PROTECTION OF THE RIGHT TO INFORMATIONAL PRIVACY IN ALGERIAN LEGISLATION

DR . CHAHRAZED AOUABED
Faculty of Law and Political Science, Mohamed Lamine Debaghine University - Sétif 2, Algeria
Email: c.aouabed@univ-setif2.dz

Received: 23/10/2023 ; Accepted: 22/01/2024 ; Published: 25/04/2024

Abstract:
The right to privacy is one of the most fundamental human rights, receiving special attention from both national and international legislations as a constitutional right that must be protected against any infringement. Islamic law preceded all positive legal systems in recognizing and safeguarding this right. However, with the advent of advanced technological revolutions that enable state intervention in private life, this right has been increasingly and rapidly violated, posing a significant challenge to its holders and advocates. These violations threaten the social value of privacy, necessitating the establishment of mechanisms to protect informational privacy as a new legal concept amid digital transformation and its associated challenges. Algeria has sought to address these violations and risks through its constitutions and legislation. Accordingly, this study aims to shed light on the most prominent risks and violations affecting privacy worldwide, particularly in Algeria, and to examine the measures taken to protect the right to informational privacy. It also questions whether these measures are sufficient and effective in safeguarding this right.
Keywords: *Privacy, Private Life, Informational Privacy*

INTRODUCTION:

The modern world has witnessed a digital revolution that has given rise to what is known as open electronic societies, deeply integrated into the virtual world and digital transactions. This widespread digital engagement spans all fields, where the continuous use of the internet for information exchange and utilization has become a major challenge, compelling individuals to provide personal and professional data, as well as their daily concerns, through digital platforms. Consequently, they are increasingly exposed to violations that infringe on their private lives, threaten their personal security, and undermine their right to informational privacy. These violations manifest in various forms, including fraud, electronic scams, eavesdropping, cyber theft, unauthorized access to stored data, and digital sabotage. In many cases, digital attacks on private life have escalated to the extent of causing the loss of personal freedom, endangering the right to life, and affecting psychological well-being, largely due to the rapid evolution of illicit technological activities that have made the world more susceptible to contemporary crimes.

As a result, the digital revolution has enabled cybercriminals to employ various means to infringe upon personal freedoms, raising significant challenges regarding electronic surveillance, digital evidence, and the provision of adequate legal protection. These challenges persist despite the existence of regulatory frameworks at both the international and national levels, as controlling such privacy-related cybercrimes remains a complex and pressing issue.

Despite the advantages of modern technology, it poses significant risks, particularly concerning the violation of users' informational privacy in the digital space. The most imminent and confirmed threat to individuals is the presence of their personal data and information within this virtual digital environment. In response to this challenge, the legislator has sought to protect users in the virtual world from privacy infringements by third parties through successive constitutions and other legislative texts. This commitment to safeguarding privacy was concretely embodied in Law No. 18-07 on the Protection of Personal Data. (Official Journal, 2018, Issue 34). In response to the

challenges of the digital age, this study seeks to examine the central research question: To what extent is the legal protection provided by the Algerian legislator for the right to informational privacy sufficient and effective, given the increasing violations and infringements on this right?

To address this question, the study adopts a descriptive approach by outlining the general concept of privacy, with a specific focus on informational privacy. Additionally, an analytical approach is employed to examine the various legal texts governing informational privacy, which primarily concern personal data and information. The study is structured into two main sections:

- **First Section: The Right to Privacy Between Tradition and Modernity** – This section explores the concept of privacy in detail, tracing its historical evolution and the emergence of informational privacy as a modern legal concern.
- **Second Section: Aspects of Protecting Informational Privacy** – This section examines the constitutional, civil, and criminal protections afforded to informational privacy, analyzing their effectiveness in safeguarding individuals against digital infringements.

First Section: The Right to Privacy Between Tradition and Modernity

Most studies addressing the right to privacy have examined it under the concept of the right to respect for private life or the inviolability of private life, which represents the traditional aspect of this right. (Al-Zoubi, 2006, p. 32) The earliest terminology associated with privacy reflected a prevailing understanding that a person's home is their fortress, safeguarding their private life from intrusion. Accordingly, the constitutions of most states initially recognized only two primary aspects of this right: the inviolability of the home and the confidentiality of correspondence. (Saleh, 2016, p. 107).

