PISSN : 2571-9904 - EISSN : 2602-7763

The Right to Privacy in Cyberspace: A Study of Its Concept, Islamic Legal Foundations, and Contemporary Technological Challenges.

HAMIDANE Badreddine

Emir Abdelkader University of Islamic Sciences in Constantine (Algeria)
hamidanebadreddine@gmail.com

Received: 08 / 08 / 2026 **Accepted**: 23 / 09 / 2026 **Published**: 30 / 09 / 2026

Abstract:

Digital privacy in cyberspace is considered one of the central issues imposed by the rapid transformations in information and communication technologies, as well as the widespread use of digital media and platforms across various aspects of life. This study aims to examine the concept of the right to digital privacy by identifying its dimensions and areas of application, while clarifying its Islamic jurisprudential foundations in light of the objectives of Islamic law (Maqāṣid al-Sharīʿa) and its principles that emphasize the protection of private life, the safeguarding of individuals' secrets, and the prevention of any form of intrusion or violation.

The study also seeks to review the most prominent contemporary technical challenges facing the protection of privacy in the digital environment, such as electronic surveillance, unauthorized access to information systems, and the collection and processing of personal data without adequate safeguards, all of which generate risks that affect individual rights and freedoms. It adopts an analytical approach that integrates conceptual, jurisprudential, and technical dimensions in order to highlight the importance of establishing an integrated framework for protecting digital privacy.

The study concludes that strengthening this right requires the development of legal and regulatory frameworks, the promotion of digital awareness, and the activation of ethical and religious guidelines to ensure a balance between benefiting from technological advancements and safeguarding human dignity and fundamental rights.

Keywords: *Right to Privacy ; Digital Privacy ; Digital Space ; Islamic Jurisprudential Foundation ; Personal Data Protection ; Contemporary Technological Challenges.*

I. INTRODUCTION

Contemporary society is witnessing profound transformations driven by the rapid advancement of information and communication technologies, which has led to a fundamental reshaping of patterns of human interaction and the increasing migration of daily life into cyberspace. Within this context, the right to privacy has emerged as one of the most pressing legal and ethical issues, given the growing risks associated with the extensive use of digital platforms, particularly the violation of individuals' private lives and the collection, processing, and dissemination of personal data in ways that often lack sufficient safeguards.

Digital privacy is of particular significance as it directly concerns human dignity and individual freedom. It is also closely linked to fundamental rights enshrined in international conventions and national legislations, in addition to being firmly grounded in the Islamic legal tradition, which places strong emphasis on preserving individuals' secrets, protecting private life, and prohibiting all forms of surveillance and intrusion.

However, this right is currently facing increasing technical challenges imposed by the modern digital environment, including the development of electronic surveillance tools, the expansion of big data analytics technologies, and the rising risks of cyberattacks and personal data breaches. These developments raise complex questions regarding the adequacy of existing legal and ethical frameworks in effectively protecting privacy.

In light of these issues, this study aims to analyze the concept of the right to privacy in cyberspace, to elucidate its Islamic jurisprudential foundations, and to examine the most prominent contemporary technological challenges that hinder its protection. The objective is to highlight the need for a comprehensive and integrated approach that balances the demands of technological advancement with the imperative of safeguarding individual rights and freedoms.

1. The Concept and Evolution of Privacy in Cyberspace

the existence of legal provisions that protect the essence of this right. This may be attributed to several considerations, most notably the fact that there are matters individuals feel the need to keep away from the knowledge and scrutiny of others. This condition is relative, as the scope of privacy for one individual may not be the same for another. Moreover, the boundaries of privacy are to a certain extent shaped by society, including its prevailing conditions, customs, and traditions. Hence, it can be argued that the concept of privacy expands or contracts depending on the differences between societies**.(Al-Zuabi, 2006, p.116)**

One of the most well-known definitions of the right to privacy is that provided by the American Law Institute, which has gained significant recognition and importance. It defines privacy through its violation, stating that it refers to any serious and unjustified infringement by a person upon another person's right to keep their affairs and circumstances from becoming known to others, and to prevent their image from being exposed to public view, thereby rendering the offender liable to the victim.

