journal Of Legal and Economic Studies ISSN 2602-7321/ EISSN 2773- 2649
Vol : 07 No: 01 Year: 2024 Page : 619 - 628

Recent Developments in the Concept of Protecting the Right to Privacy: A Study in Light of Latin and Anglo-Saxon Legislation

bouker rachida *, University of mostaganem, Algeria , rachida.bouker@univ-mosta.dz

Send Article Date: 18 /04/2024 Date of acceptance of the article: 10/05/2024

Abstract:

This article examines recent developments in privacy protection laws within Latin and Anglo-Saxon legal frameworks, highlighting the distinct approaches of each: comprehensive constitutional protections in Latin systems versus sector-specific legislations in Anglo-Saxon systems. It sheds light on the novel challenges posed by digital technology, which often surpass the current legal protections. The article recommends enhancing legal harmonization, updating legislative frameworks to keep pace with rapid technological advancements, and advocates for increased international cooperation and public awareness to ensure robust privacy protection in the digital age.

key words: Right to Privacy . Recent Developments ; Latin Legislation. Legal Protection

Introduction:

The right to privacy[1], often equated with the inviolability of personal life, stands as a cornerstone among the essential human rights, anchoring the broad spectrum of individual liberties that empower a person to manage their private affairs without interference. Tracing its origins to antiquity, the principle of privacy has been upheld in various religious texts, underscoring the critical need to shield individuals from undue surveillance. This concept gained formal recognition in the mid-20th century with its inclusion in the Universal Declaration of Human Rights of 1948, which explicitly safeguarded the privacy of personal spaces and

* Dr/ bouker rachida

[1] For an overview of the concept of privacy, please refer specifically to: Alessandro Acquisti , PRIVACY AND SECURITY OF PERSONAL INFORMATION ; Economic Incentives and Technological Solutions, https://www.heinz.cmu.edu/~acquisti/papers/acquisti_eis_refs.pdf

communications. Subsequently, this right has been reinforced by major international legal instruments such as the International Covenant on Civil and Political Rights, as well as by numerous national and regional statutes, all of which converge to protect aspects of private and family life, domicile, and correspondence.

The advent of information technology in the second half of the twentieth century marked a paradigm shift, embedding these technologies into the fabric of everyday life and thus reshaping the landscape of privacy. Digital communication innovations have propelled the benefits of technological globalization, integrating private life into a broader, interconnected digital framework. Nonetheless, the rapid proliferation of data-centric technologies, including artificial intelligence, poses unprecedented challenges. These technologies, while advancing human development and enhancing rights protections, also create a milieu conducive to unauthorized surveillance and digital breaches. Thus, they present complex threats to privacy, necessitating vigilant and adaptive legal responses to uphold this fundamental right in the digital age.

This study addresses the challenges facing the privacy protection system in the era of new technology, examining both Latin and Anglo-Saxon legislations. It relies on descriptive and analytical methodologies to understand the various aspects of digital privacy rights and to explore strategies for its protection through legislative texts.

The first topic: Privacy Protection in Latin Legislation

In this section, we will explore the French legal system as a model of foreign legislation, and then the Algerian legal system as a model of Arab legislation.**FIRST REQUIREMENT:**

First requirement : The Legal Landscape in France

In France, the right to privacy is constitutionally grounded in Article 2 of the Declaration of the Rights of Man and Citizen of 1789, which guarantees freedom in its various forms. It is also established in Article 66 of the Constitution of 1958, which ensures individual liberty.

Furthermore, French legislators are committed to a comprehensive level of legislative protection as stipulated in the European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. This includes rules and procedures adopted to protect the privacy of information in accordance with the European Directive on the protection of individuals during the automatic processing of data and its movement. From the 1960s to the 1970s, the Public Prosecutor at the French Council of State raised questions about the impact of information technology on public life and administrative decisions. In response, a commission was established in 1974 to propose measures that would form the basis

of the Law of January 6, 1978. This law has been amended several times since then to align with the General Data Protection Regulation (GDPR), including the roles and powers of the National Commission, and expanding the scope of sensitive data processing up to 2018[1].

On June 20, 2018, **Law No. 2018-493** on the protection of personal data was enacted, introducing further exceptions. This includes the processing of biometric data (e.g., fingerprints) necessary for access controls to workplaces, computers, and applications used there. The law also adjusts the role and authority of the National Commission on Informatics and Liberty in oversight and enforcement activities.

