating digital privacy under international human rights law. This research paper also explores the multiple international efforts undertaken by the United Nations and specialized organizations such as UNESCO and the Organisation for Economic Co-operation and Development (OECD) to strengthen legal and ethical protections in response to the risks posed by artificial intelligence. Particular attention is given to recent initiatives such as the Shanghai Declaration, the Seoul Declaration, and the Council of Europe's Framework Convention on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law. The study concludes that protecting privacy in the digital age requires a multilevel approach grounded in harmonizing international legal frameworks with modern technological developments and activating mechanisms of international cooperation to ensure the safe and responsible use of artificial intelligence.

Keywords: Artificial Intelligence, Right to Privacy, International Protection, Digital Privacy , AI Governance

Introduction:

Over the past two decades, the world has experienced a profound transformation driven by the digital revolution and the expanding capabilities of artificial intelligence. This has brought about a qualitative transition in the nature of social and economic relations, as well as in the very concept of the individual within society. Personal data and information have become the most valuable resource and a main focus of competition among both economic and political actors, making control over them a tool of power and influence. This new digital reality has generated a series of unprecedented challenges for the human rights legal framework, foremost among them the challenge of protecting the right to privacy, which has become increasingly threatened by surveillance, analysis, and predictive techniques utilized by artificial intelligence algorithms across various domains.

Privacy has shifted from a traditional concept linked to the sanctity of private life into a complex notion situated at the intersection of law, technology, security, and economics. The digital violation of personal data now have repercussions that extend beyond the individual to affect society and the democratic system as a whole. As concerns grow over the unethical use of artificial intelligence, calls have intensified for the establishment of global governance framework that ensures technological innovation remains consistent with the fundamental principles of human rights.

In this context, examining the international legal framework for the protection of the right to privacy assumes heightened significance, as it touches upon two central issues within the contemporary international order. The first concerns the capacity of the human rights system to adapt to the rapid pace of technological advancement; the second relates to the extent of responsibility borne by international actors and multilateral institutions in regulating the use of artificial intelligence so as to fulfill a balance between scientific progress and the protection of human dignity. Hence, studying the international legal foundations of the right to privacy and the multiple global efforts sought at protecting it in the digital environment has become both an intellectual and practical necessity.

The research problem statement arises from the question of how effective the existing international legal framework is in addressing the risks that artificial intelligence poses to the right to privacy, and whether current international efforts are sufficient to ensure respect for this right amid the ongoing global digital transformation.

This research seeks to analyze the international legal framework governing the right to privacy and to shed light the developments it has undergone in the context of the contemporary technological revolution. It focuses particularly on recent United Nations and institutional initiatives aimed at establishing a global system for the governance of artificial intelligence that upholds human values while ensuring transparency and accountability. The research also endeavors to highlight the delicate balance between the protection of privacy, on the one hand, and the requirements of technological innovation and the public interest, on the other.

The study adopts a descriptive and analytical methodology in examining the relevant international instruments and mechanisms, supported by a comparative approach to highlight points of convergence and divergence among multiple international and regional initiatives. Furthermore, a prospective approach is employed to evaluate future trends in the regulation of artificial intelligence and the protection of digital privacy.

This research is divided into two main sections. The first section examines the international foundations of privacy protection in the context of global digital transformation by analyzing the international recognition of the right to privacy and the human rights standards governing digital privacy. The second section focuses on determining and analyzing international efforts to safeguard this right from the risks linked to artificial intelligence, through a review of recent United Nations initiatives and international recommendations sought at establishing a fair and responsible global framework for the governance of artificial intelligence.

First Section: The International Foundations of Privacy Protection in the Context of Global Digital Transformation

The right to privacy constitutes one of the fundamental pillars for the protection of human dignity. It has received broad recognition in international human rights instruments since the mid-twentieth century. With the global digital transformation and the increasing dependence on data, the need has emerged to reinterpret this right in light of the new technological environment. Therefore, this section explores the international foundations of privacy protection by reviewing the most important legal texts and standards that have established the general framework for the right to privacy in the digital world.

First Subsection: International Recognition of the Right to Privacy

International recognition of the right to privacy constitutes the starting point in building the legal framework for the protection of this right, as it represents the normative basis upon which all subsequent regulatory and enforcement efforts have been built. This recognition has been consolidated through a number of major international human rights instruments that affirm the inviolability of private life and the necessity of safeguarding it from arbitrary interference, regardless of its means or forms.