It has been noted in the commentary on this definition that distinguishing between what should be disclosed to the public and what should remain confidential remains a delicate matter for which it is difficult to establish a definitive standard.**(Al-Ahwani, 1978, p.49)**

It has been defined by some jurists as the right of every individual to keep their affairs and matters that they do not wish others to know about confidential. It has also been defined as the individual's freedom to lead a private life and to safeguard its secrets from any form of interference. In another formulation, it is described as whatever a person does and does not consent to being disclosed to others. Furthermore, it has been characterized as the individual's right not to be pursued or intruded upon in their private life. It has also been defined as the right to respect the confidentiality and privacy of persons against any material or moral intrusion. Additionally, it has been described as the individual's authority to veil certain facts relating to aspects of life that the legislator has placed within the realm of secrecy, thereby protecting them

from the curiosity of others, provided that there is no legal justification permitting their violation.**(Abdel Halim, 2018, p.21)**

Some jurists have also adopted a broad definition of the right to privacy. From their perspective, privacy is not limited merely to refraining from disclosing personal information to others without justification, nor is it confined to the individual's right to remain free from the intrusion or curiosity of others. Rather, it extends beyond that to encompass a wider scope. It implies that a person should be able to live according to their own preferences and to enjoy engaging in certain private activities, even if their behavior is visible to others. **(Hijazi, 2004)**

It can be said that the concept of the right to privacy in cyberspace, as suggested by some jurists, refers to the individual's right to prevent the misuse of electronically processed data by the government, or to restrict its use in accordance with the law. Given that the right to privacy has become closely associated with informatics, computing, and data banks, this has given rise to the notion of the right to privacy in cyberspace or informational privacy. Accordingly, privacy in the digital environment may be defined as the individual's right to control information relating to them.**(Abdel Halim, 2018, p.25)**

Studies concerned with privacy and human rights in light of technological developments remain relatively limited. It can be argued that the late 1960s and the 1970s witnessed the emergence of such studies, and that this period, in particular, marked the first significant and increasing appearance of the concept of information privacy as an independent concept, distinct from other notions of privacy.

The credit for drawing attention to the concept of privacy in cyberspace, or informational privacy, during this period is largely attributed to American scholars, both of whom proposed influential concepts and definitions of information privacy. The first definition, introduced by the jurist Alan Westin in 1967, defines information privacy as « the right of individuals to determine when, how, and to what extent information about them is communicated to others», In contrast, Miller provided a more profound definition, describing informational privacy as "the ability of individuals to control the flow of information relating to them." He further considered that an individual is in a state of privacy when they are in conditions of solitude, intimacy, and concealment.**(Ayoub, 2009, p.56)**

Digital privacy in cyberspace encompasses all regulatory frameworks governing personal information, including its collection, organization, and use. This extends to data such as credit card information and medical records, as well as all rules related to the protection and security of electronic mail, mobile phones, landlines, postal mail, and all forms of communication**.(Al-Nimr, 2017, p.147)**

Considering that information is susceptible to infringement, particularly when it reflects the personal opinion of its owner rather than merely general or public information, it can be argued that such data originates from the individual themselves and is therefore intrinsically linked to their personality. In this sense, it constitutes one of the rights attached to the personality of its holder. The information itself forms the subject matter of this right. One of its key characteristics is its transmissibility, meaning that it can be communicated to another party who receives it. From this, relationships emerge either between the information and its owner or between the owner and third parties.**(Qara, 2007, p.17)**

The introduction of automated information processing systems has significantly altered many existing conditions, and the impact of such systems on society has been officially recognized in many countries, particularly with regard to individuals' private lives. Data banks, which constitute a component of automated information processing systems, have become repositories for a vast amount of secrets relating to individuals' private lives. This development has made it possible to access and retrieve personal information with ease and unprecedented speed. It has also become increasingly simple to transfer such information from one place to another through

remote communication devices that are widely distributed across various locations.**(Al-Shahat, 2011, p.82)**

This situation makes the right to privacy vulnerable to infringement by third parties, particularly in light of recent technological advancements. Consequently, information security has become an imperative necessity in order to protect data from theft, damage, and unlawful use, all of which may lead to violations of individuals' private lives.