Privacy has evolved through three historical stages, gradually shaping its modern understanding in the digital era. Initially, physical privacy emerged, recognizing privacy as a right that protects individuals from physical intrusions into their lives and property. This was followed by psychological privacy, which extended the concept to include the protection of a person's moral and intangible values. Eventually, privacy evolved into a general right, encompassing protection from all forms of interference, regardless of their nature or manifestation. This progression led to the emergence of a new dimension of privacy—informational privacy, which pertains to individuals' right to protect and control their personal data in response to the challenges posed by the digital age. (Al-Bahaji, 2005, p. 76).

1. The Concept of the Right to Privacy

Linguistically, "privacy" refers to a state of exclusivity, as opposed to generality. The Arabic root "خصّ" conveys the idea of singling out or reserving something for a particular individual. In legal and legislative contexts, there is no universally clear and precise definition of privacy, including within Algerian legislation. This lack of definition may be attributed to the differing legislative perspectives on what constitutes privacy, which are influenced by cultural values, moral principles, and religious beliefs across societies. However, at the international level, there is general consensus that privacy encompasses all matters related to an individual's dignity, family life, and personal secrets that are intentionally kept from public exposure.

The American Institute of Law defines privacy as: *"A person's serious and unjustified intrusion into another's right to keep personal matters confidential and to prevent their image from being publicly displayed."*

Similarly, French legal doctrine describes privacy as: *"A personal sphere of life exclusive to each individual, where no one may interfere without consent."* Legal scholar Hesham Mohamed Farid Rostom identifies three key elements of the right to privacy: secrecy, isolation, and anonymity, emphasizing the need for protection against any form of intrusion—whether through direct physical means or through the unauthorized dissemination of personal information.Meanwhile, Issam Ahmed Al-Bahji defines private life as a traditional aspect of the right to privacy, highlighting its characteristics as confidentiality, relativity, and freedom—suggesting that privacy is not an absolute right but one that must be balanced against other legal and social interests. (Massoudi, 2022, p. 156).

The Algerian legislation is among the legal systems that have recognized the right to privacy in its comprehensive sense, considering it an independent right. In this regard, it follows the French legislator, who has established a specific and direct legal protection for the inviolability of private life.

Regarding the legal nature of the right to privacy, one approach views it as a property right, implying that an individual has ownership over this right. Conversely, another perspective considers it an inherent personal right, inseparable from human existence. This latter view is the one adopted by the Algerian legislator, as reflected in Article 47 of the Algerian Civil Code, which recognizes a category of rights known as "personality rights", under which the right to privacy is classified.

2. The Modern Evolution of the Right to Privacy (Digital Privacy)

With the remarkable advancement in technology, states have begun storing individuals' personal data in databases and information banks, making it accessible to various entities. This accessibility increases the risk of unauthorized access, exposing these data and personal information to potential violations and breaches. (Saidani, 2020-2021, p. 86)

Recognizing the risks posed by computer processing of stored data, many countries have enacted legislation to protect such information. These laws prohibit the unauthorized use, storage, processing, or distribution of personal data via computer systems without proper authorization, whether such actions are committed intentionally or inadvertently.

Thus, informational privacy has become closely linked to information communication technologies and automated data processing systems associated with internet networks.

The American scholar Alan Westin, in his 1967 book *Privacy and Freedom*, defines informational privacy as:*"An individual's right to determine when, how, and to what extent information about them is shared with others."* Similarly, legal scholar Miller, in his book *The Assault on Privacy*, defines privacy as:*"The ability of individuals to control the cycle of information related to them." (Ben Haida, 2009-2010, p. 23)*

Informational privacy has also been defined as an individual's ability to control the confidentiality of their personal data and information, as well as to determine who may access such information, whether they are individuals, governments, or computer systems.

Another definition describes it as:*"The right of individuals to determine when, how, and to what extent their personal information is shared with others, while also regulating the collection, automated processing, storage, distribution, and use of such data in decision-making processes that affect them." (Adnan, 2013, p. 433).*

These definitions make it clear that a person's right to informational or digital privacy entails the protection of their personal data, ensuring that it is not disseminated or exposed during the processes of data collection, storage, and processing. This right is based on the principle of integrity and fairness in handling personal data. (Saidani, Ibid., p. 108).

