

The Right to Digital Privacy in The International Legal Instruments

الحق في الخصوصية الرقمية في المواثيق الدولية

CHERABCHAR Linda *

Faculty of Law and Political Science, University of Souk Ahras, (Algeria)

linda.cherabcha@univ-soukahras.dz

Date of Submission 02-04-2026 Date of Final Acceptance 29-05-2026 Date of Publication June 2026

Abstract:

The tremendous advances in modern technology have exponentially heightened threats to private life. Individuals now face pervasive constraints in personal affairs due to the continual monitoring, storage, and processing of their data through digital media. Sophisticated surveillance systems, cyber-espionage, and hacking pose serious risks to privacy and personal freedoms—especially when these practices occur without consent or are employed for intrusive purposes. Given the disruptive evolution in ICT, this study elucidates the mechanisms for safeguarding the right to digital privacy, recognizing it as a fundamental human right enshrined in international human rights treaties.

Keywords:Digital Privacy; Right to Private Life; International Legal Instruments;Cybersecurity; Protection of Personal Data.

ملخص:

أدت التطورات الهائلة في التكنولوجيا الحديثة إلى تضخيم التهديدات التي تطل الحياة الخاصة بشكل غير مسبوق. إذ بات الأفراد يواجهون قيودًا شاملة في شؤونهم الشخصية نتيجة الرصد المستمر، وتخزين ومعالجة بياناتهم عبر الوسائط الرقمية. كما تُعد أنظمة المراقبة المتطورة، والتجسس الإلكتروني، والقرصنة من أبرز المخاطر التي تهدد الخصوصية والحريات الفردية، ولا سيما عندما تُمارس هذه الأفعال دون علم الأفراد أو تُستخدم لأغراض تدخلية تمسّ بحقوقهم. وفي ظل التحولات المتسارعة التي يعرفها مجال تكنولوجيا المعلومات والاتصال، تسعى هذه الدراسة إلى توضيح آليات حماية الحق في الخصوصية الرقمية، باعتباره حقًا أساسيًا من حقوق الإنسان نصّت عليه المواثيق الدولية المعنية بحقوق الإنسان. الكلمات المفتاحية: الخصوصية الرقمية؛ الحق في الحياة الخاصة؛ المواثيق الدولية؛ الأمن السيبراني؛ حماية البيانات الشخصية

* Corresponding Author: CHERABCHAR Linda

Introduction:

International legal instruments have unequivocally enshrined and emphasized the necessity of safeguarding the individual's private life—commonly referred to as the right to privacy—as articulated in the Universal Declaration of Human Rights of 1948. In particular, Article 17 of the International Covenant on Civil and Political Rights (ICCPR) stipulates that no person shall be subjected to arbitrary or unlawful interference with their privacy, family, home, or correspondence, nor to unlawful attacks on their honor and reputation, and that everyone has the right to the protection of the law against such interference or attacks. This right is considered inherent and inalienable to the human person.

Technological and digital advancements have given rise to what is now termed "digital privacy" or "informational privacy," emerging as a direct consequence of the unprecedented global expansion in the fields of information and communication technology. The widespread reliance on the Internet, the proliferation of smart devices, and the rapid emergence of e-services have collectively redefined the contemporary landscape of human rights. In the context of international law, rights have expanded to include what are now widely referred to as digital rights.

The right to privacy is intimately linked to the broader right to liberty, as privacy represents, according to the American legal scholar Alan Westin, the very core of personal freedom in democratic societies. Nevertheless, the advent of the information revolution has rendered digital privacy increasingly susceptible to infringement and violation. This necessitates the realization of what is now known as "digital security," with the aim of protecting and promoting digital rights in general—including the right to digital privacy—through the development of secure technologies, particularly in light of the emergence of artificial intelligence.

Furthermore, the pervasive reliance on the Internet and the use of vast databanks have facilitated the storage of personal information in digital formats. Given the virtually limitless capacity of digital memory, massive amounts of personal data can now be stored and processed with ease. However, this also means that such data is vulnerable to unauthorized use, theft, and disclosure without the knowledge or consent of the data subjects—constituting a direct violation of digital privacy.

Recognizing the gravity of this phenomenon, the international community has deemed it imperative to confront the challenge both at the global and regional levels. Institutional actors have thus become increasingly aware of the threats posed by cross-border digital surveillance practices and have undertaken various measures, including the formulation of international and regional charters, to ensure the effective protection of this right.

In our study of this topic, we followed the descriptive approach by analyzing the texts of international agreements that protect the right to privacy and trying to make them consistent and in harmony with what information technology is witnessing today.

Although a number of legal instruments in the realm of human rights address privacy concerns, the current normative framework has yet to keep pace with the accelerating advancements in digital technology. While no binding global convention specifically governs digital privacy to date, significant international efforts have been made to establish protective mechanisms and promote state accountability in this domain.

