

Electronic Risks to Rights and Freedoms (The Right to privacy as a modele)**المخاطر الإلكترونية على الحقوق والحريات (الحق في الخصوصية نموذجاً)**

DR.ouarda khelifi*

State Laboratory for Health and Nutrition Social Security

E-mail: warda.khelifi@univ-khenchela.dz

The date of Submission: 2025-01-21

The date of revision:28-06-2025

The date of publication: 10-07-2025

Abstract:

The digital revolution of the late 20th century, while bringing unprecedented connectivity and information sharing, has created significant challenges for constitutional rights and freedoms, with privacy rights being particularly vulnerable to technological advancement. As digital communications evolve, traditional privacy concepts face mounting pressure from mass surveillance, data breaches, unauthorized tracking, and personal information commodification, necessitating a comprehensive examination of technology's impact on privacy rights and their legal protections. Addressing these challenges requires a multi-layered approach that combines updated legislative frameworks, robust technological safeguards, effective regulatory oversight, and privacy-by-design principles in technology development. This coordinated effort from lawmakers, technologists, and civil society is crucial for preserving individual privacy while embracing digital advancement, ultimately maintaining human dignity and personal autonomy in an increasingly connected world.

Keywords : Right to privacy - Electronic hacking - Espionage - Disclosure of personal data.

الملخص:

أحدثت الثورة الرقمية في أواخر القرن العشرين تحولاً كبيراً في عالم الاتصال وتبادل المعلومات، لكنها في الوقت نفسه خلقت تحديات جسيمة للحقوق والحريات الدستورية، حيث أصبحت خصوصية الأفراد معرضة بشكل خاص للتأثر بالتطورات التكنولوجية، ومع تطور الاتصالات الرقمية تواجه المفاهيم التقليدية للخصوصية ضغوطاً متزايدة من جراء المراقبة الجماعية، انتهاكات البيانات، التتبع غير المصرح به، وتحويل المعلومات الشخصية إلى سلعة تجارية. وهذا يستدعي دراسة شاملة لتأثير التكنولوجيا على حقوق الخصوصية والحماية القانونية المقدمة لها. ويتطلب التصدي لهذه العديد من التحديات تجمع بين تحديث الأطر التشريعية، ضمانات تكنولوجية فعالة، ورقابة تنظيمية، ومراعاة مبادئ تصميم التكنولوجيا مع مراعاة الخصوصية منذ البداية. إن هذا الجهد المنسق من المشرعين، التقنيين، والمجتمع المدني ضروري للحفاظ على خصوصية الأفراد مع تبني التقدم الرقمي، مما يساهم في الحفاظ على الكرامة الإنسانية والاستقلالية الشخصية في عالم يزداد اتصالاً.

الكلمات المفتاحية: الحق في الخصوصية - الاختراق الإلكتروني - التجسس - الكشف عن البيانات الشخصية.

* Corresponding Author.

Introduction:

The right to the privacy of personal life is a fundamental human right that lies at the core of human dignity. This right has deep historical roots, recognized by ancient civilizations and upheld by various religious doctrines. It has also been enshrined in international law, including pivotal documents such as the Universal Declaration of Human Rights and various treaties that emphasize the importance of personal privacy.

However, since the early 1980s, the emergence and rapid advancement of information and communication technologies have transformed the way individuals interact with the world. The proliferation of computers, the internet, and digital recording devices has revolutionized daily life, creating both opportunities and significant challenges. While these technologies have enhanced communication and information sharing, they have also introduced unprecedented risks to individual privacy.

The enhancement in technological capabilities has made personal data, private information, and even images and videos readily accessible yet vulnerable. Unauthorized access, data breaches, and surveillance have become commonplace, putting the sanctity of personal privacy at grave risk. This not only undermines individual freedom but also has broader implications for societal norms and the protection of civil liberties.

In this article, we will delve into the various forms of electronic violations of the right to privacy. We will explore how scientific advancements, while beneficial in many respects, can have detrimental effects on one of the most critical human rights. This examination is crucial for understanding the complex relationship between technological progress and the safeguarding of personal privacy in an interconnected world. Through this analysis, we aim to highlight the pressing need for robust legal frameworks and creative solutions to protect individuals from the potential overreach of technology in their private lives.

