International Journal of Law Research and Studies (IJLRS)

المجلة الدولية للبحوث والدراسات القانونية

Vol. (5), No. (10)

IJLRS

October 2026

الإصدار (5)، العدد (10)

Cybercrimes Involving Violations of the Right to Privacy

Ghada Abdullah Alshenqiti
Master's in Public Law, College of Law, Taibah University, Saudi Arabia
ghadashenqiti@gmail.com

Abstract

This research examines cybercrimes involving violations of the right to privacy, focusing on their legal nature, constituent elements, and common forms. Using historical, descriptive, and analytical legal methods, the study explores the development of privacy protection and the challenges posed by technological advancements. It also examines the legal framework governing privacy-related cybercrimes in Saudi Arabia, with particular reference to relevant legislation and judicial applications. The findings demonstrate that privacy-related cybercrimes encompass distinct forms of unlawful conduct requiring careful examination of their statutory elements. They further highlight the complementary roles of criminal legislation, personal data protection, and cybersecurity measures in safeguarding privacy. The study emphasizes the importance of legal awareness, accurate application of criminal provisions, and continued consideration of emerging technological challenges.

Keywords: Right to Privacy, Cybercrime, Criminal Liability, Personal Data Protection, Saudi Law.

Introduction

The increasing reliance on digital technology has brought the protection of private life into sharper focus. As individuals conduct more of their personal and professional activities through electronic systems, information once confined to private spaces may become vulnerable to unauthorized access, surveillance, and disclosure. These developments have created new challenges for the law, particularly in addressing conduct that may infringe upon privacy through technological means.

Although the right to privacy is firmly established as a legally protected interest, its protection in the digital environment requires consideration of circumstances that differ from those traditionally associated with interference in private life. The methods through which violations may occur, the nature of the information involved, and the potential consequences of its misuse raise questions concerning the scope of criminal protection and the application of existing legal provisions.

These questions are particularly relevant to Saudi Arabia, where the legal framework addresses privacy-related misconduct through criminal legislation and complementary measures concerning personal data and cybersecurity. Understanding how these provisions operate, both independently and collectively, is essential to examining the legal protection afforded to individuals against privacy-related cybercrimes.

Against this background, the present research examines privacy violations in the context of cybercrime, focusing on their legal foundations, constituent elements, common forms, and treatment

under Saudi law. Through an analysis of relevant legislation and judicial applications, the study seeks to provide a structured examination of the legal issues arising from technologically facilitated interference with private life.

Significance of the Research

The significance of this research lies in its examination of privacy as a legally protected interest within the context of technological development.

From a theoretical perspective, the research contributes to understanding the legal concept of privacy and the relationship between conventional forms of interference and those facilitated by information technologies. It also examines the distinction between the different forms of conduct capable of affecting private life and the legal conditions governing criminal responsibility.

From a practical perspective, the research clarifies common forms of privacy-related cybercrime and the legal provisions applicable to them. It also examines the Saudi legal framework governing such conduct, including the relationship between criminal sanctions, personal data protection obligations, and preventive cybersecurity measures.

Furthermore, the analysis of judicial applications contributes to understanding how relevant legal provisions have been applied to particular circumstances and the importance of distinguishing between different forms of legal liability.

Research Objectives

1. Examine the concept of the right to privacy, its legal significance, historical development, and the contemporary challenges affecting its protection.
2. Define privacy-related cybercrimes and analyze their constituent elements, with particular attention to Actus Reus (The Material Element) and Mens Rea (The Mental Element).
3. Identify and examine common forms of technologically facilitated privacy violations, including interference with image rights, electronic surveillance, unauthorized access to information systems, unlawful interference with personal data, and violations of private electronic communications.
4. Analyze the Saudi legal framework governing privacy-related cybercrimes, particularly the relevant provisions of the Anti-Cyber Crime Law.
5. Examine the complementary role of the Personal Data Protection Law and national cybersecurity measures in protecting privacy within digital environments.
6. Analyze selected Saudi judicial applications to illustrate the interpretation and application of relevant legal provisions.

Research Problem

The central problem addressed by this research concerns the legal protection of privacy against forms of interference facilitated by information and communication technologies.

Although the right to privacy has long been recognized within legal systems, the development of digital technologies has introduced methods of interference that differ from conventional violations in their technical characteristics, potential scope, and means of execution.

These developments raise questions concerning the legal classification of privacy-related conduct, the constituent elements required to establish criminal liability, and the extent to which existing legislation accommodates emerging technological practices.

Within the Saudi legal system, an additional issue concerns the relationship between the criminal provisions of the Anti-Cyber Crime Law and the broader obligations established under the Personal Data Protection Law and cybersecurity regulations.

Accordingly, the central research problem may be expressed through the following question:

To what extent does the Saudi legal framework provide protection against privacy-related cybercrimes, particularly in light of the evolving forms of technologically facilitated interference with private life?

Research Questions

1. What is the legal concept of the right to privacy, how has it developed, and what contemporary challenges affect its protection?
2. How are privacy -related cybercrimes defined, and what are the legal requirements of their material and mental elements?
3. What are the common forms of privacy -related cybercrime, and how have technological developments influenced their methods and characteristics?
4. How does Saudi criminal legislation address conduct involving unauthorized surveillance, access to information, misuse of digital images, and interference with private communications?
5. What role do personal data protection legislation and cybersecurity measures play in complementing criminal protection of privacy in Saudi Arabia?
6. What can be established from selected Saudi judicial applications concerning the legal treatment of privacy -related cybercrimes?

Research Methodology

This research adopts a combination of historical, descriptive, and analytical legal methodologies. The historical method is employed to examine the development of the right to privacy and the evolution of its legal recognition. The descriptive method is used to identify the characteristics of privacy-

related cybercrimes and explain the technological methods through which interference with private life may occur. The analytical legal method is applied to examine the constituent elements of relevant offences, interpret applicable legislative provisions, and distinguish criminal liability from other forms of legal responsibility. The research also incorporates an examination of selected judicial applications to illustrate the practical application of relevant provisions within the Saudi legal system.

Research Structure

Chapter One: The Nature of the Right to Privacy:

- Section One: The Concept and Significance of the Right to Privacy.
- Section Two: The Historical Development of the Right to Privacy.
- Section Three: Contemporary Threats to the Right to Privacy.

Chapter Two: The Nature and Constituent Elements of Privacy-Related Cybercrimes:

- Section One: The Concept of Privacy-Related Cybercrimes.
- Section Two: The Constituent Elements of Privacy-Related Cybercrimes.

Chapter Three: Common Forms of Cybercrimes Involving Violations of Privacy:

- Section One: Violations of the Right to One's Image.
- Section Two: Electronic Surveillance and Spyware.
- Section Three: Unauthorized Access to Information Systems.
- Section Four: Unlawful Interference with Personal Data.
- Section Five: Violations of Private Electronic Communications.

Chapter Four: Legal Protection Against Privacy-Related Cybercrimes in Saudi Arabia:

- Section One: Criminal Protection under the Anti-Cyber Crime Law.
- Section Two: Complementary Personal Data Protection and Cybersecurity Measures.
- Section Three: Judicial Applications.

Conclusion.

Research Findings.

Recommendations.

Chapter One: The Nature of the Right to Privacy

Human beings differ in their lifestyles, personal characteristics, cultural backgrounds, beliefs, and individual preferences. These differences influence the boundaries individuals establish between their private and public lives and, consequently, their understanding and exercise of the right to privacy. Accordingly, examining the nature of this right requires consideration of its legal foundations, conceptual scope, and relationship with other fundamental rights [1].

Islamic law has long addressed matters relating to personal privacy through principles derived from the Holy Qur'an, the Sunnah of the Prophet Muhammad, the practices of his Companions, and subsequent Islamic jurisprudence. These sources contain provisions concerning the protection of private life and the regulation of interference with individual privacy [2]. Nevertheless, defining the precise scope of the right to privacy remains challenging, particularly because it encompasses various personal interests that may overlap with other individual rights and public interests [3].

This chapter examines the nature of the right to privacy through three sections. The first addresses its concept and significance, the second traces its historical development, and the third examines the principal threats to its protection.

Section One: The Concept and Significance of the Right to Privacy

An examination of this right therefore requires an understanding of both its legal meaning and its underlying significance. Accordingly, this section is divided into two subsections. The first considers the concept and definition of the right to privacy, while the second addresses its importance to individuals and society.

The right to privacy is a fundamental aspect of individual rights and personal autonomy. Although individuals participate in social relationships and engage in public activities, they also maintain aspects of their lives that they may reasonably wish to protect from unwanted observation, disclosure, or interference. The recognition of a protected private sphere reflects the need to preserve individual dignity, autonomy, and personal freedom [4].

Subsection One: The Concept of the Right to Privacy:

An examination of the right to privacy requires an initial clarification of the concept of a right within linguistic and legal discourse.

---

[1] Sassi, Boubaker, Etouchen, and Slimani, Criminal Protection of Private Life on the Internet, Master's Thesis, Faculty of Law and Political Science, Abderrahmane Mira University, Bejaia, Algeria, 2012–2013, p. 1.

[2] Khalaf Allah, Zahra, Criminal Protection Against Violations of the Right to Privacy, Master's Thesis, Faculty of Law and Political Science, Dr. Moulay Tahar University, Algeria, 2016–2017, pp. 1–2.

[3] Al-Ustadh, Suzan Adnan, "Violation of the Right to Privacy on the Internet," Damascus University Journal of Economic and Legal Sciences, Damascus, Syria, No. 3, 2013, p. 427.

[4] Al-Zoubi, Ali Ahmed, The Right to Privacy in Criminal Law, PhD Dissertation, Faculty of Law, University of Mosul, Mosul, Iraq, 2004, p. 4.

From a linguistic perspective, the term right encompasses several meanings relating to truth, validity, certainty, and legitimacy. These meanings generally reflect the recognition of something as valid, established, or justified [5]. In legal terminology, certain jurists have defined a right as a legally recognized power or entitlement that enables an individual to exercise authority or make claims in relation to the conduct of others, with the recognition and protection of the legal system [6].