Hence, the central research question addressed in this study may be formulated as follows: **have international conventions been able to accommodate emerging digital violations?**

Chapter One: The Conceptual and Legal Framework of the Right to Digital Privacy

The contemporary world is witnessing an unprecedented digital and technological revolution. Information technology has become deeply interwoven into the fabric of daily human existence. In light of these transformations, international law has expanded the scope of human rights to encompass what are now termed digital rights—a new generation of rights enabling individuals to access and engage with digital information through smart technologies.

Section One: The Concept of the Right to Digital Privacy

Technological progress has introduced new modes of communication fundamentally reliant on the Internet and information and communication technologies (ICTs). These developments have dramatically increased the circulation and exploitation of personal data, exposing users to unprecedented risks of intrusion and unauthorized use of their private information—constituting, thereby, a violation of their digital privacy.

Subsection 1.1: The General Framework of the Right to Privacy

Ahmed Fathi Sorour defines the right to privacy as: “The right to adopt personal conduct shielded from interference by the authorities or others, with the aim of safeguarding the confidentiality of such conduct”¹. Dr. Ramsis Behnam characterizes it as: “An individual’s right to direct their own life within the universe that surrounds them”².

Broadly speaking, the right to privacy denotes the entitlement to exclude others from the sanctity of one’s private life. It encompasses the right to personal integrity, the right to live peacefully, and the right to be free from unjustified scrutiny. The right to privacy, therefore, is intimately linked to the concept of personal liberty³.

The Council of Europe’s Committee of Experts on Human Rights has acknowledged, upon surveying various legal and doctrinal sources, that no universally accepted definition of the right to privacy currently exists—whether in legislative, judicial, or doctrinal frameworks, at either the domestic or international level⁴.

Traditionally, the right to privacy encompasses the inviolability of one’s home, correspondence, and familial and emotional life. This right is marked by the following characteristics:

- **Breadth:** It spans both the material and moral dimensions of personality, thereby guaranteeing the individual a wide array of fundamental entitlements.
- **Freedom:** As a central component, it ensures that individuals may exercise autonomy in their private lives.

The aforementioned Committee reaffirmed that, despite extensive scholarly and legal engagement, there remains a lack of consensus regarding a unified definition of this right in both national and international legal systems^{5 - 6}.

Subsection 1.2: Defining Digital Privacy

There exists a multiplicity of definitions concerning digital privacy. One school of thought contends that digital privacy encompasses all facets of life that fall outside the realm of public life, which is understood as that which unfolds in the presence of, or is accessible to, the general public⁷.

Another perspective conceptualizes digital privacy as a “*sphere of secrecy*”—a protected zone over which the individual exercises exclusive authority to exclude others⁸ .

Following the monumental rise of digital technologies, the notion of privacy has become intricately bound to the digital environment. There now exists an undeniable nexus between individual privacy, computer systems, and databases—systems that often entail significant intrusions into private life. Some scholars have gone so far as to liken current technological practices to a *colonization of privacy*⁹ .

Digital privacy may thus be defined as the protection of personal data disseminated and processed through digital means. Such data may include email addresses, personal photographs, and all other types of information exchanged online through any form of digital communication¹⁰ .

The right to digital privacy is therefore inherently linked to informational systems and their applications. Given that these systems now occupy a central role in the personal sphere of individuals, the concept of digital privacy has dominated legal discourse since the 1960s¹¹.

Section Two: The Impact of the Digital Revolution on the Right to Digital Privacy

The digital technological revolution has engendered unprecedented legal challenges to the human right to privacy. Cyberspace, artificial intelligence applications, and digital platforms—including the Internet, social media, and mobile devices—have facilitated the instantaneous availability and dissemination of data and personal information at an unparalleled scale.

States, individuals, institutions, and corporations are increasingly utilizing these technologies in the absence of clearly defined legal constraints—both domestically and transnationally—thereby infringing upon individuals’ privacy rights amidst the exigencies of the digital age. This has prompted the international community to mobilize in order to establish normative frameworks that safeguard the human right to privacy in the digital era.

Subsection 2.1: Factors Contributing to Violations of the Right to Privacy

Information technology presents manifold threats to digital privacy, primarily due to the intricate entanglement between the Internet and the personal spheres of individual users, particularly through the collection, storage, and processing of private data.

Among the principal factors contributing to the infringement of privacy are the following:

1. Factors Related to Data and Information

Data or information privacy is intrinsically linked to the safeguarding of individuals’ personal information, through mechanisms that prevent unauthorized access, tampering, or destruction. It entails ensuring that individuals retain control over their own data. However, the mere storage of personal data does not render it immune to unauthorized circulation or disclosure, thus exposing it to violations of confidentiality and privacy¹².