As the digital landscape continues to expand and evolve, the right to privacy faces numerous unprecedented challenges. The pervasive nature of technology has led to increased vulnerabilities surrounding personal data, resulting in violations that can compromise individual dignity and freedoms. This raises critical questions: How can individuals protect their right to privacy in a technological era that prioritizes access and connectivity over confidentiality? What frameworks and measures are necessary to counteract electronic violations while still benefiting from technological advancements? The primary aim of this article is to critically examine the impact of technological advancements on the right to privacy, identifying risks and exploring solutions that can enhance the protection of individuals' personal rights in the digital age.

To answer this question, we will divide the topic into two main axes:

Axis One: The Conceptual Framework of the Right to Privacy.

Axis Two: Forms of Information Technology Violations of Privacy Rights

Axis One: The Conceptual Framework of the Right to Privacy.

The right to privacy is an essential element of individual autonomy and dignity, recognized across various cultures and legal systems throughout history. In our increasingly interconnected and digital world, the concept of privacy has gained new dimensions and complexities, prompting urgent discussions about its scope, definition, and protection. As

technological advancements reshape the fabric of daily life, the traditional boundaries of personal privacy are being challenged and, in many cases, breached.

The Conceptual Framework for the Right to Privacy

The right to privacy is one of the most fundamental and evolving rights in modern legal and societal discourse. It is deeply intertwined with human dignity, autonomy, and the protection by addressing three key aspects:

1. **The Concept of the Right to Privacy,**
2. **Historical Origins,**
3. **Legal Basis.**

First: The Concept of the Right to Privacy

Defining the right to privacy is a complex task due to its inherently subjective and dynamic nature. Privacy is not a static concept; it evolves with societal changes, technological advancements, and cultural shifts. What constitutes privacy in one society or era may differ significantly in another. For instance, the concept of privacy in a traditional, close-knit community may contrast sharply with that in a highly digitalized, individualistic society.

1. The Variability of Privacy

The right to privacy is influenced by several factors, including:

- **Cultural and Religious Beliefs:** In some cultures, privacy is closely tied to modesty and family honor, while in others, it is more about individual autonomy.
- **Customs and Traditions:** Societal norms dictate what is considered private. For example, in some societies, personal finances are private, while in others, they are openly discussed.
- **Technological Advancements:** The rise of the internet, social media, and surveillance technologies has redefined the boundaries of privacy. What was once considered private may now be publicly accessible.
- **Legal and Political Systems:** The extent of privacy protection varies depending on the freedoms granted by a country's legal framework.

Given this variability, scholars have struggled to provide a universal definition of privacy. Instead, they have offered diverse perspectives that reflect its multifaceted nature.

2. Scholarly Definitions of Privacy

Several prominent scholars have attempted to define the right to privacy, each emphasizing different aspects of the concept:

- **Scholar Nerson:**

Nerson defined privacy as *"the reservation that enables a person to not expose their personality to the public without consent, and in this way, one can enjoy peace and be left alone, meaning they can isolate themselves from people, following Christ's example, and be alone with themselves."*¹

This definition highlights the spiritual and psychological dimensions of privacy, emphasizing the need for solitude and personal reflection.

- **Scholar Cooley:**

Cooley described privacy as *"the individual's right to a peaceful life, that is, to be left*

¹-Adam Abdel Badee Adam Hassan: *The Right to Private Life and the Extent of Protection Guaranteed by Criminal Law*, Doctoral Thesis, Faculty of Law, Cairo University, 2000, p. 170.

without disturbance or anxiety."¹

This definition focuses on the emotional and mental well-being that privacy affords, underscoring its role in protecting individuals from external intrusions.

- **Robertson:**

Robertson framed privacy as *"the right of a person to live away from publicity."*²

This definition emphasizes the distinction between public and private life, suggesting that privacy allows individuals to control their exposure to the public eye.

- **Mamdouh Khalil Bahr:**

Bahr defined privacy as *"the scope within which a person can withdraw or seclude themselves from others with the intention of achieving a kind of tranquility and maintaining the confidentiality of their private life."*³

This definition introduces the idea of privacy as a *space*—both physical and metaphorical—where individuals can retreat to protect their personal lives.

3. The Evolving Nature of Privacy

The concept of privacy has undergone significant transformations over time. In pre-modern societies, privacy was often limited to physical spaces, such as homes or personal belongings. However, with the advent of modern technologies, the scope of privacy has expanded to include digital data, online activities, and even biometric information.