First: In the United Nations Charter and the Universal Declaration of Human Rights

The United Nations Charter of 1945 did not contain an explicit provision recognizing the right to privacy¹; however, it laid the normative foundation that paved the way for its later recognition within the international human rights system. The Charter repeatedly emphasized the respect for human dignity and the protection of fundamental rights and freedoms for all individuals without discrimination, which implicitly encompasses the protection of individuals' private lives from any violation or arbitrary interference.

Article 1, paragraph 3, of the Charter includes among the purposes of the United Nations the aim of “fulfilling international cooperation in fostering and encouraging respect for human rights and for fundamental freedoms for all,” thereby affirming the international community's commitment to protecting individual rights in all their dimensions, including the right to privacy. Furthermore, Article 55 provides that the United Nations shall promote “universal respect for, and observance of, human rights and fundamental freedoms for all without distinction,” while Article 56 obliges Member States to act, both individually and jointly, to achieve these purposes, making respect for individual rights a general international obligation.

The general framework established by the UN Charter served as the historical and conceptual foundation for the subsequent development of the international human rights system. It formed the basis for the explicit recognition of the right to privacy, as the Charter stands as a founding reference that enshrined the principle of respect for human dignity as the cornerstone of all rights and opened the door for the evolution of privacy as an independent right sought at safeguarding individuals' private lives against any intrusion or surveillance that might violate their personal integrity.

Regarding the Universal Declaration of Human Rights², the right to privacy is explicitly recognized in Article 12, which states: “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”³

This provision is considered the starting point for the protection of personal data, as it provides, on the one hand, the necessary safeguards for individuals by prohibiting interference except within the limits permitted by law. On the other hand, it establishes a framework for regulating the flow of information, which must also occur only within the boundaries set by law.

Second: In the International Covenant on Civil and Political Rights (Article 17)

Article 17 of the International Covenant on Civil and Political Rights⁴ (ICCPR) states that: “No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”⁵

The General Comment No. 16 issued by the UN Human Rights Committee on this article regarding the protection of private life states that, under Article 17, every person has the right not to be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, nor to unlawful attacks on his honour and reputation. The Committee further highlighted that this right must be guaranteed against all such interferences and attacks, whether committed by State authorities or by natural or legal persons. Therefore, the obligations imposed by this article require States to adopt legislative and other necessary measures to implement the prohibition of such interferences and to ensure effective protection of this right.

Accordingly, this Covenant may be considered one of the earliest milestones in the development of personal data protection, despite the generality of its wording. With the evolution of the digital environment, this right has expanded to encompass informational privacy, as an integral element of human dignity and individual freedom.

Third: In Other International Human Rights Instruments

In addition to the recognition of the right to privacy in general instruments such as the Universal Declaration of Human Rights and the International

Covenant on Civil and Political Rights, a number of specialized human rights treaties have also affirmed the protection of this right as a legally binding foundation. For instance, the Convention on the Elimination of All Forms of Discrimination against Women (1979)⁶, in Article 16, protects women's private life within the family context, affirming that privacy is a necessary element in preserving women's dignity and rights. Similarly, the Convention on the Rights of the Child (1989)⁷, in Article 16, states that: "No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation." This provision reflects international recognition of the significance of safeguarding children's privacy as a cornerstone of human rights.

These conventions indicate that the right to privacy is no longer merely a general principle but has become a specific legal obligation incumbent upon States Parties toward certain categories of individuals. This development strengthens the international legal foundation of the right to privacy. Furthermore, these provisions serve as a significant reference for understanding how privacy can be protected and adapted in the context of modern digital and technological transformations, encompassing artificial intelligence. They also offer a legal basis for addressing the risks that may threaten individuals' private lives in the digital environment.

The international recognition of privacy as a fundamental right in general instruments and specific conventions has established the legal foundation for this right. However, digital transformation has introduced new challenges that traditional legal texts did not anticipate, such as mass data collection, digital surveillance, and automated decision-making that directly affect individuals' lives. Accordingly, it has become necessary to examine contemporary international human rights standards governing privacy in the digital space.

Second Subsection: International Human Rights Standards Governing Digital Privacy

After the international recognition of the right to privacy was firmly established, the need arose to develop more detailed human rights standards to regulate its exercise and determine its boundaries within the digital environment. Thus, it is essential to identify the principles that balance the protection of private life, ensuring public security, and fostering technological development. From this context, a set of international standards emerged, serving as the guiding framework for interpreting and applying the right to digital privacy amid the global digital transformation.