A. Unauthorized Access to Automated Data Processing Systems

Automated data processing refers to the ensemble of operations conducted on data through an information system, encompassing functions such as recording, storing, retrieving, deleting, and compiling. As elaborated in the Explanatory Report to the 2001 Budapest Convention on Cybercrime, unauthorized access involves intellectual engagement by an individual who unlawfully infiltrates a digital system with the intent to compromise it¹³.

B. Deliberate Attacks on Automated Data Processing Systems

These consist of direct assaults on digital communication systems, typified by hacking attempts that involve accessing personal data stored on hard drives—data often downloaded from the Internet—and violating its sanctity. Such unauthorized entry presupposes a connection between the physical individual and the digital network.

2. Factors Related to Computer Memory Capacity

Computer memory allows for the storage of massive volumes of data and includes a multitude of applications and executable programs. However, the excessive accumulation of data may result in its misappropriation, theft, or misuse. Given the boundless storage capacity of modern memory systems, vast troves of personal data are vulnerable to exploitation by malicious actors, thereby threatening the digital privacy of individuals¹⁴.

Subsection 2.2: Forms of Infringement upon the Right to Digital Privacy

Violations of digital privacy assume various forms, ranging from breaches involving databanks to the deployment of malicious software such as viruses. Though the means differ, the end result remains the same: the erosion of individual digital privacy, accompanied by the unauthorized dissemination of personal data.

1. The Internet and Databanks as Tools for Digital Privacy Infringement

The Internet and databanks facilitate the storage and management of files and information by both private entities and individuals. The increasing reliance on online platforms has enhanced the speed and efficiency of data access and archiving. However, these databanks, by virtue of collecting and storing vast amounts of personal data, have become fertile grounds for digital privacy violations—including the hacking of email accounts, disclosure of sensitive financial information (such as banking credentials), and the theft of credit card numbers.

2. The Threat of Computer Viruses to Digital Privacy

A virus is a deliberately programmed piece of code designed to inflict maximum harm upon computer systems. It is characterized by its ability to self-replicate by attaching to other programs and propagating across systems, giving the illusion of autonomous reproduction.

Viruses may spread from one system to another via magnetic disks or through global telecommunication networks. Their impact on privacy is substantial, as they can corrupt or destroy personal data stored on infected devices¹⁵.

Chapter Two: International and Regional Recognition of the Right to Digital Privacy

The collective efforts of States at both the international and regional levels have converged toward safeguarding and institutionalizing the right to privacy, particularly through the enactment of legal frameworks that align with the evolving nature of digital privacy.

This includes the revision of legislative, procedural, and regulatory instruments in order to ensure the effective protection of individuals' privacy in the digital age, and to establish adequate safeguards that render this right compatible with contemporary technological and digital transformations.

Section One: The International Protection and Institutionalization of the Right to Digital Privacy

The right to privacy is considered an inherent and inalienable human right. It has therefore received considerable attention at both the national and international levels as a constitutionally guaranteed freedom. However, the digital revolution has intensified infringements upon this right, placing its protection at the center of legal and human rights discourse.

Today, one of the most pressing legal challenges lies in achieving a balance between fundamental rights and virtual environments, and in formulating binding international guarantees to secure this right within public international law. Accordingly, States now bear an affirmative duty to uphold the right to privacy, criminalize its violations, and counter infractions occurring within the digital domain.

Among the most significant steps taken at the international level are the following:

Subsection 1.1: United Nations General Assembly Resolution 68/167 (2013)

The exponential growth of digital technologies, including the rapid proliferation of information and communication technologies—now deeply ingrained in the daily lives of individuals—has empowered States, institutions, and private actors to engage in surveillance activities, intercept communications, and harvest personal data, often without the knowledge or consent of the data subjects. This reality has deeply affected a wide spectrum of human rights, most notably the right to privacy.

In response, the United Nations General Assembly adopted Resolution 68/167, entitled *The Right to Privacy in the Digital Age*. Endorsed by 57 Member States, the resolution affirms that individuals' rights offline must also be protected online. It calls upon all States to respect and safeguard the right to privacy in the context of digital communications.

The resolution also urges States to review and revise their surveillance-related laws, policies, and practices—particularly those involving the interception of communications and the collection of personal data—emphasizing the necessity of full and effective compliance with their international human rights obligations.

Additionally, the General Assembly requested the Office of the United Nations High Commissioner for Human Rights (OHCHR) to submit to the Human Rights Council at its 27th session and to the General Assembly at its 69th session a comprehensive report addressing the protection and promotion of privacy in the context of domestic and extraterritorial surveillance, digital communication interception, and the bulk collection of personal data. The report was to include expert views and recommendations for consideration by Member States.

Resolution 68/167 reiterates that international human rights law provides the universal normative framework for evaluating any interference with the right to privacy.