For example, in the digital age, privacy concerns now encompass issues like data breaches, online surveillance, and the misuse of personal information by corporations and governments. This evolution underscores the need for a flexible and adaptive understanding of privacy that can address emerging challenges.

Second: The Origins of the Right to Privacy

The right to privacy has deep historical roots, though its formal recognition as a legal concept is relatively recent.

1. Philosophical Foundations

The idea of privacy can be traced back to ancient philosophical traditions. For instance, Aristotle distinguished between the *public sphere* (the polis) and the *private sphere* (the oikos), emphasizing the importance of maintaining boundaries between the two. Similarly, Enlightenment thinkers like John Locke and Immanuel Kant highlighted the intrinsic value of individual autonomy and personal freedom, which are central to the modern concept of privacy.

2. Legal Recognition

The formal recognition of privacy as a legal right began in the late 19th century. In 1890, American lawyers Samuel Warren and Louis Brandeis published their seminal article, *"The Right to Privacy,"* in the Harvard Law Review. They argued that privacy is *"the right to be let alone"* and called for legal protections against invasive practices by the press and other entities.

This marked a turning point in the legal understanding of privacy, paving the way for its inclusion in various national and international legal frameworks.

¹-Isabelle Verdier-Buschel-Remy Prouvez, *"Utilisation des nouvelles technologies de captation de l'image et la procédure pénale"* in *Technique et droit humains* (collective work), Montchrestien, l'ex, p. 95.

²-Adam Abdel Badee Adam Hassan: Previous reference, p. 188.

³-Mamdouh Khalil Bahr: *Protection of Private Life in Criminal Law, Comparative Study*, Dar Al-Nahda Al-Arabia, Egypt, 1983, p. 168.

Third: The Legal Basis of the Right to Privacy

The right to privacy is enshrined in numerous legal instruments, reflecting its universal importance.

1. International Instruments

- **Universal Declaration of Human Rights (1948):** Article 12 states that *"No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence."*
- **International Covenant on Civil and Political Rights (1966):** Article 17 reiterates the protection of privacy against unlawful or arbitrary interference.
- **European Convention on Human Rights (1950):** Article 8 guarantees the right to respect for private and family life.

2. National Constitutions and Laws

Many countries have incorporated the right to privacy into their constitutions or legal codes. For example:

- The United States recognizes privacy through judicial interpretations of the Constitution, particularly the Fourth Amendment.
- The European Union has established comprehensive data protection laws, such as the General Data Protection Regulation (GDPR), to safeguard individuals' privacy rights.

3. Challenges in Enforcement

Despite its widespread recognition, the enforcement of privacy rights faces significant challenges. These include:

- Balancing privacy with other rights, such as freedom of expression and national security.
- Addressing the global nature of digital privacy issues, which often transcend national jurisdictions.
- Keeping pace with rapid technological advancements that create new vulnerabilities.

The right to privacy is a dynamic and multifaceted concept that reflects the complexities of human life and societal evolution. While its definition may vary across cultures and contexts, its core purpose remains the same: to protect individuals' autonomy, dignity, and personal space. As technology continues to reshape the boundaries of privacy, it is essential to develop robust legal and ethical frameworks that can adapt to these changes and ensure the continued protection of this fundamental right.

Observations on the Previous Definitions

The definitions discussed earlier reflect the **traditional concept of the right to privacy**, which primarily revolves around notions of **isolation, solitude, and seclusion**. Historically, the right to privacy emerged with a **material and physical focus**, emphasizing the protection of personal spaces such as homes and correspondence. At its inception, it was not concerned with **private information or data** as we understand it today. However, the rapid advancement of **modern technology** has fundamentally reshaped this concept, bringing it into sharper focus in relation to the **violation of automatically processed personal information**.¹ This evolution has prompted scholars to redefine the right to privacy in light of contemporary challenges. For instance:

¹-Abdelkader Amimer: *The Impact of Information Technology on the Right to Private Life*, Annals of University of Algiers 1, Issue 01, 2020, p. 446.

- *"It is the right that authorizes its holder to prevent others from intruding in any form, and it is an exclusive right that authorizes its holder to enjoy their private life alone without the interference of others."*¹
- It has also been defined as: *"The right of individuals to be protected from interference in their affairs and their families' affairs by direct physical means or through the publication of information about them."*²

These modern definitions highlight the **dynamic nature of privacy**, which now encompasses both **physical and informational dimensions**.