First: Digital Rights as Supportive Human Rights

Digital rights are an integral part of the human rights system, possessing a distinct identity that sets them apart and confers upon them a sense of originality and independence. However, these rights have a dual nature; they also serve as an effective means of supporting the multiple types and generations of other human rights.

International law plays a crucial role in safeguarding the right to privacy at the global level. It enshrines this right as one of the fundamental human rights and sets the legal frameworks necessary for its protection. Furthermore, it is a primary reference for holding states and relevant entities accountable in cases of privacy violations by defining precise criteria that determine what constitutes an infringement or breach of this right.

Therefore, states and governments are obligated, under international law, encompassing its treaties, charters, and conventions to respect and safeguard the right to privacy as a fundamental human right. These obligations include protecting individuals from any form of “arbitrary” or “unlawful surveillance” and preventing interference with their private communications and personal data. Such protection has become increasingly important in light of the rapid advances in communication technologies, which now pose a “direct threat” to individual rights and freedoms, foremost among them, the right to privacy⁸.

Thus, digital rights have become a necessary gateway to understanding and recognizing these rights. They now occupy a leading position in the dissemination of human rights culture, as well as in education and training. Moreover, they play a pivotal role in monitoring, documenting, and exchanging information concerning the degree of international compliance with these rights.

Hence, there is an urgent need to strengthen attention to digital rights at the international level and to integrate them explicitly and clearly within the broader framework of internationally recognized human rights under international human rights law⁹.

Second: The Right to Digital Autonomy

This standard concerns individuals’ right to be informed about how their digital data is collected, the purposes for which it is utilized, and the entities that have access to it. It also encompasses their right to accountability and the ability to request correction or deletion of their data. Furthermore, it includes the right to encryption, which refers to the process of converting readable data into an

encrypted format that cannot be accessed or processed without decryption. This right was affirmed in a United Nations report issued under the first UN resolution on the promotion and protection of the right to digital privacy and encryption, recognizing encryption as one of the most significant rights for protecting freedom of opinion and expression in the digital era¹⁰.

Third: The Principle of Necessity and Proportionality in Restricting Digital Privacy

The right to digital privacy ensures that neither the state nor any other official or non-official entity interferes in individuals' personal lives or spies on them whether by sharing their personal information or data, or by accessing their correspondence. Furthermore, it reinforces this right in the context of digital surveillance or interception of communications, both within and beyond national borders. Therefore, the law must guarantee protection against such violations, as affirmed by Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights. Thus, states are required to adopt measures that limit privacy violations and ensure that relevant national legislation aligns with their obligations under international human rights law, particularly those associated with surveillance, interception of communications, and personal data collection.

Any interference with digital privacy by states or other entities must be justified by legitimate necessities, such as national security or public order.

Moreover, such restrictions must be proportionate to the objective pursued, avoiding excess, arbitrariness, or infringement of human rights¹¹.

Second Section: International Efforts to Protect the Right to Privacy from the Risks of Artificial Intelligence

In light of the growing challenges posed by artificial intelligence in safeguarding personal data, international efforts have increasingly sought new ways to foster the right to privacy and address emerging technological risks. International and regional organizations have recognized that existing legal frameworks are no longer sufficient to ensure effective protection in an era of rapidly evolving monitoring and data analysis technologies. Therefore, this section emphasizes the main international and institutional initiatives aimed at protecting digital privacy against the risks of AI.

First Subsection: United Nations and Institutional Efforts to Strengthen Digital Privacy Protection

In recent years, international organizations at various levels have increasingly engaged in developing policies and standards designed to ensure the responsible use of AI technologies and protecting digital privacy. Alongside the efforts of the United Nations and the Human Rights Council, considerable institutional initiatives have emerged from specialized organizations such as UNESCO and the Organisation for Economic Co-operation and Development (OECD). These initiatives sought to establish ethical and legal principles that guide the development of AI within a framework that respects human rights and protects personal privacy.

First: United Nations and Human Rights Council Resolutions

Electronic surveillance, mass data collection, and automated information analysis have become tools that directly affect the essence of individuals' private lives, requiring a comprehensive legal and human rights response. In this regard, the efforts of the United Nations and the Human Rights Council have emerged as the most effective institutional framework for establishing international standards governing digital privacy, through their resolutions, reports, and initiatives aimed at aligning technological development with respect for human dignity and fundamental rights.