Since its inception, the CNIL (French National Commission on Informatics and Liberty) has supported internet users. At the end of 2014, it adopted a new label titled "Information Governance and Liberties." This label aims to define "the rules and best practices that allow an organization to manage its data in compliance with information and liberty principles." The CNIL also intervened in the context of the draft intelligence law before it was even discussed in the Council of Ministers. This proposed legislation sought to expand the intelligence services' powers regarding the data that could be collected, the individuals involved, and the duration of data retention.

The CNIL, concerned about these "much broader and more intrusive surveillance measures," issued an opinion. This opinion had an effect; the draft law was indeed amended to better regulate the conditions for obtaining and managing the data that could be collected. Additionally, a digital law is currently being drafted.

In addition to this, under the provisions of the penal code, French legislation imposes penalties for breaches of automated processing systems. It criminalizes unauthorized access to an information system, even without the intent of further malicious actions, and imposes stricter penalties if such access results in the deletion or modification of information or disrupts the operation of the information system. Unauthorized access is considered a primary offense in the context of serious threats and attacks on the security of information systems, affecting the privacy, integrity, and availability of information.

Additionally, the French legislator addresses in other sections of the Penal Code the criminal protection against specific violations of private life[2].

On the civil protection side of the right to privacy, French legislators have outlined in Article 9 of the Civil Code the conditions under which a judge may take necessary preventive measures to protect the right to privacy. It states, "Every person

[1] Law No. 2018-493 of June 20, 2018, on the protection of personal data

[2] For more details on these crimes, particularly see: Dr. Omar Aboul Fotouh Abdel Azim Al-Hammami, Criminal Protection of Electronically Recorded Information - A Comparative Study, Dar Al-Nahda Al-Arabiya, Cairo, 2010, p. 830

has the right to respect for his or her private life, and judges may take all necessary measures such as guardianship and sequestration, among other actions, to prevent or stop any infringement of this privacy. The judge handling urgent matters may resort to these measures whenever urgent conditions are met, without prejudice to the individual's right to compensation for any harm suffered".

Second requirement :The Legal Landscape in Algeria

Like other constitutions around the world, the Algerian Constitution has, since the inception of the modern state and its three branches of government, acknowledged the sanctity of private life. As individuals entrust the state with the authority to manage public affairs, the state, in turn, ensures that individuals have adequate space within society to live their private lives without interference from anyone. It also guarantees the necessary legal protection against any attacks targeting private life, including those involving the use of information and communication technologies to harm individuals.

Article 49 of the 1976 Constitution explicitly recognizes that the sanctity of a citizen's private life and honor cannot be violated, and the law protects them. Moreover, the secrecy of correspondence and private communications in all their forms is guaranteed. The Algerian legislator reinforced this protection in the 1996 constitutional amendment in Article 39. Additionally, Article 63 states that everyone may exercise all their freedoms, within the framework of respecting the rights recognized for others in the Constitution, especially respecting the right to honor, the privacy of private life, and the protection of family, youth, and childhood.

The legislator has also made efforts to protect natural persons in the area of processing personal data. This is considered a fundamental right guaranteed by law, and violations are subject to punishment. This was enacted through the constitutional amendment of 2016 under Article 46, and was further emphasized and maintained in Article 47 of the 2020 amendment. In line with the constitutional legislator's focus on establishing the principle of protection and the right to privacy, and directing criminal law towards criminalizing all behaviors that constitute a violation thereof.

If we refer back to Law No. **18_04**[1]**,** which defines the general rules related to mail and electronic communications, we find that the legislator has, pursuant to Article 16 of Chapter Three under the title 'Postal and Electronic Communications

[1]Law No. 18_04 dated May 10, 2018, defines the general rules related to mail and electronic communications, Official Gazette, No. 27, issued on May 13, 2018.

Institutions', obligated the members of the Regulatory Authority's board, the General Manager, and all their employees to maintain confidentiality concerning the information and inquiries they obtain in the course of performing their duties. Furthermore, the establishment and exploitation of public electronic communications networks and the provision of electronic communications services to the public are subject to data privacy conditions and the protection of information transmitted through electronic communications networks, as well as conditions protecting the private lives of subscribers and personal data, pursuant to Article 97 thereof.

Additionally, pursuant to Article 164 of the same law, the Algerian legislator has penalized anyone who violates the confidentiality of correspondences sent via mail or electronic communications, or discloses, publishes, or uses their contents without authorization from the sender or recipient, or informs others of their existence.