Elements of the Right to Privacy

Through the **new concept of the right to privacy**, we can identify several key elements:

1. **Withdrawal from the Surrounding Environment:**

The right to privacy is closely associated with the ability to **withdraw from the public sphere** and seek **isolation or seclusion**. This element underscores the importance of securing the **personal aspect of life** from any form of interference or breach.³

2. **Exclusive Authority to Object:**

Individuals possess the **exclusive authority to object** to any actions that target their private life. This empowers them to **control access** to their personal information and spaces.

3. **Potential Violators:**

Violations of privacy can be committed by **individuals, groups of individuals, or specific entities** (e.g., corporations, governments). This broad scope reflects the **diverse threats** to privacy in the modern world.

4. **Moral and Legal Framework:**

The right to privacy is both a **moral and legal framework** that includes:

Physical elements: Such as the inviolability of the home, confidentiality of private conversations, and secrecy of correspondence.

Spiritual elements: Such as political opinions, emotional life, and religious beliefs.

Legal Systems and the Protection of Privacy

While **all legal systems** recognize the existence of a **standalone right to privacy**, the **mechanisms and extent of protection** vary significantly across jurisdictions:

- **French Law:** Protects the right to privacy through **various mechanisms and diverse laws**, ensuring comprehensive safeguards for individuals.
- **English Law:** Traditionally, English law has been reluctant to provide **direct protection** for the right to privacy. Instead, it relies on **morals and societal ethics** to impose limits on intrusions into private life.⁴

¹-RachidSmichem: *The Right to Private Life*, Journal of Legal and Social Sciences, ZianAchour University of Djelfa, Twelfth Issue, December 2018, p. 166.

²-CherifiCherif: *The Extent of Respect for Privacy Rights in Electronic Accounts on the Internet*, Journal of Rights and Freedoms, Second Issue, 2015, p. 23.

³-Fadli Syed Ali: *Effects of Technological Development on the Protection of Rights in the European System for Human Rights Protection*, Professor Researcher Journal for Legal and Political Studies, Issue 2, 2020, p. 1640.

⁴-Abdul Latif Al-Humeim: *Respect for Private Life in Islamic Sharia and Positive Law*, Dar Emad for Publishing and Distribution, Amman, 2003, p. 17.

This divergence highlights the **cultural and legal differences** in how societies perceive and protect privacy.

Second: The Historical Development of the Right to Privacy

The right to privacy is as old as humanity itself, rooted in **divine laws** and **positive laws**.

Its historical development can be traced through key milestones:

1. Early Legal Protections:

In 1361, Britain enacted a law prohibiting peeping and eavesdropping, punishable by imprisonment.

In 1765, British Lord Camden issued a landmark decision prohibiting house searches and the seizure of private papers.¹

2. Modern Legal Discourse:

In 1890, two American lawyers, Samuel Warren and Louis Brandeis, published a seminal article advocating for the protection of privacy from media intrusion. They argued that privacy violations cause emotional pain and grief far more severe than physical harm. This article is widely regarded as the foundation of modern privacy law in America.²

The historical development of the right to privacy aligns with the conceptual framework discussed earlier. Initially, privacy was understood in physical terms, focusing on the protection of personal spaces and correspondence. However, as societies evolved and technology advanced, the concept expanded to include informational privacy. This shift reflects the dynamic and adaptive nature of the right to privacy, which continues to evolve in response to new challenges.

For example, the traditional definitions of privacy, such as those by Nerson and Cooley, emphasized solitude and seclusion. These definitions remain relevant but have been supplemented by modern interpretations that address digital privacy and data protection. Similarly, the legal frameworks discussed earlier—ranging from French law to English law—demonstrate the diverse approaches to safeguarding privacy in different cultural and legal contexts.

The right to privacy is a fundamental and evolving right that has undergone significant transformations over time. From its origins in physical and traditional concepts to its modern focus on informational and digital privacy, this right reflects the changing needs and values of societies. While legal systems differ in their approaches to protecting privacy, there is a **universal recognition** of its importance in safeguarding human dignity, autonomy, and personal freedom.

Third: The Legal Basis for the Right to Privacy

In this section of the research, we will review various constitutional and legal texts that established or included some form of protection for the right to privacy in Algeria, as follows: Article 47 of the Algerian Constitution stipulates that every individual has the right to the protection of their honor and preservation of their dignity.