United Nations General Assembly Resolution No. 68/167 on the Right to Privacy in the Digital Age

The United Nations General Assembly Resolution 68/167, adopted on 18 December 2013, on "The Right to Privacy in the Digital Age," expresses deep concern over the adverse impact that communication surveillance and interception may have on the enjoyment of human rights. The General Assembly affirmed that the rights of individuals offline must also be safeguarded online, calling upon all States to respect and protect the right to privacy in digital communications. It further urged States to review their procedures, practices, and legislation associated with the surveillance and interception of communications and the collection of personal data, highlighting the necessity of ensuring that such measures comply with their obligations under international human rights law, which provides the global framework for assessing any interference with the right to individual privacy¹².

The Office of the United Nations High Commissioner for Human Rights (OHCHR) report on the right to privacy in the digital age (2014).

Through the adoption of the aforementioned General Assembly Resolution No. 68/167 of 18 December 2013, the General Assembly requested the Office of

the United Nations High Commissioner for Human Rights to prepare a report on the right to privacy in the digital age. According to the text of the resolution, the report was to examine the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance of digital communications, and/or their interception and the collection of personal data, including on a mass scale, and present relevant views and recommendations¹³.

The report concluded that there is a clear and urgent need for vigilance to ensure that privacy policies and practices are accompanied by effective safeguards against abuse. As an immediate measure, States should review their domestic laws, policies, and practices to ensure compliance with international human rights law, in particular the protection of the right to privacy.

The report also underscored the significance of establishing effective and independent oversight mechanisms and ensuring adequate remedies and compensation for victims of violations¹⁴.

Additionally, the UN General Assembly reaffirmed the right to privacy in the digital age under Resolution 69/166, of 18 December 2014, urging States to respect and safeguard the right to privacy, take effective measures to prevent violations, and ensure that domestic legislation is consistent with their obligations under international human rights law¹⁵.

In this context, other resolutions were adopted by the United Nations General Assembly concerning the protection of the right to privacy in the digital age, including Resolution No. 71/199 of 19 December 2016, and Resolution No. 34/7 of 23 March 2017 on the protection of the right to privacy in the digital age.

Furthermore, Resolutions 32/13 of 1 July 2016 and 38/7 of 5 July 2018 addressed the promotion, protection, and enjoyment of human rights on the Internet. Furthermore, Resolutions No. 32/13 of 1 July 2016 and No. 38/7 of 5 July 2018 addressed the promotion and protection of human rights and the enjoyment thereof on the Internet, as well as Resolution No. 73/179 of 17 December 2018 regarding the right to privacy in the digital age¹⁶.

United Nations General Assembly Resolution on Artificial Intelligence, Privacy, and Children's Privacy (2021)

This resolution refers to the report of the Special Rapporteur on the right to privacy, issued by the Human Rights Council of the United Nations General Assembly during its 46th session in 2021¹⁷. Its main recommendations included the development of guidelines on the use of personal and non-personal data in the

context of artificial intelligence solutions, underscoring the significance of a legitimate legal basis for any processing of data by governments or companies when utilizing AI, within the broader framework of the human right to privacy. The General Assembly and the Human Rights Council reaffirmed that the rights enjoyed by individuals offline must also be safeguarded online and established data protection standards associated with AI solutions as a reference for ensuring the protection of the right to privacy in the context of artificial intelligence.

Notably, the United Nations General Assembly adopted a new resolution on AI in March 2024, with the participation of 193 member states. This resolution focused on the governance of multi-purpose artificial intelligence and global AI governance frameworks. Although it did not address general artificial intelligence (AGI) or explicitly mention digital privacy, it supported key principles such as safety, transparency, and accountability, which are fundamental to fostering the protection of the right to privacy in the digital environment.

Second: UNESCO Recommendation on the Ethics of Artificial Intelligence (2021)

The UNESCO Recommendation on the Ethics of Artificial Intelligence (2021) is regarded as the first global instrument of its kind, designed to offer a comprehensive legal and ethical framework for the governance of AI technologies and applications. It establishes a set of ethical values and legal principles intended to guide the responsible use of AI across multiple domains and sectors.

General Framework of the Recommendation

Adopted unanimously by 193 member states of the United Nations Educational, Scientific and Cultural Organization on 24 November 2021, during the organization's 41st General Conference in Paris, this recommendation constitutes the first international standard-setting instrument to systematically address the relationship between artificial intelligence and human rights¹⁸.

The recommendation aims create a global normative framework that ensures the development and use of AI in ways that respect human dignity and enhance sustainable development. The recommendation is grounded in several core principles, including:

- Respect for human rights and dignity as a fundamental basis for the use of AI.
- Protection of privacy and personal data, ensuring data security and limiting its use to legitimate purposes¹⁹.