The term private life similarly requires conceptual clarification. Although linguistic dictionaries do not necessarily provide a unified definition of private life as a distinct legal concept, they address the meaning of privacy and related terms. Privacy generally refers to matters that are particular to an individual and distinguished from those belonging to the public sphere. From this linguistic perspective, private life may be understood as the sphere of personal affairs that an individual seeks to maintain independently of unwarranted interference by others [7].

Despite this linguistic foundation, the legal concept of privacy remains difficult to define comprehensively. One of the principal reasons for this difficulty is the evolving character of private life and the absence of universally fixed boundaries between private and public matters. The meaning and scope of privacy may vary according to personal circumstances, cultural expectations, social practices, and historical developments. Consequently, attempts to establish a single definition capable of encompassing all dimensions of privacy have encountered substantial conceptual and legal challenges [8].

Legal approaches to privacy have generally differed in the extent of the protection they recognize. Some adopt a broad interpretation that associates privacy with personal liberty and individual autonomy, while others employ a narrower approach that emphasizes seclusion, solitude, and freedom from unwanted intrusion [9]. Although numerous legal systems expressly recognize and protect aspects of private life, many legislative documents do not provide an exhaustive definition of privacy. Instead, the interpretation and determination of its boundaries are frequently left to legal scholarship and judicial decisions.

[5] Al-Zaidi, Taha Ahmed, Provisions Governing Information Crimes in Islamic Jurisprudence and Law, Dar Al-Fajr for Printing and Publishing, Baghdad, Iraq, 1st ed., 1438 AH/2017, p. 127.
[6] Al-Wuhaibi, Ali Saleh Rashid, Criminal Protection of Private Life under Islamic Law and Positive Laws, Master's Thesis, Naif Arab University for Security Sciences, Riyadh, Saudi Arabia, 1422 AH/2001, p. 26.
[7] Ajali, Criminal Protection Against Forms of Infringement of Private Life through Telephone Calls and Images, op. cit., p. 34.
[8] Al-Nasiri, Nour El-Din, "The Legal Framework of the Right to Privacy," Journal of Jurisprudence and Law, Morocco, No. 9, 2013, p. 6.
[9] Salman, Ouda Youssef, "Crimes Violating the Right to Privacy through Modern Information Technology," Journal of Law, Iraq, Nos. 29–30, 2017, pp. 4–5.

This legislative approach has contributed to variations in the legal understanding of privacy, as scholarly interpretations and judicial assessments may be influenced by differences in social values, cultural traditions, moral considerations, and the circumstances of particular cases [10].

Legal scholars have consequently proposed different definitions of private life. These definitions may be broadly distinguished according to whether they adopt a negative or positive conceptual approach.

Under the negative approach, privacy is defined by reference to matters falling outside the public sphere. The French jurist Robert Badinter, for example, has been associated with an understanding of private life as encompassing matters that do not belong to public life. This approach identifies the private sphere primarily through its distinction from public activities and interests.

By contrast, the positive approach seeks to identify the substantive interests protected by the right to privacy. A definition attributed to the jurist Michel emphasizes the individual's interest in solitude, intimacy, anonymity, and discretion. Under this interpretation, privacy is not merely the absence of publicity but also the ability to maintain a personal sphere free from unwanted external involvement [11].

A further approach defines privacy through the forms of interference that may constitute its violation. The American Law Institute, in its treatment of invasion of privacy, addresses wrongful and serious interference with an individual's interest in preventing private affairs from becoming known to others, as well as the unauthorized exposure of an individual's image or person to public attention [12].

For the purposes of the present study, the latter approach is particularly relevant because it focuses on conduct that may constitute an infringement of privacy. Examining privacy through the nature and consequences of interference provides a useful analytical framework for identifying potentially unlawful intrusions and evaluating the legal mechanisms available for protecting private life.

Nevertheless, an infringement-based approach should be understood as a framework for examining violations of privacy rather than necessarily as a comprehensive definition of the right itself.

Subsection Two: The Significance of the Right to Privacy:

The right to privacy is closely associated with human dignity, personal autonomy, and the protection of individual identity. It safeguards aspects of personal life that individuals may legitimately seek to preserve from unwanted scrutiny, disclosure, or interference. Privacy therefore serves as an important condition for the exercise of individual freedom and the development of personal relationships [13].

[10] Abu Aoun, Basel, Crimes Infringing the Right to Privacy, Master's Thesis, Faculty of Law and Political Science, Mohamed Khider University, Biskra, Algeria, 2016–2017, p. 11.
[11] Jallad, Salim, The Right to Privacy: Guarantees and Limitations under Algerian Legislation and Islamic Jurisprudence, PhD Dissertation, Faculty of Humanities and Islamic Civilization, University of Oran, Algeria, 2013, pp. 13–14.
[12] Othman, Tarek, Criminal Protection of Private Life on the Internet, Master's Thesis, Faculty of Law and Political Science, Mohamed Khider University, Biskra, Algeria, 2006–2007, p. 10.
[13] Ben Haida, Mohamed, Protection of the Right to Privacy under Algerian Legislation, PhD Dissertation, Faculty of Law and Political Science, Abou Bekr Belkaid University, Tlemcen, Algeria, 2016–2017, p. 4.

Although individuals are social by nature and participate in collective life, meaningful social participation does not eliminate the need for personal space and confidentiality. Individuals may wish to conduct certain activities independently, maintain personal relationships outside public observation, or preserve the confidentiality of their thoughts, emotions, and personal information. The protection of these interests contributes to the individual's capacity to exercise autonomy and maintain a distinct personal identity.

The close relationship between privacy and the individual has been emphasized in legal scholarship. In this context, Dr. Abdel Moneim Al-Sawi described privacy in terms that associate it directly with the human person, thereby highlighting its fundamental connection to individual identity and dignity [14].

The importance of privacy extends beyond the protection of personal information or physical seclusion. It also has psychological and social dimensions. The ability to maintain a private sphere may contribute to emotional well-being, psychological security, and personal stability. When individuals have reasonable opportunities to withdraw from public observation and manage their personal affairs independently, they may experience greater freedom in their thoughts, conduct, and personal relationships.

These conditions can support individual development and participation in social, professional, and community activities. Conversely, persistent interference with private life may undermine personal autonomy, create feelings of insecurity, and discourage individuals from engaging freely in otherwise lawful activities [15].

Privacy also has a broader societal significance. The protection of private life contributes to an environment in which individuals can exercise their rights without disproportionate surveillance or unjustified interference. It may therefore support interpersonal trust, social stability, and respect for individual freedoms.

From this perspective, the legal recognition of privacy is relevant not only to individual welfare but also to the broader institutional protection of fundamental rights. Legal systems that establish clear safeguards against arbitrary interference with private life contribute to the protection of human dignity and the rule of law [16].

Accordingly, the right to privacy should not be understood exclusively as an individual interest. Its recognition and effective protection also have implications for society as a whole, particularly in

[14] Mohamed, Mohamed Nasr, The Human Right to the Protection of Private Life under International Law and Domestic Legislation, Law and Economics Library, Riyadh, Saudi Arabia, 1st ed., 1434 AH/2013, p. 32.
[15] Mohamed, The Human Right to the Protection of Private Life under International Law and Domestic Legislation, op. cit., pp. 31–32.
[16] Ajali, Criminal Protection Against Forms of Infringement of Private Life through Telephone Calls and Images, op. cit., p. 12.

relation to the protection of civil liberties and the relationship between individuals and public authorities.

Despite its significance, the right to privacy has become increasingly vulnerable to interference as a result of technological developments and changing social conditions. The development of sophisticated methods of observation, recording, communication, and information processing has introduced additional challenges to the effective protection of private life. These challenges will be examined in subsequent sections.

Section Two: The Historical Development of the Right to Privacy

The protection of private life has developed gradually through different legal and social traditions. Although contemporary legal systems recognize privacy as an important individual right, its historical foundations can be traced to earlier rules concerning the protection of the home, personal security, and freedom from unauthorized interference.

In many early legal systems, the protection of what would now be regarded as privacy-related interests was limited in scope. Particular emphasis was placed on the security and inviolability of the home, which constituted an important setting for personal and family life. However, these early forms of protection did not necessarily amount to recognition of an independent and comprehensive right to privacy [17].

Understanding the development of this right therefore requires an examination of the different stages through which legal protection evolved. This section considers three principal historical contexts: ancient legal systems, Islamic law, and modern legislation.

Subsection One: The Right to Privacy in Ancient Legal Systems:

In ancient legal systems, legal protection associated with private life was primarily concerned with the home and its physical security. Such protection generally addressed particular forms of unauthorized entry or interference with residential property rather than recognizing privacy as a distinct and comprehensive personal right [18].

The early development of these protections can be examined through ancient Eastern legal codes, particularly the Code of Hammurabi and the Laws of Manu, followed by selected Western legal traditions, including ancient Greek, Roman, and Germanic law.

1. Ancient Eastern Legal Systems:

The Code of Hammurabi, promulgated in ancient Mesopotamia during the reign of King Hammurabi, is among the earliest surviving comprehensive legal collections. It contained provisions regulating various forms of conduct, including offences involving the unlawful entry of residential premises.

[17] Khalaf Allah, Criminal Protection Against Violations of the Right to Privacy, op. cit., p. 93.
[18] Akli, Fadila, Legal Protection of the Right to Privacy, PhD Dissertation, Faculty of Law, University of Mentouri Brothers, Constantine, Algeria, 2011–2012, p. 4.

Under the provision commonly translated as addressing the act of making a breach in a house for the purpose of burglary, the offender was subject to capital punishment. The relevant rule prescribed punishment for a person who created an opening in a house to facilitate unlawful entry and theft [19].

This provision indicates that ancient Mesopotamian law recognized the need to protect residential premises against certain forms of unlawful intrusion. However, its principal concern appears to have been the prevention and punishment of conduct associated with burglary and the physical security of the dwelling. It would therefore be difficult to characterize this provision as establishing a general right to personal privacy in the contemporary legal sense.

The Laws of Manu, associated with ancient Indian legal traditions, also contained rules concerning unauthorized interference with residential premises. Compared with provisions primarily directed at burglary, these rules addressed a broader range of conduct relating to entry into and presence within another person's property.