Article 12 of the Universal Declaration of Human Rights stipulates that: “*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.*”

Similarly, Article 17 of the International Covenant on Civil and Political Rights (ICCPR), ratified by 167 States to date, provides that: “*No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor*

and reputation.” Moreover, the article mandates that “Everyone has the right to the protection of the law against such interference or attacks.”

Subsection 1.2: Report of the United Nations High Commissioner for Human Rights on the Right to Digital Privacy

This report explores key legal dimensions of the right to privacy in light of the evolution of digital technologies, focusing on the challenges of ensuring privacy in the digital era. It provides a detailed review of emerging State surveillance practices, recognizing that the formation of customary international law may originate in consistent and general State practice.

The report surveyed the legal frameworks and surveillance practices of 29 States, 5 regional and international organizations, 3 national human rights institutions, and 16 non-governmental organizations, offering an empirical foundation for the articulation of international legal norms concerning digital privacy.

Subsection 1.3: Report of the Special Rapporteur on the Right to Privacy, Human Rights Council, April 2015

In April 2015, the Human Rights Council appointed Mr. Joseph Cannataci as Special Rapporteur on the Right to Privacy, with a mandate to examine and report on violations of the right to privacy in the digital age.

In a subsequent report to the United Nations General Assembly, the Special Rapporteur offered a series of legal and policy recommendations aimed at strengthening the protection of privacy rights in the twenty-first century. In March 2016, he introduced a Ten-Point Action Plan for developing a coherent and comprehensive definition of the right to privacy in the digital age. The Plan addressed:

- The need to raise awareness regarding the risks facing personal data and information.
- The disclosure of procedural safeguards and technological measures to ensure data protection.
- The mitigation of harms resulting from privacy violations.
- The necessity of fostering a transparent and sustained dialogue among stakeholders concerning digital privacy rights¹⁶.

Furthermore, paragraph 3 of the Resolution reaffirmed that the same rights individuals enjoy offline must be fully protected online—including the right to privacy¹⁷.

Due to the lack of international consensus regarding the threshold for unlawful or arbitrary interference with privacy, the Human Rights Council requested the High Commissioner for Human Rights to submit a detailed report on the protection and promotion of privacy in the context of technological developments¹⁸.

Section Two: The Regional Protection of the Right to Digital Privacy

At the regional level, international legislative frameworks have increasingly focused on safeguarding the right to digital privacy in virtual spaces. Numerous conventions, charters, and legal reports have been adopted to institutionalize this right amidst rapid technological advancement—advancements that have, in many cases, facilitated serious violations of privacy. The escalation of such intrusions necessitated the development of a robust legal infrastructure for regional protection.

Subsection 2.1: The Role of Regional Conventions in Safeguarding Digital Privacy

The technological revolution has significantly amplified infringements upon individuals' digital privacy, thus threatening their personal security, dignity, and autonomy in cyberspace. In response, regional efforts have intensified to establish legal mechanisms to counter these threats and preserve fundamental privacy rights.

1. The 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data

This pioneering convention sought to encourage European States to enact domestic legislation responsive to the emerging technological landscape. It aimed to establish legal safeguards to ensure the protection of the right to privacy in the digital realm, especially in light of the increasing and potentially limitless threats to the rights and freedoms of individuals. As a result, various legal frameworks have been adopted by signatory States to regulate the processing and protection of personal data in accordance with evolving ICT developments.

2. The 2001 Budapest Convention on Cybercrime

Adopted in 2001 following the completion of the Draft Convention on Cybercrime on 20 April 2000, this treaty represents the first binding international instrument aimed at combating computer-related crimes. It introduced a comprehensive framework that includes:

- The establishment of legal procedures for identifying and prosecuting cyber offenders.
- The provision of investigative tools for detection, search, and seizure.
- The preservation of a balance between law enforcement efficacy and the protection of human rights.
- The promotion of cross-border cooperation in combating cybercrime.

Significantly, the Budapest Convention has reinforced international and regional collaboration in the fight against digital criminality¹⁹.

3. The 2010 Arab Convention on Combating Information Technology Offenses

Signed on 21 January 2010, this Arab regional instrument criminalized unlawful access to personal data and all related forms of digital privacy violation. Article 14 of the Convention explicitly penalizes any infringement of privacy conducted through information technologies²⁰.

The Convention aims to enhance and reinforce inter-Arab cooperation in combating information technology crimes, thereby protecting national security, public interest, and the integrity of Arab societies and individuals. Rooted in shared ethical and religious values, and mindful of the principles of Islamic law and the collective human heritage of the Arab world, the Convention calls for a unified criminal policy to counter cybercrimes, with due respect for public order and existing regional and international human rights commitments²¹.