1.1. According to its historical development, privacy has passed through three main stages: (Al-Mousawi, 2013, p.17)

1.1.1. The first stage involved recognizing privacy as a right aimed at protecting individuals from forms of material intrusion upon their lives and property, commonly referred to as physical privacy.

1.1.2. The second stage saw privacy encompassing the protection of the moral and intangible aspects of the individual, known as moral or psychological privacy.

1.1.3. The third stage conceptualized privacy as a general right whose scope extends to protecting individuals from all forms of infringement and interference in their lives, regardless of their nature or form.

Within this latter meaning, a new concept of privacy emerged, closely linked to the impact of technology on private life, namely information privacy or the right of individuals to control their personal information and data in the face of the challenges of the digital age.

The idea of privacy and its connection to information technology is considered, from a historical perspective, one of the earliest issues addressed within computer law in general. It emerged in the 1960s, in a context characterized by rapid technological development, the increasing use of computers, the establishment of data banks, and the widespread adoption of automated data processing systems.

Accordingly, the concept and evolution of privacy in cyberspace have attracted significant attention at the international and regional levels, in addition to being addressed in both Arab and Western legal systems. Privacy in the digital environment is commonly referred to as "information privacy," a term adopted by the European Community and used to denote the concept of the right to privacy on the internet.

The member states of the European Union have reached a consensus on the importance of protecting the right to informational privacy through comprehensive and extensive measures, such as the European data protection directives, which have been issued periodically in response to the evolving nature of information systems. .**(Ayoub, 2009, p.60)**

It can be said that, in one form or another, nearly all countries of the world have recognized the right to privacy in at least some of its manifestations. However, this does not necessarily imply the existence of adequate protection in all jurisdictions. While the protection of privacy in its physical sense is often more widespread and broadly recognized, the protection of informational privacy tends to be more limited.

At the same time, informational privacy has become a central concern for legislative bodies and policymaking institutions in many countries around the world. Accordingly, the right to privacy and data protection evolved significantly during the 1960s and 1970s, as a result of the influence of information technology and the potential surveillance capabilities of computer systems. This development necessitated the establishment of specific legal rules governing the collection and processing of personal data. **(Al-Mousawi, 2013, p.17)**

2. Islamic Jurisprudential Foundations of the Right to Privacy in Cyberspace:

Islamic law has established the principle of the sanctity of an individual's private life in all its forms and manifestations. This is clearly evidenced in the verses of the Holy Qur'an, the Prophetic Sunnah, and the reports and practices of the Companions (may Allah be pleased with them), all of which address and affirm such aspects of privacy and its protection.

Respect for private life is considered one of the most important human rights in Islam; indeed, it is regarded as one of the inherent personal or natural rights that are inseparable from the human being. When Islamic law affirmed the sanctity of private life, it also established equality among all people in enjoying this protection, based on the general principle of equality among Muslims.

Accordingly, there is no distinction in the enjoyment of this protection, from an Islamic perspective, between an ordinary individual and others. Islamic law does not differentiate based on a person's status, whether they are famous or an ordinary person, as all individuals are regarded equally in Islam as holders of the right to privacy. **(Al-Jundi, 1993, p.42-43)**

There is no disagreement among jurists that defining private life is a difficult matter, due to the variation in its content and the differing scope of privacy from one individual to another. Some individuals make their private lives an open book, while others keep their lives as an obscure secret. Moreover, the content of private life also varies from one society to another as a result of differences in moral values and cultural traditions**.(Al-Shahat, 2011, p.81)**

Islam has prohibited any action that infringes upon an individual's right to the sanctity of their private life. The Prophet Muhammad (peace be upon him) said: **« ظهر المسلم حمى إلا بحقه »** All individuals are equal before the divine law of God and its principles of justice and mercy in protecting privacy from surveillance and intrusion.