The protections described in this legal tradition extended to unauthorized entry and remaining on residential premises without the consent of the occupant, including certain areas associated with the dwelling, such as courtyards and surrounding grounds [20].

These provisions illustrate an early recognition of interests connected with the control of access to residential spaces, although their historical purposes and legal contexts differed from those of modern privacy law.

2. Ancient Western Legal Systems:

Ancient Western legal traditions also developed rules concerning the protection of residential premises, although the nature and extent of those protections differed across legal systems.

In ancient Greek law, certain rules addressed conduct involving unauthorized entry into a dwelling. Legal protection was associated with acts such as creating an opening in a house to facilitate unlawful entry. Such provisions suggest a concern with the physical security of residential property, broadly comparable to certain protections found in ancient Eastern legal systems [21].

Roman law contributed to the development of legal concepts concerning personal security and the protection of the home. In Roman legal thought, the dwelling occupied an important position in both domestic and social life, and certain forms of unlawful intrusion could be understood as affecting interests extending beyond physical property.

The treatment of interference with residential premises increasingly reflected the relationship between the dwelling and the personal interests of its occupants. Thus, protection could be understood as

[19] Mohamed, The Human Right to the Protection of Private Life under International Law and Domestic Legislation, op. cit., pp. 42–43.
[20] Akli, Legal Protection of the Right to Privacy, op. cit., pp. 5–6.
[21] Khalaf Allah, Criminal Protection Against Violations of the Right to Privacy, op. cit., p. 16.

extending beyond material damage to encompass aspects of personal security and the interests of the individual affected by the intrusion.

Ancient Germanic legal traditions similarly recognized the importance of domestic security and the maintenance of peace within the home. Certain Germanic legal rules treated unauthorized interference with a dwelling as conduct affecting the security and tranquility associated with residential occupation. In this respect, the protected interest was not limited to the physical structure of the home but also concerned the occupant's interest in remaining undisturbed within that space. The recognition of interference with the home as a distinct legal wrong represented a further development in the historical protection of interests associated with private life [22].

Taken together, these ancient legal traditions demonstrate that the protection of residential premises constituted an important historical foundation for later privacy-related legal principles. However, the recognition of domestic security should be distinguished from the modern concept of privacy, which encompasses a substantially broader range of personal, informational, and relational interests.

Subsection Two: The Right to Privacy in Islamic Law:

Islamic law provides a comprehensive legal and ethical framework for the protection of individual privacy. The principles governing private life are derived primarily from the Holy Qur'an and the Sunnah of the Prophet Muhammad, together with their interpretation and application in Islamic jurisprudence. These sources establish rules concerning the inviolability of the home, the confidentiality of personal affairs, and protection against unjustified interference with individual privacy [23].

One of the principal aspects of privacy protection in Islamic law is the requirement to obtain permission before entering another person's dwelling. This principle is expressly recognized in the Holy Qur'an [24], establishing with this provision a clear foundation for respecting residential privacy by prohibiting unauthorized entry into another person's home. Its significance extends beyond the physical protection of residential premises, as it also recognizes the importance of maintaining the privacy and security of domestic life.

Furthermore, Islamic law addresses other forms of interference with private life, including unjustified surveillance, intrusion into personal affairs, and the unauthorized disclosure of confidential information. These protections reflect the broader Islamic principle of respecting human dignity and safeguarding individuals against unwarranted interference [25].

[22] Akli, Legal Protection of the Right to Privacy, op. cit., pp. 17–18.
[23] Ajali, Criminal Protection Against Forms of Infringement of Private Life through Telephone Calls and Images, op. cit., pp. 43–45.
[24] The Holy Qur'an, Surah An-Nur, verse 27.
[25] Ajali, Criminal Protection Against Forms of Infringement of Private Life through Telephone Calls and Images, op. cit., pp. 43–45.

The protection of privacy under Islamic law is not restricted to a particular social or economic category. Rather, the underlying principles apply to individuals regardless of their wealth, age, gender, or social position. This reflects the general recognition of human dignity as an essential consideration in Islamic legal and ethical teachings [26].

Accordingly, the right to privacy in Islamic law may be understood as an aspect of the broader protection afforded to human dignity, personal security, and individual autonomy. Its recognition provides a legal and ethical foundation for examining the protection of private life and the circumstances under which interference with this right may be justified.

Subsection Three: The Right to Privacy in Modern Legislation:

The legal protection of privacy underwent substantial development with the emergence of modern constitutional systems and international human rights documents. During the twentieth century, privacy increasingly became recognized as an independent legal interest requiring protection against arbitrary or unlawful interference.

This development occurred at both international and domestic levels. International documents established general standards for the protection of private life, while national constitutional and legislative systems introduced provisions addressing privacy and related individual rights.

1. International and Regional Protection of the Right to Privacy:

At the international level, the Universal Declaration of Human Rights, adopted in 1948, represents an important milestone in the formal recognition of privacy as a human right.

Article 12 of the Declaration provides protection against arbitrary interference with an individual's privacy, family, home, or correspondence, as well as attacks upon honor and reputation. It also recognizes the individual's entitlement to legal protection against such interference or attacks [27].

Although the Universal Declaration is not itself a legally binding treaty, it established an influential international standard for the protection of fundamental rights and contributed to the subsequent development of international human rights law.

At the regional level, the European Convention on Human Rights, adopted in 1950, expressly recognizes the right to respect for private and family life.

Article 8 of the Convention protects the right to respect for private and family life, home, and correspondence. It also establishes conditions under which public authorities may lawfully interfere with the exercise of this right, subject to requirements relating to legality, legitimate aims, and necessity in a democratic society [28].

[26] Mohamed, The Human Right to the Protection of Private Life under International Law and Domestic Legislation, op. cit., p. 49.
[27] Akli, Legal Protection of the Right to Privacy, op. cit., p. 30.
[28] Lami, The Crime of Violation of Privacy through Electronic Means under Jordanian Legislation, op. cit., p. 74.

The European Convention therefore provides a legal framework that recognizes privacy as a protected right while also addressing circumstances in which interference may be justified by competing public interests.

2. International Conferences and the Development of Privacy Protection:

In addition to international legal documents, conferences addressing human rights contributed to the growing recognition of privacy-related challenges, particularly those arising from scientific and technological developments.

The International Conference on Human Rights, held in Tehran in 1968, examined a broad range of human rights issues, including the implications of technological progress for individual rights. Among the concerns addressed during this period was the potential effect of electronic data-processing technologies on the protection of personal privacy. The growing use of computers and automated information systems raised questions concerning the collection, retention, and processing of information relating to individuals [29].

The International Conference of Non-Governmental Organizations on Human Rights, held in Montreal in 1968, also formed part of the broader international discussion concerning the protection of human rights. The recommendations attributed to the Montreal conference included concerns about the use of modern technological methods capable of interfering with private life, as well as the legal treatment of evidence obtained through intrusive techniques [30].

These developments demonstrate that concerns about technological interference with private life emerged well before the widespread adoption of the Internet and contemporary digital communication systems.

3. Constitutional Protection of Privacy in Domestic Legal Systems:

At the domestic level, constitutional recognition has played an important role in establishing privacy as a legally protected interest. Several Arab constitutions have incorporated provisions relevant to the protection of private life, the inviolability of the home, and the confidentiality of communications. The legal foundations of these protections reflect a combination of constitutional principles, domestic legal traditions, and, in certain jurisdictions, Islamic legal values.

The Egyptian Constitution of 1971 and the Jordanian Constitution of 1952 provide historical examples of constitutional frameworks that addressed aspects of individual freedom and protection against unauthorized interference.

[29] Hamidi, Rachida, Legal Protection of the Right to Privacy, Master's Thesis, Faculty of Law and Political Science, Dr. Moulay Tahar University, Algeria, 2017–2018, pp. 16–17.
[30] Al-Mohammadi, Badr Al-Din, Civil Liability Arising from Infringement of the Right to Privacy, PhD Dissertation, Faculty of Law, University of Algiers, Algiers, Algeria, 2014–2015, p. 49.

The form and extent of constitutional protection have differed across jurisdictions. Some constitutional provisions expressly recognize privacy-related rights, while others protect private life indirectly through guarantees concerning personal liberty, domestic security, or the confidentiality of correspondence [31].

Constitutional protection also involves consideration of the relationship between individual rights and legitimate public interests. Accordingly, domestic legislation may establish the conditions under which interference with privacy is legally permissible, while remaining subject to applicable constitutional requirements and safeguards.

In Western constitutional systems, the recognition of privacy has followed different legal approaches. The French Constitution of 1958 does not expressly establish a general right to privacy in the same manner as certain contemporary constitutional provisions. Nevertheless, privacy protection has developed through constitutional principles, ordinary legislation, and judicial interpretation concerning individual liberty and fundamental rights.

In the United States, the Fourth Amendment to the Constitution provides protection against unreasonable searches and seizures. Its wording expressly refers to the security of individuals in their persons, houses, papers, and effects.

Although the Fourth Amendment does not formulate a comprehensive right to privacy, it constitutes an important constitutional safeguard against certain forms of governmental intrusion and has contributed to the development of privacy-related legal protections [32].

The development of modern legislation thus demonstrates the increasingly prominent position of privacy within domestic and international legal systems. However, the scope, legal basis, and enforceability of privacy protections continue to vary across jurisdictions [33].

The recognition of privacy as a fundamental right has consequently been accompanied by continuing efforts to determine its boundaries, regulate permissible interference, and respond to technological and social developments that present new challenges to its effective protection.

Section Three: Threats to the Right to Privacy

Interference with private life is not exclusively a contemporary phenomenon. Historically, individuals have been exposed to unauthorized observation, intrusion into residential premises, and other forms of interference with personal affairs. However, technological and social developments have

[31] Al-Zoubi, The Right to Privacy in Criminal Law, op. cit., pp. 44–49.
[32] Ajali, Criminal Protection Against Forms of Infringement of Private Life through Telephone Calls and Images, op. cit., p. 4.
[33] Chouikhi, Houda, Substantive and Procedural Criminal Provisions Concerning the Right to Privacy, Master's Thesis, Faculty of Law and Political Science, Dr. Moulay Tahar University, Algeria, 2017–2018, p. 30.

transformed both the methods through which privacy may be infringed and the potential scale of such infringements [34].