Third: Risks Threatening Digital Privacy

While modern technologies offer numerous benefits that facilitate individuals' lives, they also pose significant risks due to the vast amount of electronically stored private information. Establishing a privacy protection framework in the digital age requires addressing the specific threats posed by these technologies. The rise of information technology, particularly the internet, has introduced a series of new challenges to privacy protection. The internet has significantly increased the volume of collected, processed, and created data, while also facilitating the globalization of information and communications. This has led to decentralization and a loss of control mechanisms, diminishing the state's role in monitoring and protecting data. These challenges stem from the misuse of information technology and its applications, as illustrated by the following issues:

1. **Violation of Personal Data Confidentiality**: Since personal data forms the foundation of the right to privacy—comprising information and details about an individual that are inherently confidential—its unlawful processing constitutes one of the most serious forms of privacy violations. Such breaches occur when data handlers fail to comply with the legal requirements and procedures established at the national level.

2. **Unauthorized Disclosure of Personal Data**: Another form of privacy violation is the unlawful disclosure of personal data, particularly in electronic transactions. This issue is especially concerning in professions that rely on data confidentiality, such as banking and legal practice.

3. **Electronic Espionage**: One of the most severe privacy breaches in digital interactions is electronic espionage. This practice is directly linked to the unauthorized interception of private conversations, correspondence, and transactions conducted over the internet. Electronic espionage in the context of personal communications is defined as **"the act of eavesdropping or intercepting data transmitted between two devices over the internet"** or **"the extraction of electromagnetic emissions from a computer and converting them into readable data using technical means."** It is important to note that unauthorized electronic surveillance carried out by state authorities—when conducted outside the framework of the law—constitutes a violation of international and domestic legal standards protecting individuals' rights. If such surveillance occurs without prior judicial authorization, it is considered an abuse of state power under the pretext of safeguarding national or public security. (Dahbi, 2017, p. 148)

The dangers of electronic espionage have expanded significantly compared to the past, particularly in the era of globalization and modern technologies. Espionage is no longer limited to government authorities or intelligence agencies; surveillance tools have become increasingly accessible to ordinary individuals, especially in developed countries. In contrast, Arab countries continue to impose strict restrictions on the marketing and distribution of surveillance equipment, making it difficult to obtain such tools freely.

The methods of electronic espionage vary depending on the technological culture of users. One of the most prevalent techniques is network interception, which relies on specialized software to carry out the operation. This method allows an unauthorized third party to intrude on network communications conducted over the internet—whether text exchanges, voice calls, or video conferences. Through network interception, data can be captured, images retrieved, voice conversations monitored, and audiovisual communications intercepted via cameras during online interactions. (Abdel Azim, 2016, p. 101).

Eavesdropping, interception, and recording constitute the material element of the offense of violating the privacy of communications. Eavesdropping refers to secretly listening, by any means, to a conversation that has a confidential or private nature without the consent of the person involved. Interception of calls or conversations involves obtaining the content of a discussion between individuals or secretly capturing what a person has uttered without their knowledge, regardless of the technology used. Recording entails storing conversations on a device specifically designed for this purpose, with the intent of replaying them later. As for transmission, it refers to relaying a conversation or call that has been listened to or recorded from the original location to another place, by any means or technology.

4. .Moreover, hacking into computers and email accounts is no less dangerous than the aforementioned forms of privacy violations. The personal computer has become one of the most essential tools for modern communication among individuals, serving as a primary medium for electronic correspondence and transactions. Consequently, hacking into a personal computer is fundamentally an infringement on the privacy and confidentiality of transactions, exploiting them for various illicit purposes, which can cause significant financial and moral harm to individuals. Some scholars have linked hacking to the unauthorized processing of data, defining it as: "Unauthorized access to a data processing system using a computer." (Ibrahim, 2004, p. 242).

With regard to email hacking, email is one of the modern tools used in electronic transactions facilitated by the Internet. It enables instant message exchange, streamlining electronic communication. Consequently, email hacking poses a significant threat to the right to privacy, exposing individuals to violations of the confidentiality of transactions and correspondence across various domains. Accordingly, general legal principles mandate the establishment of safeguards to protect the confidentiality of communications, within specific limits and regulations, regardless of whether the methods used are traditional or modern.

Section Two: Aspects of Protecting the Right to Informational Privacy

Legal scholars unanimously agree that the foundation of protecting the right to privacy lies in its recognition as a personal right safeguarding an individual's private life. Given the increasing violations of informational privacy in recent years, Algeria has established a legal framework to address these challenges in the context of digital transformation, reflected in its successive constitutions and legislative provisions.