A person has the right to safeguard their own rights and preserve their privacy. Almighty God has forbidden the pursuit of matters that do not concern a person and has prohibited seeking access to the secrets of others. Islamic law thus preserves the privacy of every individual and guarantees protection of their private affairs**.(Al-Nimr, 2017, p.235)**

This is affirmed in the verse of the Holy Qur'an**: وَلَا تَقْفُ مَا لَيْسَ لَكَ بِهِ عِلْمٌ ۚ إِنَّ السَّمْعَ وَالْبَصَرَ وَالْفُؤَادَ كُلُّ أُولَٰئِكَ كَانَ عَنْهُ مَسْئُولًا»(Surah Al-Isra, 36)**

It can be said that privacy is close to secrecy, but it is not synonymous with it. Secrecy presupposes concealment, whereas privacy may exist even in the absence of complete secrecy. Secrecy requires a higher degree of confidentiality than privacy does. What is considered a secret generally falls within the scope of privacy; thus, confidentiality is regarded as a distinguishing feature of the right to privacy.

Privacy therefore entails a certain degree of concealment, and secrecy constitutes the core of private life. The purpose of safeguarding personal secrets is to protect an individual's right to privacy, as confidentiality represents one aspect of a person's private life **.(Abdel Halim, 2018, p.26)**

The disclosure of secrets via the Internet, computer systems, or data banks constitutes a form of breach of trust, and it involves defamation and violation of individuals' honor, as well as the exposure of their confidential matters. This is explicitly prohibited in Islamic law, which forbids such conduct.

The protection of people's honor and the safeguarding of their secrets are considered essential necessities that Islamic law has commanded to preserve. Accordingly, maintaining the confidentiality of individuals and their private lives is both a legal and moral obligation. Consequently, the disclosure of such secrets through Internet platforms or computer systems is regarded as a discretionary (taʿzīr) offense, punishable under Islamic law in accordance with the offender's circumstances, the nature of the offense, and the extent of the resulting harm.

Thus, any infringement upon an individual's privacy is considered a criminal act within the framework of Islamic jurisprudence**. (Al-Shahat, 2011, p.83-85)**

Accordingly, the right to privacy is linked to an individual's personal information, which may

be stored on the person's own computer device, whether at home or in the workplace. In other words, such information may exist in isolation or may be connected to a local or global communication network. It may also be held in official form by other entities with which the individual has some form of relationship**.(Al-Zuabi, 2006, p.339)**

Islamic law has taken care to protect correspondence, telegrams, telephone conversations, and other private means of communication, affirming the inviolability of their confidentiality. Likewise, certain secrets may be entrusted to governmental bodies or contained in official files held by specific institutions, such as curricula vitae or judicial records, including judgments that affect a person's reputation. All such forms of confidential information are protected under Islamic law, which criminalizes their unlawful disclosure without the consent of their owner.

Despite the significant scientific and technological progress in the field of information and the proliferation of communication tools, Islamic law has established safeguards to prevent the violation of people's secrets. This is reflected in the concept of the "muḥtasib" system, which prohibited the muḥtasib from engaging in espionage to obtain information, even in cases involving criminals.

Accordingly, human secrets remain ultimately known only to their Creator, and individual privacy constitutes a protected domain that must not be violated or exposed, as such actions cause harm to Muslims and are therefore prohibited in Islamic law.

However, if an individual infringes upon the privacy of others through computers, the Internet, or social media platforms, Islamic law provides for punitive measures. Among these is the discretionary punishment (taʿzīr), which is an undetermined penalty imposed for offenses that involve either the rights of God or the rights of individuals and for which no fixed legal punishment (ḥadd) or expiation exists. Taʿzīr penalties vary in form, and their purpose is to prevent the commission of crimes or reduce them as much as possible.

Thus, the violation of others' privacy in cyberspace is considered a crime falling within the scope of taʿzīr, and it is therefore within the jurisdiction of the competent court to determine an appropriate and deterrent punishment for the offender, in order to prevent recurrence of such offenses. **(Al-Shahat, 2011, p. 90)**

3. The Impact of Technology on Privacy in Cyberspace :

In recent years, there has been a significant breakthrough in the field of information, characterized by a convergence between the phenomena of the information explosion and the communication revolution. This development has focused on the remote processing of information through the use of satellites and computer systems.