Traditional forms of intrusion generally required physical proximity or direct access to an individual's private space. In contrast, contemporary technologies can facilitate the observation, collection, transmission, and processing of personal information without the individual's immediate awareness.

The resulting threats to privacy can be examined through three principal categories: modern surveillance and recording technologies, electronic information-processing systems and digital networks, and social factors that contribute to interference with private life.

Subsection One: Modern Scientific and Technological Methods:

Scientific and technological developments have provided significant benefits in communication, security, information exchange, and everyday activities. Nevertheless, certain technologies may also be used to interfere with private life, particularly when they enable observation, recording, or surveillance without the knowledge or consent of the individuals concerned.

Advancements in optical and audiovisual technologies have expanded the practical means through which individuals may be monitored. Devices such as telescopic lenses, infrared imaging systems, digital cameras, and smartphones can facilitate the observation or recording of activities that individuals may reasonably expect to remain private [35].

The development of smaller and more accessible recording equipment has further increased the potential for covert surveillance. Miniature cameras may be incorporated into everyday objects, including writing instruments and other portable devices, making unauthorized recording less readily detectable.

These technologies are not inherently unlawful or incompatible with privacy protection. Their implications depend on the circumstances of their use, the nature of the information collected, the consent of the individuals concerned, and the applicable legal framework.

Similar concerns arise in relation to audio-surveillance technologies.

Advances in electronic components, including transistors and miniaturized recording systems, have facilitated the development of devices capable of capturing conversations and transmitting audio signals. Such devices may be used to monitor private discussions or telephone communications without the knowledge of the persons involved [36].

[34] Chouikhi, Substantive and Procedural Criminal Provisions Concerning the Right to Privacy, op. cit., p. 3.
[35] Mohamed, The Human Right to the Protection of Private Life under International Law and Domestic Legislation, op. cit., pp. 59–60.
[36] Djilali, Abderrahmane, "Electronic Infringement of the Right to Privacy," Journal of Jurisprudence and Law, Morocco, No. 18, 2014, p. 86.

Certain surveillance technologies may also permit remote monitoring through the detection or transmission of signals associated with audio activity. Other devices can be concealed in clothing, vehicles, or personal belongings to facilitate the monitoring of an individual's location or movements.

The original literature also refers to specialized telephone-monitoring devices designed to intercept or transmit communications over extended distances. These technologies illustrate historical concerns surrounding unauthorized access to private communications and the difficulties individuals may face in detecting covert monitoring [37].

The privacy implications of these developments extend beyond the physical act of surveillance. Unauthorized observation or recording may result in the collection of confidential information, the disclosure of personal relationships, or the creation of records that can subsequently be retained, reproduced, or distributed.

Accordingly, the principal legal concern is not technological development itself but the potential use of technological capabilities in ways that interfere unlawfully or disproportionately with protected aspects of private life.

Subsection Two: Electronic Information-Processing Systems and Digital Networks:

The development of computers, electronic information systems, and digital communication networks has fundamentally transformed the collection, storage, processing, and exchange of information. Digital technologies have become essential to numerous areas of contemporary life, including communication, education, commerce, public administration, and social interaction. At the same time, their extensive use has introduced additional risks concerning the confidentiality, security, and accessibility of personal information.

The development of early electronic computers during the 1940s, including significant advances in 1946, contributed to the emergence of modern computing. Subsequent technological developments facilitated increasingly sophisticated methods of information processing and eventually supported the expansion of interconnected computer networks [38].

Although early computing and networking technologies were developed and used in scientific, governmental, and military contexts, their applications progressively expanded into commercial and civilian activities. The widespread adoption of these systems has substantially increased the volume of personal information that can be collected and maintained in electronic form.

A central feature of this development is the establishment of electronic databases and information systems. For the purposes of this discussion, a database may be understood as an organized collection

[37] Bahr, Mamdouh Khalil, Protection of Private Life under Criminal Law, Dar Al-Nahda Al-Arabiya, Cairo, Egypt, 1983, p. 13.
[38] Saghir, Youssef, Crimes Committed through the Internet, Master's Thesis, Faculty of Law and Political Science, Mouloud Mammeri University, Tizi Ouzou, Algeria, 2013, p. 3.

of data relating to particular subjects or purposes, capable of being stored, retrieved, and processed electronically to produce information for various users and applications [39].

Such databases may contain information concerning individuals' identities, communications, financial activities, personal relationships, and other aspects of private life. The concentration of personal data within electronic systems creates opportunities for efficient information management. However, it may also expose individuals to unauthorized access, improper disclosure, unlawful processing, and other forms of misuse.

These risks become particularly significant where information is collected or retained without adequate safeguards, or where individuals have limited knowledge of how their personal data is processed.

The expansion of digital networks has also facilitated the rapid transmission of information across geographical and institutional boundaries. While this development has improved communication and access to information, it has simultaneously introduced vulnerabilities associated with the interception, unauthorized acquisition, alteration, and dissemination of data.

Communication networks cannot be assumed to provide absolute confidentiality or protection against every form of unauthorized access. Their security depends on factors such as system design, technical safeguards, organizational practices, and the conduct of users and third parties [40].

Cybercriminal activity presents a further challenge to privacy protection. Unauthorized access to electronic systems may enable offenders to obtain personal information, compromise confidential communications, or misuse data for unlawful purposes.

Moreover, the ability to conduct certain activities remotely may complicate the identification of offenders, the investigation of incidents, and the enforcement of applicable legal rules.

Consequently, the protection of privacy in digital environments requires consideration of both legal and technical safeguards, including the regulation of personal data processing and measures intended to reduce unauthorized access to information systems.

Subsection Three: Social Factors Affecting the Right to Privacy:

In addition to technological developments, social conditions and changing patterns of human interaction may influence the protection of private life. Among the factors historically discussed in this context are developments in mass media, population growth and urbanization, and the use of advanced techniques in criminal activity.

[39] Al-Derbi, Ismail, and Abdel Aal, Mohamed Sadeq, Cybercrimes, National Center for Legal Publications, Cairo, Egypt, 1st ed., 2012, pp. 7–8.
[40] Rabie, Imad Mohamed, and Ziad Mohamed, "Infringement of the Right to Privacy under Cybercrime Law," Journal of Legal and Political Sciences, Algeria, No. 1, 2016, p. 16.

1. Mass Media and the Disclosure of Private Information:

The development of mass media has increased the capacity to collect and disseminate information concerning individuals and their personal affairs.

Traditional and modern media institutions perform important functions in informing the public and facilitating the exchange of information. Nevertheless, certain practices may give rise to privacy concerns, particularly where personal information is disclosed without sufficient justification or where reporting extends beyond matters of legitimate public interest.

The publication of information concerning an individual's personal relationships, family circumstances, or other private matters may constitute an interference with privacy, depending on the nature of the disclosure and the applicable legal standards.

Commercial incentives and competition for public attention may encourage some media outlets to prioritize material that attracts readership or audience engagement, including information concerning the private lives of individuals [41].

The resulting legal and ethical issues require consideration of the relationship between privacy protection and freedom of expression. Both interests may enjoy legal protection, and their interaction requires careful assessment of factors such as the public relevance of the information, the status of the individuals concerned, the manner in which the information was obtained, and the potential consequences of its disclosure.

Accordingly, the protection of private life in the context of mass media does not necessarily require the unrestricted prohibition of reporting on personal matters. Rather, it requires the establishment and application of appropriate standards governing the publication and dissemination of private information.

2. Population Growth and Urbanization:

Population growth and changes in residential patterns may also influence the practical conditions under which individuals exercise their right to privacy.

In relatively small or less densely populated communities, the physical separation of residential premises may provide greater opportunities for maintaining certain forms of domestic privacy. By contrast, the expansion of urban areas and the increasing concentration of populations within apartment buildings and closely situated residential developments may create additional opportunities for unwanted observation or interference with neighboring households [42].

[41] Ben Said, Sabrina, Protection of the Right to Privacy in the Age of Technology, PhD Dissertation, Faculty of Law and Political Science, Hadj Lakhdar University, Batna, Algeria, 2014–2015, p. 137.
[42] Mohamed, The Human Right to the Protection of Private Life under International Law and Domestic Legislation, op. cit., pp. 64–65.

High-density residential environments may involve closer physical proximity between occupants, shared facilities, and increased exposure to the activities of others. These circumstances can generate privacy concerns relating to visual observation, noise, unauthorized entry, and interference with domestic activities.

Nevertheless, population density alone does not necessarily result in privacy violations. The extent of any associated risks depends on factors such as architectural design, residential arrangements, social practices, security measures, and the effectiveness of applicable legal protections. Urbanization should therefore be understood as a contextual factor that may affect the conditions of privacy rather than as an independent violation of the right itself.

3. The Use of Advanced Technologies in Criminal Activity:

The use of technological methods to facilitate unlawful conduct represents another factor affecting the protection of private life. Advances in recording equipment, communication systems, and electronic information processing may be exploited by offenders to engage in unauthorized surveillance, obtain confidential information, or interfere with the personal affairs of others.

The use of such techniques may increase the scale or complexity of privacy-related offences, particularly where unlawful conduct can be carried out remotely or without direct physical contact with the affected individual [(43)].

Certain forms of technologically facilitated interference may also create difficulties for law enforcement authorities. These include challenges relating to the detection of unlawful conduct, the identification of responsible individuals, and the collection of admissible evidence. The potential concealment of offenders' identities and the capacity to transmit information across different jurisdictions may further complicate investigations and legal proceedings [(44)].

However, the relationship between technological development and criminal activity should not be understood as inherently causal. Technologies that facilitate unlawful interference with privacy may also support the prevention, detection, and investigation of offences.

The relevant legal challenge is therefore to regulate the misuse of technological capabilities while preserving their legitimate applications and ensuring that measures adopted for security or law enforcement purposes remain consistent with applicable privacy protections.

Taken together, these social and technological factors demonstrate that threats to privacy arise from a combination of individual conduct, institutional practices, technological capabilities, and broader social conditions. The effective protection of private life consequently requires a legal framework capable of addressing diverse forms of interference while maintaining an appropriate relationship between individual rights, public interests, and technological development.