¹-Seddiki Nabila: *Protection of the Right to Privacy*, Journal of Legal, Administrative and Political Sciences, Faculty of Law, Abu Bakr Belkaid University Tlemcen, Issue 06, 2008, p. 14.

²-Sawadkia Hani: *Protection of the Right to Privacy*, Journal of Legal and Political Research and Studies, Issue 03, p. 83.

Additionally, every person has the right to ensure the confidentiality of correspondence, communications, and privacy of messages in all forms.

The aforementioned rights cannot be violated except by a reasoned judicial decision.

The personal protection of information related to individuals is considered an inherent right that cannot be violated or waived. Anyone who violates these stipulated rights shall be subject to punishment.¹

In accordance with the above article, the legislator issued Law No. 18-07 dated June 10, 2018, regarding the protection of natural persons in the field of processing personal data.² Article 02 of this law emphasized that the processing of personal data, regardless of its source or form, must be carried out within the framework of respecting human dignity, private life, and public freedoms, and must not infringe upon people's rights, honor, and reputation.³

Article 47 of the Algerian Civil Code also stipulates that any individual subjected to illegal assault relating to their personal rights has the right to demand the cessation of these assaults and claim compensation for these violations.⁴

In addition to what was stated in Article 93 of the Information Law, which stipulated the necessity of respecting individuals by not violating them while ensuring their honor. It is also prohibited to violate the privacy of public figures in any form and to commit aggression against them.⁵

The Algerian Penal Code also criminalized acts that violate the right to privacy under Articles 303 bis and 303 bis 1.⁶

Axis Two: Forms of Information Technology Violations of Privacy Rights

The modern world has achieved remarkable advancements thanks to scientific and technological progress, even reaching the point of considering the possibility of living on other planets. However, some aspects of this progress have been used negatively, harming human dignity and tarnishing reputations and honor.

To address these issues, **penal systems** have criminalized actions that violate the right to privacy, and legislators have enacted laws to prevent and combat crimes related to information and communication technologies. For example, the **Algerian legislator** introduced **Law No. 09-04**⁷, which includes specific rules for preventing and addressing such crimes.

In this section, we will explore the most significant forms of **electronic violations** of the right to privacy, as follows:

First: Espionage and Its Impact on the Violation of Privacy

¹-Official Gazette of the Algerian Republic, No. 82, issued on: 15 Jumada Al-Oula 1442 AH corresponding to: December 30, 2020, p. 04.

²-Law No. 18-07 dated: 25 Ramadan 1439 corresponding to: June 10, 2018, regarding the protection of natural persons in processing personal data, Official Gazette No. 34, issued on: 25 Ramadan 1439 AH corresponding to: June 10, 2018, p. 11.

³-Article 02 of Law No. 18-07.

⁴-Order No. 75-58 dated: 20 Ramadan 1395 corresponding to: September 26, 1975, containing the amended and supplemented Civil Code.

⁵-Organic Law No. 12-05 dated: 18 Safar 1433 corresponding to: January 12, 2012, relating to Information.

⁶-Order No. 66-156 dated: 18 Safar 1386 corresponding to: June 08, 1966, containing the amended and supplemented Penal Code.

⁷-Law No. 09-04, dated August 5, 2009, containing specific rules for the prevention and combating of crimes related to information and communication technologies.

Espionage is one of the most dangerous and socially condemned practices, often intersecting with other morally reprehensible behaviors such as **gossip and slander**¹. In general, espionage involves **tracking and monitoring an individual's activities** for unlawful purposes. It can take various forms:

1. Ground Espionage

This refers to the use of **ground-based technologies** that do not rely on air frequencies or Hertz waves². It often involves **nanotechnology devices**, which are microscopic and invisible to the naked eye. A **nanometer** is a unit of measurement equal to one billionth of a meter.³

While nanotechnology has been used in fields such as **medicine, industry, and agriculture**, its impact on individual privacy has been overwhelmingly negative. Technological advancements have reached the point where **nanoscale devices** can penetrate a person's psyche and even **read their intentions**, particularly aggressive ones. These technologies have been promoted as tools for **detecting terrorist intentions** in suspects before they commit crimes. For instance, the **United States** has employed such technologies in **ports and airports** to prevent potential attacks.⁴

However, many legal experts argue that the use of **body scanners** in airports for security purposes constitutes a form of espionage, as it violates individual privacy.⁵

Additionally, the **rapid development of digital technology** has enabled espionage through **audio and visual devices**, such as cameras, recording devices, surveillance systems, and eavesdropping tools. As a result, individuals' behaviors and movements are now **recorded in audio and video** without their knowledge, regardless of their location.