4. Algeria's position on the Arab Convention on Combating Information Technology Crimes 2010

Algeria acceded to and officially ratified the Convention. Algeria signed the Convention on December 21, 2010, and then ratified it by Presidential Decree No. 14-252 dated September 8, 2014. It subsequently entered into force for Algeria as one of the ratifying states

This means that Algeria has adopted an Arab framework for cooperation in combating cybercrime, particularly in the areas of criminalization, investigation, judicial cooperation, and mutual assistance among Arab states.

Its position is also consistent with its domestic legislation, especially Law 09-04 concerning the prevention and combating of crimes related to information and communication technologies.

It can be said that "Algeria has taken a position in support of the Arab Convention on Combating Information Technology Crimes of 2010".

Subsection 2.2: Reports and Documents Issued by the European Union

A series of official reports and legal documents have been published by the European Union, all of which converge on the objective of protecting digital privacy and preventing the misuse of personal data in cyberspace. Among the most important instruments are the following:

1. European Parliament Report on Telecommunication Systems

This report articulated the collective position of EU Member States regarding information security, reaffirming the individual's right to privacy as guaranteed under the European Convention on Human Rights of 1950.

The report also cited precedents from the European Court of Human Rights, which ruled that the interception of communications—even if permitted by domestic law—constitutes a serious breach of Article 8 of the Convention when carried out arbitrarily or disproportionately. It further emphasized that permanent surveillance conducted by intelligence agencies constitutes a violation of the principle of proportionality embedded in the Convention.

Although the Convention does not explicitly refer to the technical dimensions of telecommunication or digital security, such protections are implicitly provided under Article 8²².

2. The General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) represents a landmark legal instrument in the domain of data protection and privacy within the European Union (EU). Enacted as Regulation (EU) 2016/679, it came into full force and effect on 25 May 2018, thereby repealing the Data Protection Directive 95/46/EC, which had previously governed the regulation of personal data within the EU.

Unlike its predecessor, which required transposition into national legislation by each Member State, the GDPR functions as a directly binding regulation, ensuring a harmonized and unified legal framework across all EU countries. Its scope extends far beyond the geographic boundaries of the European Union. In fact, any entity—whether public or private, governmental or corporate—regardless of its physical location, that processes the personal data of individuals located within the EU, falls under the regulatory ambit of the GDPR. This extraterritorial reach constitutes one of its most groundbreaking features, establishing jurisdictional authority based on the data subject's location rather than the data controller's domicile.

The primary objective of the General Data Protection Regulation (GDPR) lies in the consolidation and reinforcement of the fundamental rights and freedoms of individuals, particularly in the context of the data-driven and interconnected digital landscape. Enacted in response to the increasing complexity of data processing technologies and the transnational nature of information flows, the

GDPR serves as a legal bulwark against arbitrary, opaque, and exploitative practices involving personal data.

At its core, the GDPR is designed to safeguard personal data throughout its entire lifecycle—from the moment of collection to its processing, storage, and eventual transfer, whether domestic or cross-border. In doing so, it reshapes the balance of power between data subjects and data controllers by codifying a set of binding legal obligations on organizations and public authorities that handle personal information.

These obligations include principles such as:

- Lawfulness, fairness, and transparency: Data must be processed in a manner that is lawful and comprehensible to the individual concerned.
- Purpose limitation: Data must be collected for specified, explicit, and legitimate purposes.
- Data minimization: Only data necessary for the intended purpose should be collected and retained.
- Accuracy: Data controllers must ensure that personal data is kept accurate and up to date.
- Storage limitation: Data should not be retained longer than necessary.
- Integrity and confidentiality: Adequate technical and organizational safeguards must be in place to prevent unauthorized access, alteration, or loss.

Simultaneously, the General Data Protection Regulation (GDPR) grants a comprehensive suite of enforceable rights to data subjects—natural persons whose personal data is processed—thereby enhancing individual autonomy and reinforcing informational self-determination.

These rights constitute a cornerstone of the regulation and reflect a paradigm shift in data protection philosophy, transitioning from a controller-centric approach to one that is fundamentally data subject-oriented.

The GDPR recognizes that in the context of pervasive data collection and algorithmic processing, individuals must be endowed with legal tools to access, challenge, and control the ways in which their personal data is handled. To this end, the regulation codifies the following principal rights:

1. Right of Access (Article 15) : Data subjects have the right to obtain confirmation from data controllers as to whether their personal data is being processed. If so, they are entitled to access the data and receive supplementary information about the purposes of processing, categories of data, recipients, retention periods, and the existence of automated decision-making, including profiling.
2. Right to Rectification (Article 16); This right empowers individuals to request the correction of inaccurate personal data or the completion of incomplete information, thus ensuring the accuracy and reliability of personal records.
3. Right to Erasure – “Right to be Forgotten” (Article 17): Data subjects may request the deletion of their personal data in specific circumstances, such as when the data is no longer necessary for the purposes for which it was collected, if consent is withdrawn, or if the processing is unlawful. This right balances individual dignity with the public’s interest and freedom of expression.