Such information or data constitutes the subject matter of crimes involving violations of privacy in cyberspace, particularly through the breach of confidentiality of information and data stored within information systems. An information system is defined as a set of human, material, technical, organizational, and cognitive components that interact and work together in order to carry out the processes of data collection, information processing, and dissemination.**(Abdel Halim, 2018, p.74)**

Determining the nature of the impact of modern technology, primarily represented by the Internet, on the right to privacy is not an easy task. This is because the type and extent of this impact vary from one society to another, depending on its prevailing cultural and moral values. Some individuals, for instance, share personal and family photographs on social networking platforms for purposes of social interaction, while others openly disclose their inner feelings to strangers within the digital space. Hence, the element of relativity within each society becomes clearly evident.

Modern technology exerts a significant and potentially serious influence on private life. Computer and Internet-related crimes constitute an intelligent form of criminal behavior that occurs within an electronic and digital environment. Such crimes are committed by individuals

with a high level of intelligence and technical expertise, using advanced technological tools. As a result, they cause harm and losses to society as a whole at various levels**.(Al-Nimr, 2017, p.64)**

Information represents the lifeblood of systems; therefore, it has become essential to preserve the integrity of information and prevent any forms of attack directed against it, whether through destruction and sabotage or through alteration and falsification, particularly when such information relates to individuals' private and personal lives. This necessity has become even more pressing with the emergence of what is known as "electronic armed robbery," which aims at capturing or recording electronically processed information and data during their transmission and broadcasting from computers through remote processing.

Consequently, any person with a certain level of technical knowledge of computer systems may be capable of infringing upon computer data and information, which may represent the personal life of the entity for which they work. Such acts may include multiple forms of violations, such as the insertion of false data and information, manipulation of data, or what is referred to as information fraud. **(Ayoub, 2009, p.141-144)**

When individuals use Internet websites, they tend to expect a greater degree of anonymity in their activities than they would in the physical world. In the latter, their presence can be observed and monitored by others. Unless a person discloses their personal data, they assume that no one will know who they are or what they are doing.

However, cyberspace—particularly the Internet—creates a range of new challenges for privacy protection. Among the most prominent of these challenges is that information systems significantly increase the volume of data collected and processed, while also enabling the flow of information and communications across borders without regard to geography or national sovereignty.

Individuals provide their data to both domestic and foreign entities, which raises serious risks regarding the use of such data, especially in countries where adequate legal frameworks for personal data protection are not in place**.(Lami, 2017, p.50-51)**

The development of technologies and Internet-based communication tools has contributed to the proliferation of various forms of privacy violations, particularly through the use of such technologies to eavesdrop on individuals, intercept their communications and confidential information, and track their activities, whether by governments or private individuals.

Violations of the right to privacy on the Internet also occur in multiple forms through advanced surveillance technologies, or through interference in information systems via hacking and unauthorized access, as well as the monitoring and interception of computer systems **.(Al-Nimr, 2017, p.66)**

4. Sources of Threats to Privacy in Cyberspace:

There is no doubt that technological development has many advantages and benefits; however, it also has disadvantages, particularly when it concerns personal information that affects individuals' private lives. Awareness of the dangers posed by computers to the right to privacy began to emerge in Western countries more than thirty years ago. Voices advocating for the protection of privacy grew louder in response to the risks associated with automated processing of personal data.

The first significant step in this regard was taken in France, where a law was enacted on 6 January 1978 aimed at protecting private life from the risks of information technology. This law established a number of offenses punishable by law in cases where certain rules are not respected during the collection of information, as well as during the processing and storage stages within computer memory.**(Al-Aakoum, 2004, p.16)**

As Internet crimes are relatively recent offenses, specifically classified as high-technology crimes, existing penal laws in their current form are often considered insufficient and not

adequately effective in addressing this new form of criminality. Consequently, many legal scholars face considerable difficulties in understanding the nature, motives, and characteristics of such crimes, particularly in light of the rapid and extensive development in the use of the Internet, as well as the increasing diversity and complexity of methods used in committing modern technological offenses.**(Herwal, 2014,p.14)**

Moreover, risks arise from the collection of information via the Internet, even for a short period of time, as this may lead to the aggregation of personal data and information about the user. Such data may then be exploited to construct a profile of the individual, thereby turning it into a tool of control and surveillance in the hands of both governments and private actors.