- Transparency and accountability in the design and operation of AI systems, enabling individuals and societies to understand how decisions are made and what their effects are.²⁰
- Fairness and non-discrimination, to prevent AI from reinforcing existing inequalities or biases²¹.
- Continuous human oversight, to preserve human centrality in decision-making processes²².

These principles form the ethical foundations that UNESCO urges member states to incorporate into their national AI policies in order to reduce potential risks that AI may pose to fundamental rights and freedoms²³.

Digital Privacy within the Framework of the UNESCO Recommendation

The recommendation places special attention on safeguarding the right to digital privacy, regarding it as one of the core pillars of AI ethics. It emphasizes that the collection and processing of personal data must comply with the principles of legality, transparency, proportionality, and legitimate purpose, while requiring states to establish national data protection frameworks consistent with international ethical standards²⁴.

Moreover, it emphasizes the need to empower individuals to control their personal data and to ensure that technical actors and institutions developing or deploying AI systems are held accountable in cases of privacy rights violations²⁵.

The recommendation further calls for the creation of independent national bodies on AI ethics, responsible for assessing the ethical and technical risks related to data collection and analysis, and for developing mechanisms for the periodic review of digital systems that have an effect on fundamental rights²⁶.

Consequently, this recommendation is considered a pivotal step in establishing the right to digital privacy within the ethical and legal framework governing modern technologies, making it a key international reference in the formulation of legislation and policies associated with responsible artificial intelligence²⁷.

Third: OECD Principles on Responsible Artificial Intelligence

The Organisation for Economic Co-operation and Development (OECD) has played a key role in enhancing respect for the right to privacy. In 1978, the OECD started developing guidelines and reference framework for privacy protection and data transfer. These guidelines were adopted by the OECD Council in 1980 under the title “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.” The recommendations highlight the need to respect

privacy and individual freedoms, while balancing potentially conflicting values, such as the right to privacy and the free flow of information²⁸.

At the forefront of the recommendations, the Council recognized that the free transborder flow of personal data contributes to economic and social growth. This recognition imposes on member countries to ensure the protection of personal data, privacy, and individual freedoms within a coherent legal and regulatory framework that prevents any obstruction to the cross-border flow of data²⁹.

Although these guidelines are non-binding, they serve as important reference principles applicable to both automated and non-automated data processing. The OECD recommendations identify eight key guiding principles for protecting privacy and ensuring the secure transborder flow of personal data: collection limitation, which restricts data collection to what is necessary; data quality, ensuring that data is relevant and accurate; purpose specification, defining clear objectives for data collection; utilize limitation, restricting data use to specified purposes; security safeguards, ensuring the protection and integrity of data; openness, promoting transparency in data handling; individual participation, allowing individuals to access and correct their data; and accountability, ensuring responsible data management³⁰.

In May 2019, the (OECD) adopted its international principles on the development of trustworthy artificial intelligence, the first intergovernmental standards for the responsible governance of AI, endorsed by over 42 countries. These principles, presented in 2024³¹, provide guidance for the development of responsible AI systems and highlight the significance of human values, fairness, transparency, explainability, safety, reliability, and accountability. Although these principles are not legally binding, they have had a profound influence on national AI policies and may, in the future, contribute to the formation of customary international norms in this field³².

Second Subsection: Recent International Efforts Toward Global Governance of Artificial Intelligence and the Protection of Privacy

Amid growing concerns about the unethical use of artificial intelligence technologies, international efforts have not been limited to the United Nations but have also extended to specialized organizations seeking to establish normative and ethical frameworks to regulate technological development and ensure its alignment with human rights. Among the most notable initiatives is UNESCO's Recommendation on the Ethics of Artificial Intelligence (2021) the first

comprehensive global document addressing the relationship between technological innovation and human values. Therefore, this section examines the general framework of that recommendation and the place of digital privacy within its provisions.

First: The Seoul Declaration on AI Safety (2024)

The Seoul Declaration was adopted at the conclusion of the Second Global AI Safety Summit, held on May 21–22, 2024, under the joint auspices of the Republic of Korea and the United Kingdom, following the inaugural summit in London³³.

The declaration seeks to develop shared governance frameworks among countries to foster safety, innovation, and inclusivity in artificial intelligence, while highlighting the need to respect human rights and safeguard privacy in the development and deployment of intelligent systems. The Seoul Declaration introduces a significant step toward coordinating international efforts to establish common standards that balance technological innovation with the requirements of safety and ethical responsibility³⁴.