4. Right to Restriction of Processing (Article 18): In certain situations, individuals can request that data processing be restricted—meaning the data may only be stored and not further processed—particularly when the accuracy of the data is contested or the processing is unlawful but erasure is not desired.
5. Right to Data Portability (Article 20): This innovative right allows data subjects to receive their personal data in a structured, commonly used, and machine-readable format and to transmit that data to another controller, thereby enhancing data interoperability and user choice in the digital marketplace.
6. Right to Object (Article 21): Data subjects may object to the processing of their data for purposes based on legitimate interests or tasks carried out in the public interest, as well as for direct marketing. Controllers must cease processing unless compelling legitimate grounds override the individual's rights.
7. Rights Related to Automated Decision-Making and Profiling (Article 22): Individuals are entitled not to be subject to decisions based solely on automated processing, including profiling, which produce legal effects or similarly significant consequences. Where such processing is necessary or based on explicit consent, appropriate safeguards—such as human intervention—must be in place.

Collectively, these rights aim to recalibrate the balance of informational power in favor of the individual, ensuring that personal data is not simply an economic asset or institutional resource, but a manifestation of identity and autonomy. The GDPR thereby establishes not only procedural rights but also substantive protections aligned with the evolving ethical, technological, and human rights dimensions of the digital age.

By articulating these rights and pairing them with stringent compliance requirements, the GDPR promotes a legal culture of accountability, transparency, and respect for individual autonomy. It obliges data controllers and processors not only to respect these rights but also to demonstrate proactive compliance through documentation, data protection policies, risk assessments, and, where necessary, the appointment of Data Protection Officers (DPOs).

In this sense, the GDPR does not merely regulate data processing—it redefines the digital rights framework for individuals, positioning data protection as a central pillar of human dignity and democratic participation in the information age.

Moreover, the GDPR imposes strict consent requirements, mandating that consent be freely given, specific, informed, and unambiguous, and that individuals must be able to withdraw such consent at any time without adverse consequences.

One of the central mechanisms introduced by the GDPR is the principle of accountability, which obliges data controllers to not only comply with the regulation but also to demonstrate such compliance. This is operationalized through detailed documentation requirements, Data Protection Impact Assessments (DPIAs), and the mandatory appointment of Data Protection Officers (DPOs) in certain contexts.

In terms of enforcement, the GDPR empowers national supervisory authorities—such as the CNIL in France or the ICO in the United Kingdom—to investigate data breaches, impose corrective measures, and issue substantial administrative fines. These penalties can reach up to €20 million or 4% of the global annual turnover of the infringing entity, whichever is greater.

The GDPR also plays a critical role in regulating international data transfers, ensuring that personal data exported from the EU to third countries enjoys an adequate level of protection. Mechanisms such as Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs) have been codified as lawful tools for cross-border data exchanges.

In conclusion, the GDPR serves as the cornerstone of digital rights protection in the EU, reflecting a comprehensive legal response to the complex challenges posed by data-driven technologies. It not only reinforces the individual's control over personal information but also sets an international benchmark for data privacy standards globally.

Its primary objectives are to simplify, standardize, and modernize the legal framework for data protection, ensuring that individuals retain full control over their personal information within the digital ecosystem and that their rights and freedoms are respected at all stages of data processing²².

Conclusion:

International legal norms have formally recognized the right to privacy, as enshrined in various international instruments, thereby establishing a general legal framework for its protection. However, the unprecedented rise of digital technologies and the exponential reliance on the Internet have transformed the nature of this right, integrating it into the broader paradigm of the digital age.

The right to digital privacy now faces profound and evolving challenges in virtual environments, particularly due to the absence of a binding international legal regime specifically regulating its scope. As a result, this right remains vulnerable to infringement, exploitation, and misuse—often without the knowledge or consent of the individuals concerned.

Digital privacy has emerged as one of the most essential components of human rights in the modern technological landscape. While international human rights law, through its core instruments and the efforts of both global and regional organizations, has affirmed the legal status of this right, it must be emphasized that no circumstance justifies the violation of fundamental human rights and freedoms, nor their misuse in ways that contravene international legal principles.

Recommendations:

1. The principal challenge confronting the right to privacy in the digital age lies in the absence of binding and clearly defined legal norms tailored to address the specificities of digital technologies.

While the international legal community has long recognized the right to privacy as a fundamental human right—most notably through instruments such as the Universal Declaration of Human Rights (Article 12) and the International Covenant on Civil and Political Rights (Article 17)—these texts were conceived in an era that did not foresee the profound transformations brought about by digital infrastructures, big data analytics, machine learning, and cross-border data transfers.