1. Constitutional Protection of the Right to Informational Privacy

Algerian constitutions, throughout their successive amendments, have enshrined the protection of individuals' private lives, considering it a fundamental principle that must not be violated. They affirm that private life is a guaranteed right, and the state ensures its protection by preventing any infringement on human dignity. Since the sanctity of the human person encompasses various aspects, including private life and personal privacy, it is constitutionally safeguarded against any form of violation.

Article 47 of the 2020 constitutional amendment explicitly recognizes the protection of informational privacy, affirming that safeguarding natural persons in the processing of personal data is a fundamental right recognized and protected by law. This reflects the Algerian legislator's intent to align with contemporary legal issues, particularly in the realm of digital information, while also reinforcing the Constitution as a general source of legislative authority. This commitment is further reaffirmed in Article 81 of the 2020 constitutional amendment.

2. Civil Protection of the Right to Informational Privacy

The Algerian Civil Code.(Official Journal, 1975) does not provide an extensive framework for privacy rights and does not specifically address informational privacy or its protection, as its primary focus is the regulation of transactions and contractual relationships among individuals. However, Article 47 of the Civil Code implicitly includes privacy as one of the inalienable personal rights, which are non-financial in nature and cannot be subject to commercial transactions, waiver, or renunciation. These rights are tied to public order and morality and are inherent to individuals from birth until death.

Among these personal rights are physical, mental, and psychological integrity, the right to private life, and the right to life itself. Article 47 explicitly mandates respect for this right due to its direct association with the individual, asserting that any unlawful infringement upon it must be remedied and compensated. The provision states: "Any person who has been unlawfully harmed in one of their inherent personal rights may request that the infringement be ceased and claim compensation for any damage suffered."

In this context, the principles of tort liability apply, as an unlawful act is considered a deviation from the expected standard of conduct or a violation of a legal rule. Unlawful processing of personal data, for instance, constitutes a tortious act, and the responsible party must compensate the affected individual whenever damage has occurred.

3. Criminal Protection of the Right to Informational Privacy

Article 303 bis of the Algerian Penal Code stipulates imprisonment ranging from six months to three years, in addition to a fine, for anyone who intentionally infringes on the sanctity of private life through any technological means. This includes intercepting, recording, or transmitting private or confidential conversations without the consent of the concerned party, as well as capturing, recording, or transmitting images of an individual in a private setting without their authorization.

Furthermore, Article 303 bis 1 criminalizes the retention, dissemination, or utilization of unlawfully obtained recordings related to private or confidential conversations. The phrase "by any technological means" is intended to extend protection to all forms of private communication, including those facilitated by rapid technological advancements.

Ultimately, these measures aim to establish evidentiary mechanisms that can hold cybercriminals accountable. However, technical surveillance arrangements are often implemented without the knowledge or prior consent of the individuals being monitored, raising concerns about potential misuse. (Zeibha, 2011, p. 157).

Article 301 of the Algerian Penal Code also criminalizes the disclosure of professional secrets. This provision can be applied, for example, in cases where certain administrative bodies, such as tax

authorities, use computer systems to collect personal data related to individuals. In such instances, employees of these institutions are entrusted with safeguarding this information. If an employee discloses such data, they would be committing the crime of breaching professional confidentiality, particularly when the disclosed information is of a confidential nature.

Furthermore, the Algerian legislator has extended protection to digital data in general, including personal data, under Articles 394 bis to 394 bis 8 of the Penal Code. These provisions criminalize acts that compromise automated data processing systems. (Mbareki, 2018, pp. 469-481) Specifically, the legislator criminalizes unauthorized access to information systems, considering this act, in itself, to be a crime. At first glance, it is evident that merely hacking a computer system—whether for the purpose of accessing data or even for mere entertainment—constitutes an unlawful violation of the information system. (Zeibha, Ibid., p. 46)

Fourth: Ensuring the Protection of Personal Data under Law No. 18-07 (Criminal Protection)

Law No. 18-07 aims to regulate the processing of personal data while respecting the right to privacy and human dignity, without infringing upon individuals' rights, honor, and reputation.

Article 2 of Law No. 18-07 stipulates that the processing of personal data, regardless of its source or form, must be carried out in compliance with human dignity and must not violate individuals' rights, honor, or reputation. To safeguard individuals' right to privacy, the legislator has established substantive and procedural rules governing the collection, storage, and processing of personal data.