Although the declaration primarily focuses on ensuring the safety, innovation, and inclusiveness of intelligent systems, it intersects with efforts to safeguard digital privacy by emphasizing the principles of transparency, accountability, and technical safety. These key elements in protecting the right to privacy within a secure digital environment.

Second: The Shanghai Declaration on Global AI Governance (2024)

The Shanghai Declaration was announced on July 4, 2024, at the conclusion of the World Artificial Intelligence Conference, with the participation of several countries and international organizations. This declaration is regarded as one of the most recent global initiatives highlighting the international dimension of AI and the unprecedented challenges it poses to digital security and individual privacy³⁵.

The declaration focuses on promoting international cooperation in the development and application of AI technologies, while ensuring safety and reliability, and enhancing equal opportunities among countries in formulating their national AI strategies. It also calls for the establishment of a global mechanism for managing AI affairs under the auspices of the United Nations, as well as raising public awareness to ensure broad participation in shaping relevant policies. The significance of this declaration lies in its comprehensive and global

nature, as it lays the foundations for principles that may eventually evolve into an international charter adopted by the United Nations to regulate artificial intelligence and safeguard digital rights³⁶.

Efforts to protect the right to privacy have continued, as reflected in the Final Declaration of the “Action for AI” Summit held in Paris (February 2025), which represents one of the most recent international initiatives in AI governance. The summit brought together 58 countries, along with the European Union and the African Union Commission. The declaration focused on inclusive and sustainable AI and acknowledged the significance of global governance. However, it also demonstrated divergent international perspectives and failed to produce concrete regulations or binding provisions to govern general AI. Therefore, its link to the right to digital privacy remains indirect, as it contributes more broadly to enhancing the principles of safety, transparency, and accountability, which underpin privacy protection in the digital environment³⁷.

Third: The Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law (2024)

In response to the urgent need for global governance of AI, the Council of Europe took a pioneering step by presenting the first legally binding international treaty on AI, the Framework Convention on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law³⁸.

Adopted on May 17, 2024, and opened for signature on September 5, 2024, this convention marks a milestone in global efforts to establish common standards for AI governance. It seeks to create a harmonized approach among signatory countries while respecting the diversity of legal systems and regulatory traditions across different jurisdictions.

The convention aims to ensure that the development and use of AI systems are consistent with the principles of human rights, democracy, and the rule of law, by requiring state parties to adopt legislative and regulatory measures to safeguard privacy and personal data at all stages of the of AI systems’ lifecycle. Furthermore, it reinforces the principles of transparency and accountability, and calls for international cooperation in developing suitable ethical and legal frameworks³⁹.

Importantly, the AI Framework Convention does not exist in isolation but rather aims to complement and reinforce existing international human rights instruments. It explicitly refers to a broad range of global and regional human rights treaties, encompassing the Universal Declaration of Human Rights, the

International Covenant on Civil and Political Rights, the International Covenant on Economic, Social and Cultural Rights, and the European Convention on Human Rights, among others. This approach highlights the Convention's role in extending the protection of human rights into AI technologies.

As the following section examines the specific provisions of the AI Framework Convention, it is necessary to keep this broader context in mind. The Convention serves as a key legal instrument within an evolving network of global governance initiatives sought at ensuring that the transformative potential of AI technologies is harnessed in ways that respect and foster fundamental rights and democratic values⁴⁰.

Although this Convention was issued by the Council of Europe and is therefore formally a regional European treaty, it possesses a distinctly international character due to its openness to non-European countries such as the United States and Japan. Hence, it represents a regional instrument in origin but global in scope and substance, marking a significant step toward establishing a binding international framework for AI governance and the protection of the right to digital privacy.

However, the Convention faces several challenges. Despite its “legally binding” nature, it lacks strong enforcement mechanisms, unlike the more stringent regulatory framework of the European Union. Furthermore, its general and principle-based provisions may lead to varying interpretations and implementations among member states, potentially undermining the uniformity of international standards. Additionally, the flexibility granted to the private sector may also result in regulatory fragmentation, complicating compliance for global developers.

Effective application will require unprecedented international cooperation, which may prove difficult amid current political polarization and geopolitical tensions. Furthermore, technical challenges persist, such as monitoring compliance with risk assessment requirements associated with computing capabilities and defining safety standards for high-risk technologies.

Conclusion

This study revealed that safeguarding the right to privacy in the age of artificial intelligence represents one of the most pressing challenges facing international human rights law, given the cross-border nature of digital technologies and their growing intrusion into individuals' private lives. The analysis demonstrated that, although the international legal framework recognized

the right to privacy at an early stage, it still lacks specialized mechanisms capable of keeping pace with modern technological developments.