As a result, the threat posed by the Internet to individuals' private lives has become an established fact. The Internet has succeeded in overcoming the barriers of distance, thereby amplifying the potential for intrusion into personal privacy. **.(Al-Nimr, 2017, p.69)**

There are numerous ways in which computer systems may threaten individuals' right to privacy. However, the fundamental issue lies in the fact that anyone who possesses access to data keys within a computer system is able to collect extensive personal information about a specific individual in a manner that was previously impossible.

The danger is further amplified by the possibility that the information used may be inaccurate. One of the primary manifestations of the risks posed by information systems to the right to privacy is the ease of access to individuals' personal data within the unified system of data banks. This risk is exacerbated by the possibility of breaching these databases via the Internet.

In some cases, the perpetrator may go beyond mere access to information and deliberately manipulate, destroy, or exploit such data for financial gain, particularly through blackmailing individuals to whom the data relates. **(Abdel Halim, 2018, p.82)**

One of the risks associated with the Internet is the act of hacking, which involves unauthorized access, intrusion, or unlawful persistence within a private communication system. Such activities may also include the collection of information about the private lives of others through intelligent software that is delivered via email or disguised as malicious links.

These tools are capable of spying on users and tracking their web browsing activity through Internet directories or newsletter lists. The most significant forms of threats to privacy in cyberspace are manifested through the interception and monitoring of Internet communications, in addition to the unauthorized intrusion into information systems. **.(Al-Nimr, 2017, p.72)**

4.1. The main features of the risks posed by computers and data banks to the right to private life can be summarized as follows: (Al-Mousawi, 2013, p.10-11)

4.1.1. Many large institutions, including both governmental and private companies, collect extensive and detailed data about individuals relating to their financial, health, educational, or family status.

4.1.2. The widespread use of digital data transmission has created a security problem, as it has facilitated electronic eavesdropping and cyber-espionage. In the field of data transmission, threats to privacy arise from the inability of communication networks to provide absolute or complete security for the confidentiality of transmitted data.

4.1.3. One of the most significant risks posed by data banks to private life is the possibility that they may contain inaccurate or incomplete information that has not been properly updated or corrected.

4.1.4. Personal information that was previously isolated, fragmented, and difficult to access has become, in the digital environment, aggregated, readily available, and easily accessible, making it more susceptible than ever to use for surveillance purposes.

4.1.5. The integration of computing, communications, and multimedia technologies has enabled highly advanced surveillance tools, including audio, visual, and textual

monitoring systems, in addition to automated tracking and data collection software.

In sum, information systems constitute a threat and risk to individuals' privacy due to the diversity of personal data and the multiplicity of its sources. In many cases, such data is provided by individuals themselves when obtaining various official documents from different administrative bodies. This risk is further heightened by the ease and speed with which such information can be transmitted.

In the digital world and within global information networks, users leave numerous traces and indicators that are linked to them in the form of digital records, including the websites they visit, the time spent online, the information they search for, the materials they download, the messages they send, as well as the services and goods they request or purchase. All of these constitute personal-content records related to individuals. Moreover, browsing and navigating the Internet generates substantial amounts of information on the visited websites.

II. Results and discussion :

The study reached a set of findings, the most notable of which are:

- The findings revealed that the right to privacy in cyberspace has become a fundamental right increasingly exposed to growing challenges as a result of rapid technological development and the expanding use of information systems. They also indicated that the concept of privacy is no longer a fixed traditional notion, but rather a flexible one shaped by the nature of societies as well as their technological and cultural advancement.
- The findings further confirmed that Islamic law preceded modern legal systems in establishing the principle of protecting private life and safeguarding individuals' secrets, through texts and rulings that prohibit espionage and criminalize violations of privacy.
- The study also demonstrated that the most prominent threats to digital privacy include cyber intrusions, the collection and processing of data without adequate legal or ethical safeguards, as well as the continuous surveillance of users across digital networks. Moreover, the weakness of legal frameworks in some countries exacerbates the risks associated with personal data protection.
- Finally, the findings emphasized the necessity of strengthening legislative frameworks and security technologies, alongside promoting societal awareness, in order to ensure effective protection of digital privacy and to achieve a balance between technological advancement and the safeguarding of individuals' fundamental rights.