[(43)] Al-Mohammadi, Civil Liability Arising from Infringement of the Right to Privacy, op. cit., p. 4.
[(44)] Mohamed, The Human Right to the Protection of Private Life under International Law and Domestic Legislation, op. cit., pp. 66–67.

Chapter Two: The Nature and Legal Elements of Cybercrimes Involving Violations of the Right to Privacy

The development of information and communication technologies has introduced forms of criminal conduct that differ from conventional offences in the means through which they are committed. Although unlawful interference with individual rights is not a recent phenomenon, technological developments have expanded the circumstances in which such interference may occur, particularly where electronic systems are used to obtain, process, or disclose personal information [45].

Among the legal interests potentially affected by these developments is the right to privacy. Unlike conventional intrusions that may require physical access to a person's home or private documents, technologically facilitated interference may occur through electronic networks and devices without direct physical contact with the affected individual. This distinction raises questions concerning the classification of privacy-related conduct and the legal requirements for establishing criminal responsibility [46].

This chapter examines the nature of privacy-related cybercrimes and their constituent elements. The first section addresses the concept and legal characteristics of these offences, while the second considers Actus Reus (The Material Element) and Mens Rea (The Mental Element).

Section One: The Concept of Cybercrimes Involving Violations of Privacy

The concept of privacy-related cybercrime must be understood within the broader framework of offences involving information technology. Accordingly, it is necessary to distinguish cybercrime as a general legal category from the particular offences that interfere with protected aspects of private life.

The development of information technology has contributed to the emergence of conduct involving computers, electronic systems, and information networks that may fall within the scope of criminal legislation. Legal scholarship has employed different expressions to describe such conduct, including computer crime, Internet crime, information technology crime, and cybercrime. These differences reflect the various approaches adopted in defining offences according to the technology used, the protected interest affected, or the nature of the prohibited conduct [47].

The legal literature has also proposed different definitions of cybercrime. Some approaches focus on the relationship between criminal conduct and information technology, while others define the concept primarily by reference to the use of computers or electronic systems in carrying out unlawful activities [48].

---

[45] Maashi, Samira, "The Concept of Cybercrime," Legal Forum Journal, Biskra, Algeria, No. 7, 2010, p. 275.
[46] Lami, The Crime of Privacy Violation through Electronic Means under Jordanian Legislation, op. cit., pp. 18–19.
[47] Al-Shukri, Adel Youssef, "Cybercrime and the Crisis of Criminal Legality," Journal of the Kufa Studies Center, Kufa, Iraq, No. 7, 2008, p. 111.
[48] Ghayeb, Mahrous Nassar, "Cybercrime," Al-Taqani Journal, Iraq, No. 9, 2011, p. 103.

Within the Saudi legal framework, Article 1(8) of the Anti-Cyber Crime Law defines a cybercrime as an act involving the use of computers or information networks in violation of the provisions of that Law [49].

This statutory definition is significant because it connects the classification of cybercrime to conduct prohibited under the legislation. Consequently, the involvement of information technology does not independently establish criminal liability. The relevant conduct must satisfy the requirements of an applicable criminal provision.

The protection of privacy has traditionally been associated with the prevention of unjustified interference with an individual's personal affairs, private premises, and confidential correspondence. However, the development of information technology has expanded the methods through which such interests may be affected [50].

Electronic devices and digital platforms facilitate the collection, storage, transmission, and dissemination of information relating to individuals. Although these functions may serve legitimate purposes, their misuse can expose personal information and private communications to unauthorized access or disclosure. The nature of these risks also depends on the circumstances in which individuals use digital technologies. Differences in personal behavior, awareness, and patterns of information disclosure may influence the opportunities for interference with private life. Nevertheless, voluntarily sharing certain information does not necessarily authorize every subsequent use or disclosure of that information [51].

For the purposes of this research, privacy-related cybercrimes may be understood as offences involving the use of information technology to interfere unlawfully with legally protected aspects of an individual's private life, where the relevant conduct satisfies the elements prescribed by criminal legislation. This understanding emphasizes three considerations. First, the conduct must affect a legally protected privacy interest. Second, its technological characteristics must be relevant to the applicable offence. Third, criminal liability must be established according to the statutory requirements governing that conduct.

Accordingly, privacy-related cybercrime should not be regarded as one universally defined offence with identical elements in every legal system. Rather, it encompasses different forms of prohibited conduct that may affect overlapping interests, including the confidentiality of communications, personal information, and identifiable images.

The investigation and prosecution of privacy-related cybercrimes may present difficulties arising from the characteristics of electronic systems and digital evidence. One challenge concerns the detection and identification of prohibited conduct. Some activities may occur without the immediate

[49] Kingdom of Saudi Arabia, Anti-Cyber Crime Law, Council of Ministers Resolution No. 79, dated 7 Rabi I 1428 AH, approved by Royal Decree No. M/17, dated 1428 AH, Art. 1(8).
[50] Ben Saeed, Protection of the Right to Privacy in the Age of Technology, op. cit., p. 84.
[51] Lami, The Crime of Privacy Violation through Electronic Means under Jordanian Legislation, op. cit., p. 18.

knowledge of the affected individual, particularly where access to information takes place remotely or through compromised electronic accounts [52].

A further difficulty concerns the preservation and examination of electronic evidence. Digital records may be altered, deleted, or distributed across multiple devices and systems. These characteristics may complicate the reconstruction of events and the determination of the circumstances in which information was obtained or disclosed [53].

The identification of the individual responsible may also present difficulties, particularly where electronic activities involve several interconnected services or systems. However, these challenges should not be understood as making cybercrimes inherently impossible to investigate or prove. Their practical significance depends on the circumstances of the offence, the availability of relevant evidence, and the investigative methods permitted by law.

Legal systems have adopted different approaches to addressing conduct involving information technology. These differences may concern the definition of offences, the scope of criminal protection, and the requirements governing liability [54].

More broadly, the capacity of digital systems to collect and retain substantial quantities of information raises concerns about the potential for intrusive monitoring and the erosion of individual control over private information. These concerns reinforce the importance of legal safeguards against unjustified access and surveillance [55].

The distinctive characteristics of privacy-related cybercrimes therefore require attention not only to the technological methods involved, but also to the legal elements through which criminal responsibility is established.

Section Two: The Legal Elements of Cybercrimes Involving Violations of Privacy

Criminal liability cannot be established solely on the basis that an individual's privacy has been affected. The relevant conduct must fall within a criminal prohibition, and the constituent elements prescribed by that prohibition must be proved.

Criminal-law analysis commonly distinguishes between Actus Reus (The Material Element), which concerns the external elements of the offence, and Mens Rea (The Mental Element), which concerns the mental state required for criminal responsibility [56].

[52] Ibrahim, Khaled Mamdouh, Internet Governance, Dar Al-Fikr Al-Jami'i, Alexandria, Egypt, 1st ed., 2011, p. 363.
[53] Sassi, Boubaker, Criminal Protection of Private Life through the Internet, op. cit., pp. 53–55.
[54] Al-Obaidi, Osama bin Ghanem, "Protection of the Right to Privacy against Computer and Internet Crimes," Arab Journal for Security Studies and Training, Riyadh, Saudi Arabia, No. 47, 1429 AH, p. 51.
[55] Rabee, Violation of the Inviolability of Private Life under Cybercrime Law, op. cit., pp. 15–16.
[56] Ibrahim, Khaled Mamdouh, Cybercrimes, Dar Al-Fikr Al-Jami'i, Alexandria, Egypt, 1st ed., 2009, p. 98.

These elements provide a framework for examining privacy-related cybercrimes. Nevertheless, their precise requirements must be determined by the applicable statutory provision rather than by treating all technologically facilitated privacy violations as one offence.

Subsection One: Actus Reus (The Material Element):

The actus reus refers to the external conduct constituting a criminal offence. It represents the objective dimension of criminal liability and concerns the behavior prohibited by law. The material element is commonly examined through three components: criminal conduct, criminal result, and causation. However, the necessity of establishing each component depends on the statutory definition of the particular offence. Some offences require proof of a specific consequence, while others are completed through the commission of the prohibited conduct itself [(57)].

1. Criminal Conduct:

Criminal conduct refers to the external behaviour constituting the prohibited act. It may consist of an affirmative act or, where the law imposes a relevant duty, an omission. The criminal-law literature recognizes the significance of voluntary conduct in establishing the material element, while the particular form of conduct depends on the nature of the offence [(58)].

In privacy-related cybercrimes, the relevant conduct may involve the use of computers, electronic networks, or other technological devices to carry out prohibited activities. Such conduct may occur through digital systems without direct physical contact with the person whose privacy is affected [(59)].

Depending on the applicable statutory provision, the prohibited conduct may include producing, preparing, transmitting, or storing material affecting private life. These activities must be distinguished because criminal legislation may attach different legal consequences to each of them [(60)].

Image-related offences provide an example of the importance of this distinction. Legal approaches may differ regarding whether the unauthorized recording of an individual's image is independently prohibited or whether liability depends on the circumstances of recording or its subsequent dissemination [(61)].

The legal significance of preparatory conduct must also be considered. Activities undertaken before the commission of an offence do not necessarily establish criminal responsibility merely because they

(57) Ibrahim, Khaled Mamdouh, Cybercrimes, Dar Al-Fikr Al-Jami'i, Alexandria, Egypt, 1st ed., 2009, p. 98.
(58) Al-Zuhairi, Ashjan Khalis, and Nais, Linda Mohammed, Commentary on the Saudi Criminal Law: General Part, Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 1st ed., 1438 AH/2017, p. 63.
(59) Ibrahim, Khaled Mamdouh, Internet Governance, op. cit., p. 383.
(60) Al-Sulami, Civil Liability for Privacy Violations under the Saudi Anti-Cyber Crime Law, op. cit., pp. 87–88.
(61) Salim, Al-Jaida, Bouzidi, and Hamitoush, Infringement of the Right to One's Image in the Context of Modern Technological Developments, Master's Thesis, Faculty of Law and Political Science, Abderrahmane Mira University, Bejaia, Algeria, 2015–2016, p. 14.

may facilitate subsequent unlawful conduct. Their punish ability depends on whether the applicable law expressly criminalizes them or recognizes another relevant basis for liability [62].