2. Satellite Espionage

The launch of **satellites** has made it easier to spy on people's lives, monitor their activities, and uncover their secrets, no matter where they are. This form of espionage is often used by **states against other states, organizations, or individuals**.

3. Espionage Through Viruses

The use of **computers and mobile phones** has exposed individuals to the risk of **viruses** that can damage software, information, and emails, creating significant concerns for users.

A **virus** is a small program embedded in computer disks or drives with the intent of causing harm. It can attach itself to other programs, remain dormant for a period, and then activate to replicate and spread within the system. Viruses can **destroy programs, data, and information** stored in a computer's memory. Their damage may extend to **corrupting file directories**, making it impossible for the computer to recognize or read them again, or even **merging files** to render them useless.⁶

Viruses can also process **personal information** to extract new data through methods such as **data matching, statistical analysis, and integration of various elements**. This allows

¹-CherifiCherif, *Previous Reference*, p. 26.

²-Ben Said Sabrina: *Protection of the Right to Privacy in the Age of Technology*, Doctoral Thesis, University of Batna, 2015, p. 102.

³-Ahmed TawfiqHijazi: *Nanotechnology - The Modern Technological Revolution*, Dar Kunuz Al-Ma'rifa Al-Ilmiyya for Publishing and Distribution, Jordan, 2012, p. 11.

⁴-Ben Said Sabrina: *Previous Reference*, p. 102.

⁵-*Ibid.*, pp. 107-108.

⁶-Quoted from Cherifi, *ibid* , p. 25.

criminals to **translate an individual's life into actionable data** within seconds, which can then be used for **unlawful purposes**, such as exposing someone's past or blackmailing them.¹ These viruses pose a significant threat to individual privacy, especially when deployed by a **specific individual or entity** with the intent to **destroy personal files and information**, which are considered private matters that no one should access without permission.

4. Electronic Espionage

This refers to the **interception or capture of data** transmitted between two devices over the internet or the translation of **electromagnetic emissions** from a computer into usable data. It involves the use of **technical means** to eavesdrop on digital communications.²

Second: The Broader Implications of Digital Espionage

The rise of digital espionage has far-reaching consequences for the **right to privacy**:

- **Loss of Control:** Individuals often lose control over their personal information, as it can be accessed, manipulated, or destroyed without their consent.
- **Psychological Impact:** The knowledge that one is being monitored can lead to **anxiety, stress, and a sense of vulnerability**.
- **Legal and Ethical Challenges:** The use of advanced technologies for espionage raises **ethical questions** about the balance between **security and privacy**, as well as the need for **robust legal frameworks** to protect individuals.

The digital age has brought unprecedented challenges to the **right to privacy**, with espionage taking on new and sophisticated forms. From **ground-based nanotechnology** to **satellite surveillance** and **cyber viruses**, the threats to privacy are diverse and evolving. While technological advancements offer immense benefits, they also require **strong legal and ethical safeguards** to prevent misuse and protect individuals' fundamental rights.

Second: Hacking and Its Impact on the Violation of Privacy

The rapid technological advancements in communication tools, the increasing reliance on the internet, and the unlimited use of social media platforms such as **Facebook, Instagram, and Twitter** have led to the unexpected spread of **hacking** by unauthorized individuals. These individuals gain access to websites or remain on them for extended periods without permission.³

Hacking is defined as *"the unauthorized access to another person's computer using advanced programs that require high technical expertise and skill."*⁴

This crime is typically committed by **cybercriminals** who possess the competence and experience to infiltrate internet networks.

Third: Disclosure of Personal Data and Its Impact on the Violation of Privacy

While the **traditional concept of the right to privacy** imposes on professionals such as **lawyers, doctors, and administrators** the obligation to maintain **professional confidentiality** regarding the personal data of their clients, the accelerated pace of technological development has led to clear violations of privacy through the **disclosure of personal data**, particularly by **bank employees**.