III. Conclusion:

In light of the foregoing discussion, it becomes evident that privacy in cyberspace has emerged as a highly complex legal, ethical, and technological issue, as a result of the rapid development of information systems and the widespread use of the Internet across various spheres of life. The study has shown that the right to privacy is no longer confined to its traditional scope, but is now closely linked to the protection of personal data and digital information within an increasingly open environment characterized by the fast and extensive circulation of data through global networks. It has also highlighted that Islamic law has given considerable attention to safeguarding private life and protecting individuals' secrets, in harmony with modern principles of privacy protection. Nevertheless, technological advancement has generated significant challenges, particularly electronic surveillance, hacking, and data misuse, which necessitate the strengthening of legal, technical, and ethical frameworks to ensure effective protection of digital privacy and to achieve a balance between technological progress and the safeguarding of fundamental human rights.

- **Referrals and references:**

- **Books :**

1. Al-Zuabi, Ali Ahmed (2006), **Right to Privacy in Criminal Law – A Comparative Study, First Edition,** Modern Book Institution, Tripoli, Lebanon.
2. Al-Ahwani, Hossam El-Din Kamel (n.d**.), The Right to Respect Private Life – The Right to Privacy: A Comparative Study**, Dar Al-Nahda Al-Arabia, Cairo, Egypt.
3. Abdel Halim, Djamal Saleh (2018), **Criminal Protection of the Right to Privacy in Relation to Information Systems**, First Edition, Dar Al-Nahda Al-Arabia, Cairo, Egypt.
4. Hegazy, Mostafa Ahmed Abdel Jawad (2004), **Civil Liability of Journalists for Violating the Sanctity of Private Life**, Dar Al-Nahda Al-Arabia, Cairo, Egypt.
5. Ayoub, Pauline Antonius (2009), **Legal Protection of Private Life in the Field of Informatics – A Comparative Study**, First Edition, Al-Halabi Legal Publications, Beirut, Lebanon.
6. Al-Nimr, Walid Salim (2017), **Privacy Protection on the Internet, First Edition**, Dar Al-Fikr Al-Jami'i, Alexandria, Egypt.
7. Qarra, Amal (2007**), Criminal Protection of Informatics in Algerian Legislation**, Second Edition, Dar Houma Printing, Publishing and Distribution, Algeria.
8. Al-Jundi, Husni (1993), **Safeguards of the Sanctity of Private Life in Islam, First Edition**, Dar Al-Nahda Al-Arabia for Publishing and Distribution, Cairo, Egypt.
9. Al-Shahat, Ibrahim Muhammad Mansour (2011), **Electronic Crimes in Islamic Sharia and Positive Law: A Comparative Jurisprudential Study**, First Edition, Dar Al-Fikr Al-Jami'i, Cairo, Egypt.
10. Al-Akoum, Walid (2004), **The Concept and Phenomenon of Cybercrime, Third Edition, Proceedings of the Conference on Law, Computers and the Internet**, College of Sharia and Law, United Arab Emirates University.

- **Theses and Dissertations:**

1. Herwal, Hiba Nabila (2013/2014), **Internet Crimes – A Comparative Study, PhD Thesis, Faculty of Law and Political Science**, University of Abou Bekr Belkaid, Tlemcen, Algeria.
2. Lami, Muntadhar Abdul Wahab (2017), **The Crime of Privacy Violation via Electronic Means in Jordanian Legislation – A Comparative Study**, Faculty of Law, Middle East University, Amman, Jordan.

- **Journal article:**

1. Al-Mousawi, Mona Turki & Fadlallah, Jean Cyril (2013**), Informational Privacy and Its Importance and Risks of Modern Technology**, Market Research and Consumer Protection Center, Baghdad College Journal of Economic Sciences University, Baghdad, Iraq.