Accordingly, the material element must be assessed by identifying the particular conduct prohibited under the relevant statutory provision, rather than assuming that every activity associated with electronic interference constitutes a completed offence.

2. Criminal Result:

In offences that require proof of a prohibited result, the criminal result represents the consequence legally attributed to the relevant conduct. Criminal-law scholarship distinguishes between consequences involving observable changes and those involving infringement of a legally protected interest. In privacy-related offences, the relevant harm may concern the confidentiality of information, the inviolability of private life, or another interest protected by law [63].

However, it is necessary to distinguish the infringement of a protected legal interest from a statutory requirement to prove an independently identifiable result. Some offences may be completed by carrying out the prohibited conduct in the circumstances prescribed by law, without requiring proof of additional material damage.

The legal analysis must therefore determine whether the applicable offence requires a distinct result or whether completion of the prohibited act is sufficient.

3. Causation:

Where a prohibited result constitutes an element of the offence, a causal relationship may be required between the accused person's conduct and that result. The technological characteristics of cybercrimes may complicate the examination of causation. Electronic activities may involve interconnected devices, multiple communications, and several stages of information processing, potentially making the factual sequence difficult to reconstruct [64].

Nevertheless, technological complexity does not eliminate the legal requirement to establish causation where it forms part of the offence. Equally, causation should not be treated as an additional requirement in offences for which the legislature has not prescribed a separate result.

The correct approach is therefore to identify the elements of the relevant offence and determine whether a causal connection must be established in the particular circumstances.

[62] Abdelrazzaq, Moussa, Criminal Protection of Internet Users, Master's Thesis, Faculty of Law and Political Science, Larbi Tebessi University, Tebessa, Algeria, 2015–2016, p. 29.
[63] Al-Hawamdeh, Lawrence Saeed, "Cybercrimes: Their Constituent Elements and Methods of Combating Them," Al-Mizan Journal for Islamic and Legal Studies, Amman, Jordan, No. 1, 2016–2017, p. 19.
[64] Saghir, Crime Committed through the Internet, op. cit., p. 68.

4. The Legal Significance of Consent:

Consent may be relevant to determining whether particular conduct constitutes unlawful interference with privacy. Legal scholarship has examined the circumstances in which an individual's authorization may affect the lawfulness of activities involving private information or personal affairs [65].

However, consent cannot be treated as a universal condition determining the existence or absence of the material element in every privacy-related cybercrime. Its legal significance depends on the relevant statutory provision, the nature of the protected interest, the validity and scope of the authorization, and any applicable legal limitations.

For example, permission to access particular information does not necessarily authorize its disclosure or use for an unrelated purpose. Accordingly, the absence or presence of consent must be assessed in relation to the conduct prohibited by law, rather than presumed to determine criminal liability in every case.

Subsection Two: Mens Rea (The Mental Element):

Mens Rea (The Mental Element) concerns the mental state required for establishing criminal responsibility. In the analysis of intentional offences, criminal intent is commonly examined through the elements of knowledge and will. Knowledge concerns awareness of the relevant factual circumstances, while will concerns the voluntary commission of the prohibited conduct and, where required, the intended consequence [66].

The precise mental element nevertheless depends on the applicable statutory provision. It is therefore necessary to distinguish general criminal intent from any additional purpose required for a particular offence.

1. General Criminal Intent:

General criminal intent ordinarily involves the knowledge and will required by the relevant intentional offence. In the context of privacy-related cybercrimes, the mental element may concern awareness of the relevant circumstances and the deliberate performance of conduct prohibited by law. For example, an offence involving intentional unauthorized access may require examination of whether the accused deliberately entered an electronic system without the authorization required for such access.

The distinction between voluntary conduct and conduct undertaken without the requisite mental state is important. Nevertheless, questions concerning coercion, mistake, or other circumstances affecting

[65] Jallad, The Right to Privacy between Safeguards and Restrictions under Algerian Legislation and Islamic Jurisprudence, op. cit., pp. 140–141.
[66] Al-Zuhairi and Nais, Commentary on the Saudi Criminal Law: General Part, op. cit., pp. 98–99.

responsibility must be evaluated under the relevant legal rules, rather than assuming that the absence of a particular motive automatically excludes criminal liability [67].

Accordingly, general criminal intent must be established by examining the elements required by the particular offence and the evidence relating to the accused person's conduct and awareness.

2. Specific Criminal Intent:

Specific criminal intent arises where the legislature requires an additional purpose or objective beyond the general mental elements associated with the prohibited conduct. Criminal-law scholarship distinguishes such an intention from general criminal intent because the offence requires proof that the accused acted for a particular purpose identified by law [68].

Within privacy-related cybercrimes, this distinction is especially significant where statutory provisions specify purposes such as threatening another person, obtaining protected information, or interfering with private data. It would therefore be inaccurate to conclude that every privacy-related cybercrime requires a general intention to violate privacy and, in addition, a separate specific intention to achieve that result. Rather, specific criminal intent is required only where the applicable offence expressly or necessarily includes that additional mental element.

An example involving a recording device illustrates the relevance of intention. Where a device records information accidentally, the circumstances may differ materially from those in which an individual deliberately uses it to interfere with another person's private life. However, the legal consequences must still be assessed according to the applicable offence and the evidence establishing its constituent elements [69].

Consequently, the determination of specific intent must be based on the requirements of the relevant criminal provision rather than on the general characterization of the conduct as an invasion of privacy.

5. Establishing the Mental Element:

Establishing the mental element of a cybercrime may present evidentiary challenges because intention is not ordinarily capable of direct observation. The relevant mental state may therefore need to be assessed through the circumstances surrounding the conduct and the evidence available in the particular case. Such evidence may concern the manner in which access was obtained, the sequence of electronic activities, the handling of private information, and other facts relevant to the statutory requirements.

[67] Saghir, Crime Committed through the Internet, op. cit., p. 72.
[68] Al-Zoubi, The Right to Privacy in Criminal Law, op. cit., p. 187.
[69] Khalfi, Abdelrahman, "The Right to Private Life under Algerian Criminal Legislation," Journal of Communication in Economics, Administration and Law, Algeria, No. 45, 2016, p. 82.

The criminal-law literature recognizes the importance of examining the circumstances of each offence and the evidence submitted when determining whether the required criminal intent has been established [70].

However, the existence of electronic activity or interference with privacy should not, by itself, be treated as conclusive proof of the accused person's mental state. The competent judicial authorities must assess the available evidence and determine whether the required elements have been established in accordance with the applicable law.

Concluding Observations

Privacy-related cybercrimes involve technologically facilitated conduct that may affect several legally protected aspects of private life. Their criminal classification depends not merely on the use of information technology, but on the conduct prohibited by the applicable legislation and the requirements governing criminal responsibility.

The examination of Actus Reus (The Material Element) demonstrates the importance of distinguishing prohibited conduct from any additional result, causal requirement, or circumstance prescribed by law. Similarly, the analysis of Mens Rea (The Mental Element) establishes the need to identify the required mental state and to distinguish general criminal intent from any additional specific purpose stipulated by the relevant offence.

These distinctions provide the legal foundation for examining the common forms of privacy-related cybercrimes addressed in the following chapter.

Chapter Three: Common Forms of Cybercrimes Involving Violations of Privacy

The development of information and communication technologies has substantially transformed the methods through which individuals' privacy may be violated. While traditional interference with private life frequently involved direct observation or physical intrusion, contemporary violations may occur remotely through digital devices, electronic networks, and online communication platforms. Consequently, the scope of potential interference has expanded to include personal images, electronic communications, stored information, and activities conducted within digital environments [71].

These forms of interference are not technologically fixed. Developments in digital systems continue to create new methods of accessing, collecting, manipulating, and disseminating personal information. Recent cybersecurity assessments have identified the continued significance of social engineering, malicious software, compromised accounts, and techniques increasingly supported by artificial intelligence [72].

---

[70] Al-Hawamdeh, Cybercrimes: Their Constituent Elements and Methods of Combating Them, op. cit., p. 25.

[71] Marneez, Fatima, Infringement of the Right to Privacy through the Internet, PhD Dissertation, Faculty of Law and Political Science, Abou Bekr Belkaid University, Tlemcen, Algeria, 2012–2013, p. 4.

[72] European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2026, European Union Agency for Cybersecurity, 22 September 2026.

Nevertheless, technological capability must be distinguished from criminal liability. The use of an electronic device does not independently establish a criminal offence; the conduct must satisfy the elements prescribed by the applicable legislation.

This chapter examines five common forms of interference with privacy: violations of image rights, electronic surveillance, unauthorized access to information systems, unlawful interference with personal data, and violations of private electronic communications.

Section One: Violations of the Right to One's Image

An individual's image constitutes an important aspect of personal identity. It may disclose information concerning physical appearance, social relationships, personal circumstances, and activities that form part of private life. Consequently, the unauthorized recording, dissemination, or manipulation of identifiable images may interfere with privacy, dignity, or other legally protected interests [(73)].

The expansion of digital photography and online communication platforms has increased the accessibility of image-recording technologies and the speed at which photographs and recordings may be distributed. These developments have also introduced new methods of manipulating visual representations [(74)].

1. The Concept and Legal Nature of Image Rights:

The right to one's image may generally be understood as an individual's legally protected interest in controlling certain uses of their identifiable visual representation, subject to limitations and exceptions established by law.

Legal scholarship has adopted different approaches concerning the nature of this right. The first considers it an aspect of privacy because the recording or publication of an image may disclose elements of an individual's private life. The second regards image rights as independent personality rights capable of protection even where the relevant image does not reveal confidential information. The third recognizes a dual legal character, acknowledging that image rights may overlap with privacy protection without being entirely dependent on it [(75)].

The distinction is legally significant. An image recorded in a private setting may constitute interference with private life, while the unauthorized commercial exploitation of a person's photograph may primarily concern control over the use of their likeness.