The 2018 legislative milestone in the field of digital privacy protection, marked by the enactment of Law No. 18_07[1], relates to the protection of natural persons in the processing of personal data, which has been described in some scholarly studies as a deontological code for automated information processing. This law aims to establish rules for the protection of natural persons concerning personal data processing, stipulating in Article 2 that personal data processing, regardless of its source or form, must respect human dignity, private life, public freedoms, and not infringe upon the rights, honor, or reputation of individuals.

In the context of defining certain terms for the purposes of this law, the Algerian legislator defines personal data as any information, regardless of its medium, related to an identified or identifiable person, directly or indirectly, particularly through an identification number or one or more elements specific to their physical, physiological, genetic, biometric, psychological, economic, cultural, or social identity.

Upon examining the provisions of this law, we find that the Algerian legislator has criminalized several behaviors that can be categorized into three main groups:

- Unlawful collection of personal data: This includes using illegal methods to collect personal data.

[1]Law No. 18-07 dated June 1, 2018, concerning the protection of natural persons in the processing of personal data, published in the Official Algerian Gazette, Issue No. 34, on June 10, 2018.

- Crimes committed during processing: This includes violating the preconditions for processing, breaching the obligations of the data controller during processing.
- Unlawful exploitation of personal data: This includes violating the terms of declaration or authorization, and disclosing personal data.

Furthermore, to strengthen the constitutional and legislative protection of personal data, the same law established an independent administrative authority for the protection of personal data, referred to as "the National Authority," headquartered in Algiers. The National Authority enjoys legal personality, financial, and administrative independence. It can be considered as an administrative safeguard for the right to electronic privacy in Algeria.

In conclusion, it can be said that this law has emerged within the context of ongoing efforts to modernize our legislative system towards enhancing the protection of human rights and consolidating the principles of the rule of law, within the framework of executing the esteemed President’s program for judicial reform. This legislative project aims to adapt our legal system to the developments observed in the legal systems of many countries, which strive to establish legal frameworks that allow for the optimal use of modern technologies in various fields, while ensuring the protection of rights and private freedoms.

This law project aligns with the provisions and principles set forth in international instruments ratified by our country, including the International Covenant on Civil and Political Rights, which was adopted by the United Nations General Assembly on December 16, 1966, and to which Algeria acceded in 1989. Specifically, Article 17 of the Covenant states: '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. Everyone has the right to the protection of the law against such interference or attacks.'"

In regards to our country, Algeria, although there are many laws that contain scattered references to the protection of personal data, such as the provisions of the Penal Code related to the protection of private life and the confidentiality of correspondence, there was no specific law for the protection of personal data. Hence, the significance of this law arises to fill this gap that has existed in Algeria for years.

This law excludes from its application certain data processing activities, as is the case in all countries, due to the nature of these data and especially those processed for the purposes of defense and national security, and for crime prevention,

monitoring, and suppression, and included in judicial databases. This legislative project does not apply to data processing carried out by an individual purely for domestic activities or for family use only, considering the limited risk of infringing on private life, as these are data related to personal and family matters.

This law also establishes the fundamental principles governing the processing of personal data, where such processing can only be conducted with the explicit consent of the concerned individual. The law specifies the circumstances under which this consent is not mandatory, particularly in cases of processing carried out under a legal obligation, or if it is necessary to protect the life of the individual concerned, or to perform a task in the public interest, or as part of the exercise of official authority. Personal data must be processed in a lawful and fair manner, collected for specific, clear, and legitimate purposes, and kept in a form that allows identification of the concerned individuals for no longer than necessary to fulfill the purposes for which it was collected and processed, as determined by the processor in the license presented to the proposed national authority for the protection of personal data.

The significance of this law is evident in judicial cooperation, for instance, and even in the official judicial assistance requests sent by judges as part of their duties in cases with international dimensions. They request data according to official judicial assistance mandates, and we have agreements with these countries. However, these agreements stipulate that for certain information to be provided, a law protecting personal data must be in place. When it is known that the requesting country does not have legislation protecting personal data, it may not provide that information or may only provide it under certain conditions. Therefore, this law is essential in the legal arsenal of the Algerian state and is also crucial for the promotion of human rights and the protection of personal data of natural persons.

The second topic: Privacy Protection in Anglo-Saxon Legislation

In this section, we will explore the landscape of protection in the United States, focusing on both constitutional and legislative aspects.