Recent international initiatives, particularly the Shanghai Declaration on Global AI Governance (2024), the Seoul Declaration on AI Safety (2024), and the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law (2024), reflect a clear trend toward consolidating the principles of international cooperation, shared responsibility, and balancing technological innovation with the protection of fundamental rights, foremost among them the right to privacy.

Therefore, the study reached the following conclusions:

1. Digital privacy has become a natural extension of traditional privacy and is governed by the same fundamental principles that protect private life.
2. The Council of Europe Framework Convention represents an important step toward the internationalization of AI ethics standards and their integration with states' human rights obligations. However, its effectiveness ultimately relies on the extent of ratification, the seriousness of implementation, and its capacity to address existing shortcomings.
3. There remains a lack of international coordination in establishing a unified global framework that balances cybersecurity requirements with digital privacy protection.
4. The growing dependence of states and organizations on non-binding initiatives highlights the need to transform these principles into explicit contractual obligations.

Based on the above, the study offers the following recommendations:

1. Calling for the drafting of a comprehensive international instrument, under the auspices of the United Nations, to regulate the use of artificial intelligence in light of human rights principles.
2. Enhancing coordination between international and regional mechanisms to avoid duplication of efforts and ensure normative consistency in privacy protection.
3. Encouraging states to develop comprehensive national legislation that guarantees transparency and accountability in data processing and the use of AI technologies.
4. Integrating the concept of digital privacy into legal and human rights education and training programs to raise awareness of the emerging risks related to artificial intelligence.

¹ The Charter of the United Nations was signed in San Francisco on June 26, 1945, and entered into force on October 24, 1945.

² The Universal Declaration of Human Rights was adopted and proclaimed by United Nations General Assembly Resolution 217 (III) on December 10, 1948.

³ See Article 12 of the Universal Declaration of Human Rights (1948).

⁴ The International Covenant on Civil and Political Rights was adopted by United Nations General Assembly Resolution 2200 (XXI) on December 16, 1966, and entered into force on March 23, 1976.

⁵ Khaled Hassan Ahmed, *The Right to Personal Data Privacy between Legal Protection and Technical Challenges: A Comparative Study*, Dar Al-Kutub wa Al-Dirasat Al-Arabiya, Egypt, 2020, p. 96.

⁶ The Convention on the Elimination of All Forms of Discrimination against Women was adopted by United Nations General Assembly Resolution 34/180 on December 18, 1979, and entered into force on September 3, 1981.

⁷ The Convention on the Rights of the Child was adopted and opened for signature, ratification, and accession by United Nations General Assembly Resolution 44/25 on November 20, 1989, and entered into force on September 2, 1990.

⁸ Chaalal Mokhtar, *The Right to Privacy in the Digital Space and Its Protection in International Law*, Doctoral Dissertation, Faculty of Law and Political Science, University of Oran, 2023, p. 131.

⁹ Al-Saadi, Wissam Naamat Ibrahim. *Digital Rights and the International Protection Mechanisms Established for Them within the Framework of International Human Rights Law*, Fourth International Conference on Legal Issues, Tishk International University, Vol. 1, Iraq, April 30, 2019, p. 355.

¹⁰ Al-Azzazi, Nabil Mohamed. *Digital Human Rights*, *The Legal Journal*, Vol. 19, No. 1, Cairo University, February 2024, p. 694.

¹¹ Ounaf, Hadjer, and Hireche, Soumia. *Digital Rights in Algeria: A Study of Concepts and Protection Mechanisms*, *Journal of Political Horizons*, Al-Madar Knowledge Center for Research and Studies, Vol. 7, No. 1, 2023, p. 254.

¹² United Nations, Office of the High Commissioner for Human Rights. *The Right to Privacy in the Digital Age*, Report of the Special Rapporteur to the 27th Session of the Human Rights Council, Document No. A/HRC/27/37, Geneva, June 30, 2014. Published on the official website:

<https://www.ohchr.org/AR/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx>

(accessed October 25, 2025).

¹³ Ibid.

¹⁴ For more details, see: Rizk Salmoudi, Linda Rabaia, Hadil Al-Razi, and Issam Barahma, "The Contemporary Position of Public International Law Rules on the Right to Privacy in the Digital Age," *Arab American University Research Journal*, Vol. 3, No. 2, 2017, p. 13.