[(73)] Salman, Ouda Youssef, "Crimes Violating the Right to Privacy through Modern Information Technology," Journal of Law, Iraq, Nos. 29–30, 2017, p. 6.

[(74)] Fuzay, Nabil, Criminal Protection of the Right to One's Image under Egyptian Law, Dar Mahmoud Publishing, Cairo, Egypt, 1st ed., 2016, p. 9.

[(75)] Raddad, Simaa Jabbar, The Legal Nature of the Right to One's Image, Master's Thesis, College of Law, University of Al-Qadisiyah, Al-Diwaniyah, Iraq, 2017, pp. 2–3.

Accordingly, the classification of image-related conduct should depend on the nature of the protected interest and the circumstances of the alleged interference. It should not automatically be assumed that every unauthorized use of an individual's image constitutes a criminal violation of privacy [76].

2. Common Forms of Interference with Image Rights:

Interference with image rights may occur through recording, dissemination, or manipulation.

Unauthorized recording involves obtaining an individual's image in circumstances in which recording may be restricted by law. The legal significance of this activity depends on the location, the circumstances of recording, the purpose of the conduct, and the relevant statutory requirements [77].

Unauthorized dissemination occurs where an identifiable image is transmitted, published, or otherwise made accessible beyond the purposes or recipients for which its use was legally permitted. An image may have been obtained lawfully while its subsequent publication raises separate legal concerns [78].

Image manipulation may involve altering an authentic image or presenting it in a misleading context. Such conduct may misrepresent an individual's appearance, actions, or circumstances and potentially affect both privacy and reputation [79].

Modern generative artificial intelligence introduces an additional dimension to image manipulation. Synthetic media technologies can produce realistic visual representations depicting identifiable individuals in circumstances that did not occur.

The United States National Institute of Standards and Technology has examined the risks associated with synthetic content, including the generation of non-consensual intimate imagery depicting real individuals. The report also addresses technical approaches to identifying synthetic material and establishing content provenance [80].

These developments demonstrate that legal analysis of image-related interference must extend beyond conventional photography to consider synthetic representations and digital impersonation. Nevertheless, the artificial generation or modification of an image does not automatically establish a

[76] Al-Hait, Sama Saqf, The Right to One's Image: An Aspect of the Right to Privacy or an Independent Right?, Master's Thesis, Faculty of Law and Public Administration, Birzeit University, Palestine, 2017, p. 8.

[77] Bouchala, Ramzi, Interception of Telephone Calls and Taking Photographs: Between Criminalization and Permissibility, Master's Thesis, Faculty of Law and Political Science, Larbi Ben M'hidi University, Oum El Bouaghi, Algeria, 2014–2015, p. 35.

[78] Naima, Majadi, "Criminal Protection of the Right to One's Image," Journal of Legal Studies and Research, Algeria, No. 7, 2017, pp. 226–227.

[79] Salim and Bouzidi, Infringement of the Right to One's Image in the Context of Modern Technological Developments, op. cit., pp. 14–15.

[80] Chandra, Bilva, Jesse Dunietz, Kathleen Roberts, Yooyoung Lee, Peter Fontana, and George Awad, Reducing Risks Posed by Synthetic Content: An Overview of Technical Approaches to Digital Content Transparency, NIST AI 100-4, National Institute of Standards and Technology, United States, 2024.

criminal offence. Liability depends on the nature of the conduct and the requirements of the applicable law.

Section Two: Electronic Surveillance and Spyware

Electronic surveillance constitutes another form of potential interference with private life. It may involve monitoring communications, observing digital activities, or collecting information from electronic devices without the authorization required by law.

The protection of private affairs against unjustified surveillance is consistent with Islamic principles concerning respect for personal privacy. The Holy Qur'an expressly prohibits spying, reflecting a broader ethical obligation to refrain from unwarranted intrusion into the affairs of others [81].

1. The Concept of Electronic Surveillance:

Surveillance may be conducted through direct observation or through technological means that enable information to be collected remotely. The development of electronic networks has expanded the possible scope of monitoring because information may be obtained from devices and services without physical proximity to the individual concerned [82].

For the purposes of this study, unlawful electronic surveillance may be understood as monitoring or collecting information relating to individuals through digital technologies without the legal authorization or justification required for that activity.

The legal significance of surveillance is therefore determined not merely by the technology employed, but by the nature of the monitoring, the information obtained, and the applicable legal requirements [83].

2. Spyware and Contemporary Surveillance Methods:

Spyware generally refers to software capable of monitoring activity or collecting information from an electronic device, frequently without the awareness or authorization of its user. Earlier forms of spyware commonly involved recording keyboard input, monitoring online activity, and collecting information stored on computers. Such software could compromise the confidentiality of passwords, messages, and other personal records [84].

[81] The Holy Qur'an, Surah Al-Hujurat, verse 12.
[82] Al-Zaidi, Taha Ahmed, Provisions Governing Information Crimes in Islamic Jurisprudence and Law, op. cit., pp. 288–289.
[83] Al Mawash, Dirgham Jaber Atoush, The Crime of Information Espionage, Arab Center for Studies and Scientific Research, Cairo, Egypt, 1st ed., 1438 AH/2017, pp. 83, 89 and 91.
[84] Al-Ghathbar, Khaled bin Sulaiman, and Al-Qahtani, Mohammed bin Abdullah, Information Security in Simple Language, Center of Excellence in Information Assurance, Riyadh, Saudi Arabia, 1st ed., 1429 AH/2009, p. 76.

Contemporary surveillance threats may also affect smartphones and interconnected services. Depending on the technical capabilities involved, compromised devices may expose communications, stored photographs, account information, and other private data.

However, spyware should be distinguished from malicious software more generally. Not all malicious applications are designed for surveillance, and not every application with monitoring capabilities is necessarily deployed unlawfully.

The legal assessment must therefore consider the manner in which the technology is installed or used, the scope of the information collected, and whether the activity satisfies the elements of an applicable criminal prohibition.

Section Three: Unauthorized Access to Information Systems

Unauthorized access to information systems is closely associated with the protection of private information. Digital devices and electronic accounts frequently contain personal documents, communications, photographs, and other records. Obtaining access to these systems without lawful authorization may consequently expose information that would otherwise remain confidential [85].

1. The Concept of Unauthorized Access:

Unauthorized access generally involves entering a computer, electronic account, information system, or network without the permission or legal authority required for that activity. The legal definition of unauthorized access must be distinguished from the technological methods through which it may occur. An individual may obtain access through sophisticated software or through the misuse of credentials or existing permissions [86].

It is also necessary to distinguish the initial act of obtaining access from subsequent activities such as copying, altering, disclosing, or destroying information. These activities may involve different legally protected interests and may satisfy different statutory provisions.

Accordingly, unauthorized access should not automatically be treated as legally identical to every subsequent misuse of information obtained from a compromised system.

2. Methods of Unauthorized Access:

Unauthorized access may occur through compromised credentials, malicious software, exploitation of software vulnerabilities, or manipulation of individuals into disclosing confidential information. A particularly significant method is social engineering, which involves using deception or manipulation to persuade individuals to reveal sensitive information or provide access that would otherwise be unavailable [87].

---

[85] Rabhi, Aziza, Information Secrets and Their Criminal Protection, PhD Dissertation, Faculty of Law and Political Science, Abou Bekr Belkaid University, Tlemcen, Algeria, 2017–2018, pp. 111–112.
[86] Ibrahim, Khaled Mamdouh, Cybercrimes, Dar Al-Fikr Al-Jami'i, Alexandria, Egypt, 1st ed., 2009, p. 242.
[87] Al-Ghathbar and Al-Qahtani, Information Security in Simple Language, op. cit., pp. 70–71.

Phishing is one manifestation of this technique. It commonly involves fraudulent communications presented as originating from a legitimate organization or trusted person. Recent cybersecurity assessments indicate that these methods have evolved beyond conventional email messages. Voice-based phishing, impersonation assisted by artificial intelligence, and deceptive authorization requests have become relevant concerns in contemporary digital security [88].

These techniques may facilitate access to private accounts and information. However, the distinction between the method of intrusion and the statutory offence remains essential. An individual's criminal liability must be determined by the conduct established and the requirements of the applicable law, rather than by the mere occurrence of a cybersecurity incident.

Section Four: Unlawful Interference with Personal Data

The increasing collection and processing of information through electronic platforms has made personal data protection an important aspect of contemporary privacy law.

Digital services routinely collect information relating to identification, communication, financial transactions, and online activities. Although such processing may serve legitimate purposes, it can also create risks involving unauthorized access, disclosure, or misuse [89].

1. The Concept of Personal Data:

Personal data generally refers to information relating to an identified or identifiable individual. It may include names, contact details, identification information, photographs, financial records, and other information capable of identifying a person directly or indirectly.

Importantly, personal information is not necessarily limited to confidential information. Data may remain personal even where it is accessible to others, although the legal conditions governing its processing may differ [90].

This distinction is significant because modern data-processing systems may combine different categories of information to identify individuals or develop profiles concerning their activities and preferences.

2. Common Forms of Unlawful Interference:

The common forms of interference with personal data include unauthorized access, improper disclosure, and unlawful collection or processing. Unauthorized access concerns obtaining personal information without the authority required by law.

---

[88] Computer Emergency Response Team for the EU Institutions, Bodies and Agencies (CERT-EU), Threat Landscape Report 2025: A Year in Review, European Union, 8 April 2026, section "Social Engineering Evolves Beyond E-mail".
[89] Sassi and Boubaker, Criminal Protection of Private Life on the Internet, op. cit., p. 19.
[90] Ghoneim, Riham Asim, "Personal Information Available on the Web," Recent Trends in Libraries and Information, Cairo, Egypt, No. 37, 2012, p. 233.

Improper disclosure involves making information available to a person or entity not legally entitled to receive it. For example, information collected for a legitimate transaction may subsequently be disclosed for an unrelated or unauthorized purpose [91].

Unlawful collection or processing may arise where information is obtained, retained, or used in circumstances that do not satisfy applicable legal requirements. Digital tracking mechanisms may also facilitate the collection of information concerning online behaviour and user preferences. Nevertheless, such technologies are not inherently unlawful; their legal status depends on the information processed and the requirements governing the relevant activity [92].