¹-Susan Adnan Al-Ustadh: *Violation of Privacy Through the Internet (A Comparative Study)*, Damascus University Journal for Economic and Legal Sciences, Issue 03, 2013, p. 435.

²-Article 3 of the 2001 Budapest Convention on Cybercrime.

³-Rashid Hassan Hussein Ayyash: *The Crime of Hacking Information Systems and Networks*, University of Jerusalem, Palestine, 2019, p. 67.

⁴-Omar Majd Abu Bakr bin Yunus: *Crimes Arising from the Use of the Internet*, Dar Al-Nahda Al-Arabiya, Egypt, 2004, p. 331.

For example, personal data has become vulnerable to **illegal disclosure** in the context of **electronic banking transactions**. This was evident in the case of the **Swiss Bank**, where French clients affiliated with the Directorate General for Competition, Consumer Affairs, and Fraud Control attempted to **decrypt personal data** of French citizens holding accounts in the bank. The goal was to use this data in investigations related to **tax evasion**.¹

Fourth: The Algerian Legislator's Stance on Violations of the Right to Privacy

The **Algerian legislator** has classified certain actions that violate the right to privacy as **criminal offenses**, punishable by **imprisonment ranging from six months to three years** and a **fine of 50,000 DZD to 300,000 DZD**. These penalties apply to anyone who intentionally violates the privacy of individuals using any technology, including:

- **Recording, transmitting, or intercepting private or confidential conversations** without the consent of the parties involved.
- **Capturing, recording, or transmitting images** of a person in a private setting without their consent.²

The same penalties apply to:

- Anyone who **retains, stores, or makes available to the public or third parties** recordings, images, or documents obtained through the aforementioned actions.³

Despite the **criminal protections** provided by the legislator for any act that constitutes a violation of the right to privacy, regardless of the technical means used, the issue of **proof** remains a significant obstacle in prosecuting perpetrators of such crimes. This is particularly challenging since the legislator has classified these offenses as **intentional crimes**.

Conclusion:

In this research paper, we have established that the **illegal use of information and communication technologies (ICTs)** poses a significant threat to the right to privacy. The pervasive reach of these technologies has led to an alarming increase in unauthorized surveillance and the exposure of individuals' private lives to various forms of **espionage**. Intruders can now exploit technological advances to access personal data and confidential information stored on devices, email accounts, and cloud services. Moreover, **cybercriminals** have harnessed the power of social media platforms to disseminate and publicly expose sensitive information, further undermining privacy rights. Given these pressing challenges, there is an urgent need to enhance legislative, technical, and regulatory frameworks aimed at preventing such violations at both national and international levels. Governments, organizations, and individuals must collaborate to establish robust measures that effectively safeguard privacy in this digital era.

Legal frameworks must evolve to keep pace with technological advancements and the sophisticated tactics employed by those who seek to undermine privacy. Stronger data protection regulations, such as the **General Data Protection Regulation (GDPR)** in the

¹-DhahabiKhadouja: *The Right to Privacy in the Face of Electronic Violations (A Comparative Study)*, Journal of the Professor Researcher for Legal and Political Studies, Issue 8, December 2007, p. 150.

²-Article 303 bis of the amended and supplemented Penal Code.

³-Article 303 bis 1 of the amended and supplemented Penal Code.

European Union, should serve as a model for implementing comprehensive privacy laws worldwide. Countries must develop and enforce legislation that mandates transparent data handling practices and provides individuals with tools to control their personal information. In addition to legislative efforts, individuals play a crucial role in protecting their privacy. Adopting effective protection systems for personal information is vital in an era where digital threats are omnipresent. Measures such as:

- **Using Strong Passwords:** Creating complex passwords and changing them regularly can help secure accounts against unauthorized access.
- **Implementing Encryption Tools:** Encryption adds an additional layer of security to sensitive communications and files, making it difficult for intruders to access this information.
- **Utilizing Secure Networks:** Accessing the internet through trusted, secure networks can minimize the risks of data interception.

By staying informed about the latest cybersecurity threats and best practices, individuals can significantly enhance their privacy protection.

However, the fight for privacy cannot rely solely on technical and legal measures. Social awareness and education are critical components in ensuring the protection of the right to privacy. Promoting a culture of responsible electronic interaction can empower individuals to take ownership of their privacy. Increasing public awareness of the risks and consequences of privacy violations, as well as educating individuals about their rights, will foster a more informed citizenry capable of navigating the digital landscape safely.