Regarding substantive rules, they impose restrictions on data collection, storage, and processing, which essentially serve as guiding principles for data processing. Article 9 of Law No. 18-07 specifies that the data controller must collect data lawfully and must also adhere to the declared purpose stated in the authorization or processing declaration request, as well as comply with the specified timeframes necessary for achieving these purposes.

As for procedural rules, they primarily consist of obligations requiring the data controller to undertake specific formal procedures before initiating processing. The data controller is also required to inform the data subject that their personal data will be processed and obtain their explicit consent.

Furthermore, the legislator has introduced provisions outlining the necessary measures to ensure the security and confidentiality of personal data. Given that the effective enforcement of personal data protection laws depends on an independent authority overseeing compliance, the Algerian legislator has enacted rules to facilitate cooperation with the national authority in carrying out its functions, as well as to ensure respect for its decisions. Any breach of these procedural rules constitutes a criminal offense under the Personal Data Protection Law.

The Algerian legislator has imposed a series of procedural obligations on data controllers, and any violation of these obligations is subject to criminal penalties. These offenses include the failure to comply with prior formal procedures, the failure to obtain the data subject's consent, the failure to ensure the security and confidentiality of data, and the failure to cooperate with the national authority.

Regarding the violation of prior formal procedures, data controllers are required to undertake a series of formal steps before collecting and storing individuals' personal data. The purpose of these measures is to prevent the creation of secret files containing individuals' personal information, which could later be used for blackmail or threats. These formal procedures include submitting a prior declaration to an independent authority known as the national authority, and in exceptional cases, obtaining a specific authorization for processing.

Article 12 of Law No. 18-07 states that:*"Unless otherwise provided by law, all personal data processing operations are subject to prior declaration to the national authority or require its authorization in accordance with the provisions of this law."*

Failure to comply with prior formal procedures constitutes a criminal offense punishable by imprisonment ranging from a minimum of two (2) years to a maximum of five (5) years, in addition to a fine ranging from 200,000 DZD to 500,000 DZD. This represents one of the most severe

penalties under the law, highlighting the legislator's recognition of the seriousness of such offenses in this domain.

Regarding the offense of failing to obtain the data subject's consent, Article 55 of Law No. 18-07 criminalizes the processing of personal data without obtaining the explicit consent of the data subject. Any individual who processes personal data in violation of Article 7 of this law is subject to imprisonment ranging from one (1) year to three (3) years and a fine ranging from 100,000 DZD to 300,000 DZD. The same penalty applies to any person who processes personal data despite the data subject's objection, particularly when the processing is intended for commercial advertising or when the objection is based on legitimate grounds.

Concerning the offense of failing to ensure data security and confidentiality, Article 65 of Law No. 18-07 criminalizes the processing of personal data without implementing appropriate technical and organizational measures to ensure data security. The legislator penalizes inadequate or ineffective security measures taken by the data controller. However, by contrast, if the data controller has implemented sufficient security measures and a data breach nonetheless occurs, no offense is established, as the controller's obligation is one of means rather than results.

The legislator has prescribed a financial penalty for failure to comply with data security requirements, ranging from 200,000 DZD to 500,000 DZD. This classification suggests that the Algerian legislator considers the violation of security procedures to be a minor offense rather than a serious crime warranting imprisonment. However, the adequacy of this penalty remains debatable, given that ensuring data security is a fundamental obligation that data controllers must prioritize. The prescribed penalty appears disproportionate to the severity of the offense committed.

Regarding the failure to comply with the obligation to cooperate with the National Authority, Article 61 of Law No. 18-07 penalizes any act that obstructs the work of the National Authority, including resisting investigations, refusing to provide necessary documents, concealing or destroying records, and transmitting information that contradicts the actual content of the records.

Furthermore, Article 56 of Law No. 18-07 imposes a stricter penalty for failure to comply with the National Authority's decisions, particularly regarding the temporary or permanent suspension of data processing or the submission of false statements. This severity is justified by the potential risks associated with continuing personal data processing activities and the submission of false information to the National Authority, which could severely impact individuals' privacy rights. The prescribed penalty includes imprisonment ranging from two (2) to five (5) years and a fine ranging from 200,000 DZD to 500,000 DZD. This penalty is more severe than the one imposed for obstructing the work of the National Authority.