First requirement :Constitutional Protection

The U.S. Constitution does not explicitly mention the right to privacy, whether in its broad sense encompassing all aspects of human privacy or even the privacy of information which is central to privacy in the information technology environment. Despite this, there is a consensus among American legal scholars that privacy is one

of the constitutional rights implicitly affirmed in the constitutional amendments included in the Bill of Rights.[1]

Second requirement :Legislative Protection

The legal framework in the United States is characterized by the diversity of its sources; there is no single comprehensive privacy law that governs the collection and use of personal information by both public and private sectors, whether online or offline. Instead, there are various laws that regulate the collection and use of personal information, each with a specific scope covering only certain industrial or economic sectors and typically applying only to government activities.

The legislation concerning the public sector consists of laws that protect the privacy of citizens from government intrusion or misuse. These protections are often procedural, and some of the most important federal laws that protect individuals' privacy against government actions include:

1. **The Fourth Amendment**: Protects against unreasonable searches and seizures, thereby limiting government access to private information without a warrant.
2. **The Privacy Act of 1974**: Regulates the federal government's collection, use, and disclosure of personal information, establishing a code of fair information practices that requires federal agencies to respect the privacy rights of individuals.
3. **The Freedom of Information Act (FOIA)**: Provides the public the right to request access to records from any federal agency, indirectly supporting privacy by promoting transparency and accountability in government.
4. **The Electronic Communications Privacy Act (ECPA) of 1986**: Protects wire, oral, and electronic communications while they are being made, are in transit, and when they are stored on computers. The Act applies to email, telephone conversations, and data stored electronically.
5. **The Health Insurance Portability and Accountability Act (HIPAA) of 1996**: Protects personal health information by controlling the way healthcare providers and other entities process and handle health-related information.

[1] For further information, particularly refer to: Dr. Walid El-Sayed Selim, Guarantees of Privacy on the Internet, Dar Al-Jamea Al-Jadida, Alexandria, 2012.

6. **The Children's Online Privacy Protection Act (COPPA) of 1998**: Regulates online collection of personal information by persons or entities from children under 13 years of age.[1]

These federal statutes are complemented by state laws that can vary significantly from one state to another, offering additional protections that reflect the diverse priorities and concerns of different states. This decentralized and sector-specific approach to privacy legislation in the U.S. enables flexibility and specialization but can also lead to gaps in protection and inconsistencies across different contexts and jurisdictions.

Conclusion:

This study examines recent transformations in the concept of privacy protection through the lens of Latin and Anglo-Saxon legislation. The continuous change in the digital landscape has necessitated a reshaping of the boundaries and expectations of privacy, underscoring the urgency of enhancing legal protections in this domain.

The study has yielded several findings and recommendations:

Key Findings:

1. Rapid technological developments have presented new challenges that traditional laws in both Latin and Anglo-Saxon systems have been inadequate in addressing.
2. Legislation in Latin countries, such as the French system, demonstrates a strong constitutional commitment to privacy that is explicitly recognized and extensively protected across various legal areas.
3. In contrast, Anglo-Saxon systems, particularly in the United States, rely on an implicit constitutional recognition supported by amendments and sector-specific legislation that protects privacy in specific contexts.
4. Latin countries often have comprehensive privacy laws that offer broad protection applicable to both the public and private sectors alike.
5. Anglo-Saxon legislation, especially in the U.S., is characterized by a piecemeal approach that addresses privacy issues through a variety of specific, context-dependent laws. **Recommendations:**

[1]Please refer to the following website:" https://www.congress.gov/bill

1. The study recommends the need for periodic updates to the legal system to keep pace with technological advancements, ensuring the continuity and effectiveness of privacy protection.
2. It also underscores the necessity of international cooperation and the establishment of common privacy standards, given the cross-border nature of digital data and privacy threats."

Bibliography List setting:

-First: legal texts

1. Law No. 2018-493 of June 20, 2018, on the protection of personal data
2. Law No. 15-04 dated February 1, 2015, defining the general rules concerning electronic signing and certification, Official Gazette, Issue No. 06, published on February 10, 2015.
3. Law No. 18-07 dated June 1, 2018, concerning the protection of natural persons in the processing of personal data, published in the Official Algerian Gazette, Issue No. 34, on June 10, 2018.

-Second: books

1. Dr. Omar Aboul Fotouh Abdel Azim Al-Hammami, Criminal Protection of Electronically Recorded Information - A Comparative Study, Dar Al-Nahda Al-Arabiya, Cairo, 2010, p. 830
2. Dr. Walid El-Sayed Selim, Guarantees of Privacy on the Internet, Dar Al-Jamea Al-Jadida, Alexandria, 2012.