2. Consequently, existing international norms, although conceptually robust, are often technologically agnostic, failing to articulate the precise obligations of state and non-state actors in managing the lifecycle of personal data.

The rapid proliferation of smart technologies, ubiquitous surveillance capabilities, and algorithmic decision-making mechanisms has created legal vacuums that are readily exploited in both private and public sectors. Without a universally binding and technologically adaptive treaty governing digital privacy, protection remains fragmented and heavily dependent on national interpretations and regional instruments, such as the EU's General Data Protection Regulation (GDPR). These

disparities expose individuals to uneven standards of protection, particularly in jurisdictions lacking adequate legislative and enforcement capacities.

2. As communication technologies continue to evolve, the role of the State will be increasingly vital in ensuring that these technologies are deployed in a manner consistent with international human rights obligations.

In the face of evolving digital architectures and increasingly sophisticated forms of surveillance—ranging from metadata mining to facial recognition and behavioral profiling—the State must transcend its traditional regulatory functions and assume a proactive, multi-dimensional role.

This includes not only the adoption of domestic legislation aligned with international human rights standards but also the establishment of independent oversight bodies capable of scrutinizing governmental and corporate practices.

Furthermore, States must invest in legal and technical expertise to engage meaningfully in international norm-making processes, particularly within bodies such as the United Nations Human Rights Council, the International Telecommunication Union (ITU), and other multilateral platforms addressing the intersection of digitalization and human rights.

States are also expected to strike a careful balance between national security imperatives and the preservation of individual rights. The invocation of cybersecurity concerns, counter-terrorism efforts, or public order must not become a pretext for excessive and disproportionate data collection or surveillance.

The principles of necessity, legality, proportionality, and legitimate aim must be systematically integrated into both legal frameworks and technological designs. Importantly, this duty is not limited to government action alone; States must also regulate private entities, especially large transnational technology corporations that exercise quasi-sovereign control over data ecosystems, often operating beyond the effective reach of domestic laws.

In sum, the future of privacy protection hinges on state responsiveness, normative innovation, and global cooperation. The establishment of a coherent, enforceable, and human rights-centered international legal regime for digital privacy remains not only a legal necessity but a moral imperative in preserving dignity, autonomy, and democratic integrity in the 21st century.

Suggestions:

1. Given the cross-border nature of the digital revolution and its legal implications, States must adopt comprehensive domestic legislation to protect the right to privacy. Such legislation should articulate both substantive and procedural dimensions of privacy protection in the digital age.
2. Governments and public institutions must adhere strictly to the limitations imposed by international human rights instruments, particularly when engaging in surveillance activities or requesting access to personal data held by private entities. These obligations require scrupulous compliance with the principles of necessity, legality, and proportionality.
3. States should establish continuous and inclusive dialogue with relevant stakeholders—including civil society organizations, the private sector, and data protection authorities—in order to raise awareness, develop best practices, and ensure a balanced approach between national security imperatives and the inviolability of individual privacy in the digital sphere.

4. The need to create a balance between criminalizing cyber activities, exchanging electronic evidence, and protecting the right to privacy.
5. Activating an international platform for exchanging information and evidence, sharing electronic evidence, and protecting victims while ensuring the protection of human rights online.

Citations:

1. Ahmed Fathi Sorour, *The Criminal Protection of Private Life*, Cairo, Dar Al-Nahda Al-Arabiya, 1986, p. 34.
2. Samuel D. Brandeis and Louis D. Warren, *The Right to Privacy*, *Harvard Law Review*, 1890, p. 23.
3. Marouk Nasreddine, *The Right to Privacy*, *Journal of the Faculty of Islamic Sciences (Al-Sirat)*, Year 04, Issue 07, June, p. 75.
4. Privacy is an inherent human right and a fundamental pillar for the establishment of democratic societies in preserving human dignity. It is essential for safeguarding dignity and supports other rights such as freedom of expression, access to information, and freedom of association, all of which are affirmed by international human rights law. – Mohamed Hassan Emad Makawy, *Digital Privacy in International Law and Conventions*, *Journal of Media Research and Studies*, Issue 20, 2022, p. 22.
5. Kazem Al-Sayyid Atiyah, *The Criminal Protection of the Accused's Right to Privacy – A Comparative Study between Egyptian, French, American, and English Law*, Dar Al-Nahda Al-Arabiya, 2007, p. 60.
6. Abeer Hassan Al-Obaidi, *The Human Right to Privacy in the Context of the Digital Revolution*, *Journal of Jurisprudential and Legal Studies*, Issue 44, Kingdom of Saudi Arabia, January 2024, p. 1075.
7. R. Badinter, *Le droit au respect de la vie privée*, JCP, Paris, 1968, doct. No. 2136; R. Gassin, *L'atteinte à la vie privée*, Dalloz Penal, p. 6.
8. J. Carbonnier, *Droit Civil: Les Personnes. Personnalité, Incapacité, Personnes Morales*, Paris, Coll. Thémis Droit, PUF, 1995, p. 254.
9. Mokhtar Shaalal, *The Right to Privacy in Digital Space and Its Protection under International Law – Protection of Facebook Users: A Case Study*, Doctoral Thesis, University of Oran 1, 2022–2023, p. 64.
10. Paul M. Schwartz and Daniel J. Solove, *Principles of the Law: Data Privacy*, The American Law Institute (ALI), 2020, p. 121.
11. Ibid., p. 78.
12. Nasima Bathi, *The Crime of Unauthorized Access or Stay in an Information System*, *Journal of Legal and Political Jurisprudence*, Vol. 1, No. 1, p. 77.
13. Afifi Kamel Afifi, p. 269.
14. Toni Issa, *The Legal Organization of the Internet – A Comparative Study in Light of Domestic Laws and International Conventions*, Halabi Legal Publications, Beirut, 2001, p. 169.
15. Walid El-Sayed Salim, *Privacy Guarantees on the Internet*, New University House, Alexandria, 2012, p. 209.
16. Lassel Bent Nabi Yasmine and Nabil Mogaddar, *The Right to Digital Privacy*, *Journal of Future Studies in Legal and Political Affairs*, Vol. 5, No. 01, 2021, p. 7. Juliane Damen, Lena Kohler, Sean Woodard, *The Human Right of Privacy in the Digital Age*, Universitasverlag Potsdam, 2017, p. 80.
17. UN 2015b, A/HRC/28/L.27, 3f; and UN 2016a, A/HRC/31/64, 18f.

18. *The Right to Privacy in the Digital Age*, Office of the High Commissioner for Human Rights, 27th Session, 30 June 2014, pp. 6–7.
19. Mokhtar Shaalal, op. cit., p. 142.
20. Article 14 of the *Arab Convention on Combating Information Technology Offenses*, 2010.
21. Preamble of the *Arab Convention on Combating Information Technology Offenses*, 2010.
22. <https://support.kaspersky.com/kpc/1.0/ar-AE/192969.htm>

Bibliography:

A – Books:

1. Ahmed Fathi Sorour, *The Criminal Protection of Private Life*, Cairo, Dar Al-Nahda Al-Arabiya; 1986.
2. Kazem Al-Sayyid Atiyah, *The Criminal Protection of the Accused's Right to Privacy – A Comparative Study between Egyptian, French, American, and English Law*, Dar Al-Nahda Al-Arabiya; 2007.
3. Walid El-Sayed Salim, *Privacy Guarantees on the Internet*, New University House, Alexandria; 2012.
4. Toni Issa, *The Legal Organization of the Internet – A Comparative Study in Light of Domestic Laws and International Conventions*, Halabi Legal Publications, Beirut; 2001.
5. R. Badinter, *Le droit au respect de la vie privée*, JCP, Paris; 1968, doct. No. 2136.
6. R. Gassin, *L'atteinte à la vie privée*, Dalloz Pénal; 1974.
7. J. Carbonnier, *Droit Civil – Les Personnes. Personnalité, incapacité, personnes morales*, Paris, Coll. Thémis Droit, PUF; 1995.
8. Juliane Damen, Lena Kohler, Sean Woodard, *The Human Right of Privacy in the Digital Age*, Universitasverlag Potsdam; 2017.
9. Paul M. Schwartz and Daniel J. Solove, *Principles of the Law: Data Privacy*, The American Law Institute (ALI); 2020.

B – Theses:

- Mokhtar Shaalal, *The Right to Privacy in Digital Space and Its Protection under International Law – Protection of Facebook Users: A Case Study*, Doctoral Thesis, International Law, University of Oran 1; 2022–2023.

C – Journal Articles:

1. Nasima Bathi, *The Crime of Unauthorized Access or Stay in an Information System*, Journal of Legal and Political Jurisprudence, Vol. 1, No. 1; Year Unknown.
2. Marouk Nasreddine, *The Right to Privacy*, Journal of the Faculty of Islamic Sciences (Al-Sirat), Year 04, Issue 07, June; 2003.
3. Lassal Bent Nabi Yasmine, Nabil Mogaddar, *The Right to Digital Privacy*, Journal of Future Studies in Legal and Political Affairs, Vol. 5, No. 01; 2021.
4. Mohamed Hassan Emad Makawy, *Digital Privacy in International Law and Conventions*, Journal of Media Research and Studies, Issue 20; 2022.

D – International Legal Instruments:

1. *Universal Declaration of Human Rights*; 1948.
2. *Arab Convention on Combating Information Technology Offenses*; 2010.
3. *Budapest Convention on Cybercrime*; 2001.