- ¹⁵ Dihya Abdelatif and Ben Belkacem Ahmed, “The New Role of the United Nations in Protecting the Right to Privacy in the Digital Age,” *Al-Ustadh Al-Bahith Journal for Legal and Political Studies*, Vol. 2, No. 8, December 2018, p. 501.
- ¹⁶ United Nations General Assembly, Resolution No. 73/179 of December 17, 2018, entitled “The Right to Privacy in the Digital Age,” Seventy-third Session, A/RES/73/179.
- ¹⁷ United Nations General Assembly, Human Rights Council, Artificial Intelligence and Privacy, and the Privacy of Children, Report of the Special Rapporteur on the Right to Privacy, Joseph A. Cannataci, Forty-seventh Session of the Human Rights Council (22 February–19 March 2021), Document No. A/HRC/46/37, United Nations, Geneva, January 21, 2021.
- ¹⁸ UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence. Paris, November 24, 2021, p. 4.
- ¹⁹ UNESCO. (2021), paras. 23–26.
- ²⁰ UNESCO. (2021), paras. 33–38.
- ²¹ UNESCO. (2021), paras. 40–42.
- ²² UNESCO. (2021), para. 47.
- ²³ UNESCO. (2021). Press Release: Historic Agreement Adopted to Guide the Development of Artificial Intelligence Worldwide, November 25, 2021.
- ²⁴ UNESCO. (2021), paras. 25–26.
- ²⁵ UNESCO. (2021), paras. 34–35.
- ²⁶ UNESCO. (2022). Implementing the Recommendation on the Ethics of AI: First Steps and National Strategies. Paris, p. 15.
- ²⁷ United Nations University. (2022). UNESCO’s AI Ethics Recommendation: A Global Standard-Setter in the Making. Tokyo.
- ²⁸ Jamal Youssef Bedir. *Modern Trends in Knowledge and Information Management*. Dar Kunooz Al-Ma’rifah, Jordan, 2013, p. 244. Mona Al-Ashqar Jabbour and Mahmoud Jabbour. *Personal Data and Arab Laws (Security Concerns and Individual Rights)*. Arab Center for Legal and Judicial Research, League of Arab States, Beirut, Lebanon, 2018, p. 51.
- ²⁹ Mouna Al-Ashqar Jabbour and Mahmoud Jabbour. *Ibid.*, p. 52.
- ³⁰ Jamal Youssef Bedir. *op. cit.*, p. 245. Ben Gara, Mostafa Aisha. “The Right to Informational Privacy between Technological Challenges and the Reality of Legal Protection.” *Journal of Jurisprudence and Law*, No. 42, April 2016, p. 78.
- ³¹ OECD. *Digital Economy*. OECD Publishing, 2020, p. 273.
- ³² OECD, Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449), adopted on 22 May 2019, updated in 2024.

³³ “Seoul Declaration for Safe, Innovative and Inclusive AI,” AI Seoul Summit, May 21, 2024, available at: https://www.mofa.go.kr/eng/brd/m_5674/view.do?seq=321007 (accessed 22 October 2025).

³⁴ Marie Davidsen Buhl, Ben Bucknall, Tammy Masterson, Emerging Practices in Frontier AI Safety Frameworks, arXiv, February 5, 2025, available at: <https://arxiv.org/abs/2503.04746> (accessed October 24, 2025).

³⁵ Readings on the Contents of the Shanghai Declaration on Global AI Governance, Emirates Center for Strategic Studies and Research. Available at: <https://www.ecssr.ae/ar/products/1/197487> (accessed October 24, 2025, at 16:00).

³⁶ Shanghai Declaration on Global AI Governance, World Artificial Intelligence Conference, Shanghai, July 4, 2024, Ministry of Foreign Affairs of the People’s Republic of China. Available at: https://www.mfa.gov.cn/eng/xw/zyxw/202407/t20240704_11448351.html (accessed October 22, 2025).

³⁷ Ministry for Europe and Foreign Affairs of France, Joint Statement on the AI Summit, Paris, February 2025, available at: <https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-affairs/ai-summit-paris-2025/> (accessed October 24, 2025).

³⁸ Council of Europe, Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law, Strasbourg, 24 May 2024, available at: <https://www.coe.int/en/web/artificial-intelligence/framework-convention>.

³⁹ Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law, art 5, 6, 7, 16.

⁴⁰ Chang, Cheng-chi (Kirin), The First Global AI Treaty: Analyzing the Framework Convention on Artificial Intelligence and the Eu AI Act (December 20, 2024). 2024 University of Illinois Law Review (Online) 86 (2024), Available at SSRN: <https://ssrn.com/abstract=5069335> or <http://dx.doi.org/10.2139/ssrn.5069335>, (accessed October 21, 2025).