In conclusion, while technological advancements have brought numerous benefits to society, they have also introduced significant risks to personal privacy. Addressing these risks necessitates a **multi-faceted approach** that combines legal reforms, technological innovations, and a commitment to societal awareness. This comprehensive strategy will help create a safer digital environment where the fundamental right to privacy is protected.

As we move forward in this increasingly interconnected world, it is paramount that all stakeholders—governments, organizations, and individuals—recognize the importance of privacy as a fundamental human right. By prioritizing privacy protection, we can contribute to a future where individuals feel secure in their ability to engage with technology without fear of intrusion or exploitation.

List of references:

1- Books:

- Abdul Latif Al-Humeim: *Respect for Private Life in Islamic Sharia and Positive Law*, Dar Emad for Publishing and Distribution, Amman, 2003.
- Ahmed Tawfiq Hijazi: *Nanotechnology - The Modern Technological Revolution*, Dar Kunuz Al-Ma'rifa Al-Ilmiyya for Publishing and Distribution, Jordan, 2012.
- Omar Majd Abu Bakr bin Yunus: *Crimes Arising from the Use of the Internet*, Dar Al-Nahda Al-Arabiya, Egypt, 2004.
- Mamdouh Khalil Bahr: *Protection of Private Life in Criminal Law, Comparative Study*, Dar Al-Nahda Al-Arabia, Egypt, 1983.
- Isabelle Verdier-Buschel-Remy Prouvez, "Utilisation des nouvelles technologies de captation de l'image et la procédure pénale" in *Technique et droit humains* (collective work), Montchrestien, l'ex

-Rashid Hassan Hussein Ayyash: *The Crime of Hacking Information Systems and Networks*, University of Jerusalem, Palestine, 2019.

2- Journals:

- Abdelkader Amimer: *The Impact of Information Technology on the Right to Private Life*, Annals of University of Algiers 1, Issue 01, 2020.

-Cherifi Cherif: *The Extent of Respect for Privacy Rights in Electronic Accounts on the Internet*, Journal of Rights and Freedoms, Second Issue, 2015.

-Dhahabi Khadouja: *The Right to Privacy in the Face of Electronic Violations (A Comparative Study)*, Journal of the Professor Researcher for Legal and Political Studies, Issue 8, December 2007.

-Fadli Syed Ali: *Effects of Technological Development on the Protection of Rights in the European System for Human Rights Protection*, Professor Researcher Journal for Legal and Political Studies, Issue 2, 2020.

-Rachid Smichem: *The Right to Private Life*, Journal of Legal and Social Sciences, Zian Achour University of Djelfa, Twelfth Issue, December 2018.

-Sawadkia Hani: *Protection of the Right to Privacy*, Journal of Legal and Political Research and Studies, Issue 03.

-Seddiki Nabila: *Protection of the Right to Privacy*, Journal of Legal, Administrative and Political Sciences, Faculty of Law, Abu Bakr Belkaid University Tlemcen, Issue 06, 2008,

Susan Adnan Al-Ustadh: *Violation of Privacy Through the Internet (A Comparative Study)*, Damascus University Journal for Economic and Legal Sciences, Issue 03, 2013.

3-Theses:

- Adam Abdel Badee Adam Hassan: *The Right to Private Life and the Extent of Protection Guaranteed by Criminal Law*, Doctoral Thesis, Faculty of Law, Cairo University, 2000.

-Ben Said Sabrina: *Protection of the Right to Privacy in the Age of Technology*, Doctoral Thesis, University of Batna, 2015.

4-Laws and Decrees:

- Official Gazette of the Algerian Republic, No. 82, issued on: 15 Jumada Al-Oula 1442 AH corresponding to: December 30, 2020.

-Law No. 09-04, dated August 5, 2009, containing specific rules for the prevention and combating of crimes related to information and communication technologies.

-Law No. 18-07 dated: 25 Ramadan 1439 corresponding to: June 10, 2018, regarding the protection of natural persons in processing personal data, Official Gazette No. 34, issued on: 25 Ramadan 1439 AH corresponding to: June 10, 2018.

-Order No. 75-58 dated: 20 Ramadan 1395 corresponding to: September 26, 1975, containing the amended and supplemented Civil Code.

-Order No. 66-156 dated: 18 Safar 1386 corresponding to: June 08, 1966, containing the amended and supplemented Penal Code.