CONCLUSION

By nature, human beings have always sought to safeguard their privacy, protect their personal sphere, and maintain a degree of control over their data. It is well established that individuals do not wish for their personal information to be accessible to just anyone at any time. However, the advent of modern technology—particularly artificial intelligence and digital systems—has given rise to numerous cybercrimes closely linked to these technologies. Those who master these tools often exploit them to infringe on individuals' private lives, taking advantage of their vulnerability and inability to control their personal data. Since information and data are the cornerstone of accessing individuals' private details, discussions on privacy have evolved in tandem with advancements in information technology and the growing need for its protection. Consequently, legal frameworks and fundamental principles must be established to safeguard digital privacy.

Recognizing the risks of digital privacy violations and aiming to prevent such crimes, legislators have revised and amended domestic laws to align with current transformations and the pervasive influence of technological and digital advancements in all aspects of life.

Based on our study of this subject, we have reached several key conclusions, the most important of which are:

- The right to privacy is inherently linked to human personality, necessitating clear legal protection, especially in the context of the information revolution.
- The need to protect informational privacy stems from the fact that it revolves around personal data directly related to individuals and their families.
- The widespread use of information technology has led to an increase in privacy violations, prompting states to enact legal frameworks that must be upheld to ensure the protection of informational privacy.

In light of these findings, the greatest challenge facing the right to privacy in this digital era is the establishment of comprehensive legal frameworks at both international and domestic levels. Given the ease with which personal information can now be accessed in various forms, individuals across societies face significant risks. Therefore, we propose the following recommendations:

- Implement mechanisms and measures to combat data breaches and unauthorized access through digital programs that enhance personal data protection.
- Establish regulatory legal frameworks governing all institutions that collect and process personal data.
- Urge the Algerian legislator to enact specific laws addressing cybersecurity and internet usage, with strict provisions for combating crimes that infringe upon individuals, including privacy-related offenses.
- To ensure effective protection of personal data, legislators should impose stricter penalties for failing to implement security measures, including introducing custodial sentences alongside financial sanctions.

REFERENCES :

First: Legal Texts

- Official Journal of the People's Democratic Republic of Algeria. (2016). *Constitution of the People's Democratic Republic of Algeria.*
- Official Journal of the People's Democratic Republic of Algeria. (2020). *Constitutional Amendment of 2020,* issued by Presidential Decree No. 20-442 dated December 30, 2020, related to the issuance of the constitutional amendment approved by the referendum of November 1, 2020. Issue No. 82.
- Official Journal of the People's Democratic Republic of Algeria. (1975). *Ordinance No. 75-58 of September 26, 1975, on the Civil Code, as amended and supplemented.*
- Official Journal of the People's Democratic Republic of Algeria. (2018). *Law No. 18-07 of June 10, 2018, on the Protection of Natural Persons in the Processing of Personal Data.* Issue No. 34.

Second: References

1. Books

- Ibrahim, K. M. (2004). *Cyber Crimes.* University Thought House, Egypt.
- Abdel Azim, M. E. (2016). *Cyber Crimes Affecting Private Life.* Arab Renaissance House, Egypt, 1st edition.
- El-Bahji, I. A. (2005). *The Protection of the Right to Privacy in Light of Human Rights and Civil Liability: A Comparative Study.* New University Publishing House.
- Al-Zoubi, A. A. (2006). *The Right to Privacy in Criminal Law.* Modern Book Institution, Lebanon.
- Saleh, M. Z. A. (2016). *International Legal Protection of Personal Data on the Internet Between International Treaty Law and National Law.* Arab Studies Center, Egypt, 1st edition.

2. Articles

- Massoudi, H. (2022). Protection and Promotion of the Right to Privacy in the Digital Age: A Review of the UN Human Rights Commission Report in its 28th Session. *Journal of Law and Political Science, University of Khenchela,* Vol. 9, No. 1.
- Dahbi, K. (2017). The Right to Privacy Against Electronic Attacks: A Comparative Study. *Journal of the Research Professor for Legal and Political Studies,* Vol. 1, No. 8, December.

- Adnan, S. (2013). Violation of Private Life on the Internet. *Damascus University Journal of Economic and Legal Sciences,* Vol. 29, No. 3.
- Mbarekiya, M. (2018). Criminal Protection of the Right to Digital Privacy in Algerian Legislation. *Journal of Sharia and Economics, Emir Abdelkader University for Islamic Sciences, Constantine,* Vol. 9, No. 1.

3. Theses

- Saidani, N. (2020-2021). *Criminal Protection of the Right to Privacy in the Field of Informatics.* Doctoral Dissertation in Law, University of Batna 1, Hadj Lakhdar.