A distinction must therefore be maintained between unlawful interference with personal data and cybercrime in the strict criminal-law sense. Certain conduct may constitute a regulatory violation without necessarily satisfying the constituent elements of a criminal offence. The legal classification must consequently be established through the applicable legislation.

Section Five: Violations of Private Electronic Communications

The confidentiality of correspondence constitutes an important aspect of personal privacy. Private communications may contain information concerning family relationships, financial circumstances, professional activities, and other matters that individuals do not intend to disclose publicly [93].

The development of electronic communication services has expanded the methods through which correspondence may be exchanged, stored, and accessed. These developments have also introduced additional risks to communication confidentiality [94].

1. Unauthorized Access and Interception:

Violations of electronic communications may occur through unauthorized interception of messages in transmission or unlawful access to correspondence stored in electronic accounts. Interception concerns communications during transmission, whereas unauthorized account access may involve messages that have already been received and stored. This distinction is legally significant because the relevant criminal provisions may prescribe different requirements depending on the nature of the conduct [95].

The legal assessment should therefore identify whether the alleged interference involved interception, unauthorized entry into an account, or subsequent disclosure of its contents.

2. Account Compromise and Disclosure of Private Communications:

[91] Rabhi, Information Secrets and Their Criminal Protection, op. cit., p. 50.
[92] Abdelkader, Omaimer, "Criminal Protection of the Right to Privacy in the Digital Environment," Journal of Law and Business, Hassan I University, Morocco, No. 20, 2018, p. 81.
[93] Al-Nasser, Mohammed Qasim, The Right to Confidentiality of Correspondence in Selected Constitutional Systems, Master's Thesis, College of Law, University of Babylon, Iraq, 1422 AH/2002, p. 11.
[94] Hadi, Uday Jaber, "Criminal Protection of Email," Risalat Al-Huquq Journal, Iraq, No. 3, 2010, p. 156.
[95] Rabhi, Information Secrets and Their Criminal Protection, op. cit., pp. 217–221.

Modern communication services allow messages to be exchanged across interconnected devices and platforms. Although this functionality facilitates communication, unauthorized access to an account or connected device may expose personal messages and associated information to third parties.

Account compromise may result from stolen credentials, deceptive authentication requests, or other techniques used to obtain access. Recent cybersecurity reporting has documented the development of social engineering techniques involving artificial intelligence-assisted impersonation and misuse of digital authorization processes [96].

The unauthorized disclosure of private correspondence may constitute a further and distinct form of interference, particularly where information is distributed beyond its intended recipients.

Consequently, the protection of electronic communications requires attention to the confidentiality of transmitted messages, the security of stored correspondence, and the legal significance of subsequent disclosure.

Concluding Observations

Common forms of privacy-related cybercrime demonstrate that interference with private life may affect different legally protected interests. Violations involving personal images, electronic surveillance, unauthorized access, personal data, and private communications may overlap in practice, but they should not be treated as legally identical.

Recent technological developments, particularly synthetic media and artificial intelligence-assisted deception, have further expanded the potential methods through which privacy may be compromised. The appropriate legal analysis therefore requires identification of the protected interest, the specific conduct involved, and the statutory elements establishing criminal liability.

Chapter Four: Legal Protection against Privacy-Related Cybercrimes in Saudi Arabia

The development of digital technologies in Saudi Arabia has increased the importance of protecting personal privacy within electronic environments. As digital systems have become integral to communication, commercial activities, and the delivery of public and private services, the potential consequences of unauthorized access to personal information have acquired greater legal significance.

Saudi Arabia has developed a framework that addresses these risks through criminal legislation, personal data protection requirements, and cybersecurity regulation. These mechanisms perform complementary but distinct functions. Criminal legislation defines offences and penalties, data

[96] Computer Emergency Response Team for the EU Institutions, Bodies and Agencies (CERT-EU), Threat Landscape Report 2025: A Year in Review, European Union, 8 April 2026, section “Social Engineering Evolves Beyond E-mail.”

protection legislation regulates the processing of personal information, and cybersecurity requirements seek to reduce the likelihood and consequences of information security incidents [97].

The distinction between these mechanisms is important because conduct affecting privacy may give rise to criminal, regulatory, or civil liability according to the applicable legal provisions.

This chapter examines three aspects of the Saudi framework: criminal protection under the Anti-Cyber Crime Law, complementary data protection and cybersecurity measures, and judicial applications illustrating the protection of privacy-related interests.

Section One: Criminal Protection under the Anti-Cyber Crime Law

The Saudi Anti-Cyber Crime Law, issued by Royal Decree No. M/17 in 1428 AH, constitutes a principal legislative basis for addressing offences committed through computers and information networks. Article 2 identifies objectives including enhancing information security, protecting rights arising from the legitimate use of computers and information networks, and safeguarding public interests [98].

Rather than establishing a single offence encompassing every possible invasion of privacy, the Law criminalizes specified forms of conduct involving electronic systems and digital information.

1. Unauthorized Interception of Electronic Communications:

Article 3(1) addresses the interception or reception of data transmitted through an information network or computer, including eavesdropping, without lawful justification. The provision is significant because electronically transmitted information may contain personal communications and other confidential material.

The offences specified in Article 3 are subject to imprisonment for a period not exceeding one year and a fine not exceeding SAR 500,000, or either penalty.

Nevertheless, the application of this provision requires proof of the specific prohibited conduct and the circumstances prescribed by law. The mere existence or use of monitoring technology does not independently establish criminal liability.

2. Invasion of Privacy through Camera-Equipped Devices:

Article 3(4) expressly criminalizes invasion of privacy through the misuse of camera-equipped mobile phones or comparable devices. This provision recognizes that electronic recording technologies may be employed to interfere with legally protected aspects of private life.

[97] Al Jarallah, Abdulaziz bin Gharmallah, Internet Crimes and Their Penalties under the Saudi Anti-Cyber Crime Law, Dar Al-Kitab Al-Jami'i, Riyadh, Saudi Arabia, 1st ed., 1438 AH/2017, pp. 41–43.
[98] Kingdom of Saudi Arabia, Anti-Cyber Crime Law, op. cit., Art. 2.

Its application, however, should not be interpreted as establishing that all photography without express consent automatically constitutes a criminal offence. The relevant legal question concerns whether the circumstances amount to the prohibited invasion of privacy.

Article 3(5) separately addresses defamation and harm inflicted through information technology. This provision may become relevant where the publication of images or other digital material affects an individual's reputation. The distinction between privacy infringement and reputational harm must be maintained because the protected interests and relevant statutory conditions are not necessarily identical.

3. Unauthorized Access and Interference with Private Information:

The Anti-Cyber Crime Law contains several provisions concerning unauthorized access, but their legal requirements differ. Article 3(2) concerns unauthorized access undertaken for the purpose of threatening or blackmailing another person to perform or refrain from performing an act [99].

Article 4(2) addresses unauthorized access to specified banking, credit, and securities-related information for the purposes prescribed by that provision [100].

Article 5(1) concerns unauthorized access undertaken for the purpose of deleting, destroying, leaking, damaging, altering, or redistributing private data. Article 5 provides for imprisonment not exceeding four years and a fine not exceeding SAR 3 million, or either penalty, for the offences specified in that article [101].

These provisions demonstrate the importance of distinguishing unauthorized access from other forms of interference. The legal classification depends on the information involved, the conduct established, and any additional purpose required by the relevant offence.

Consequently, it would be inaccurate to assume that every instance of unauthorized access necessarily satisfies all provisions relating to interference with private information.

4. Electronic Content Affecting Private Life:

Article 6(1) addresses the production, preparation, transmission, or storage of material falling within the categories specified by the Law, including material affecting the inviolability of private life. The offences specified in Article 6 carry a maximum penalty of five years' imprisonment and a fine not exceeding SAR 3 million, or either penalty [102].

This provision differs from Article 3(4), which specifically addresses the misuse of camera-equipped devices. The distinction is significant because the production, preparation, transmission, or storage of material may involve different acts from the original recording of an image.

[99] Kingdom of Saudi Arabia, Anti-Cyber Crime Law, op. cit., Art. 3.
[100] Kingdom of Saudi Arabia, Anti-Cyber Crime Law, op. cit., Art. 4.
[101] Kingdom of Saudi Arabia, Anti-Cyber Crime Law, op. cit., Art. 5.
[102] Kingdom of Saudi Arabia, Anti-Cyber Crime Law, op. cit., Art. 6.

Accordingly, the statutory classification must reflect the particular activity attributed to the accused and the requirements of the applicable provision.

5. Confiscation and Ancillary Measures:

Article 13 permits the competent court, subject to the protection of good-faith third-party rights, to order the confiscation of devices, software, or other means used in committing offences under the Law, as well as proceeds derived from such offences. The provision also permits the closure of a website or service location under the conditions specified by law [(103)].

These measures may be relevant where electronic devices or online platforms facilitate the commission of privacy-related offences. However, confiscation and closure are subject to judicial determination and should not be presented as automatic consequences of every violation.

The Anti-Cyber Crime Law therefore provides several forms of criminal protection, while requiring the legal elements of each offence to be assessed independently.

Section Two: Complementary Personal Data Protection and Cybersecurity Measures

Criminal legislation constitutes an important mechanism for responding to privacy-related offences. Nevertheless, the protection of personal information also requires regulation of legitimate data-processing activities and measures intended to prevent information security incidents.

Saudi Arabia's legal framework addresses these issues through the Personal Data Protection Law and national cybersecurity requirements.

1. The Personal Data Protection Law:

The Saudi Personal Data Protection Law was issued by Royal Decree No. M/19 in 1443 AH and subsequently amended by Royal Decree No. M/148 in 1444 AH. The Law establishes a dedicated framework for regulating the processing of personal information. Article 1 adopts a broad definition of personal data that includes information capable of identifying an individual directly or indirectly. The definition expressly encompasses categories such as names, identification details, contact information, financial information, and images [(104)].

The scope of this definition reflects the significance of protecting individuals from misuse of information that enables their identification, whether directly or through association with other data.

2. Rights of Data Subjects and Conditions of Processing:

Article 4 recognizes several rights of data subjects, including rights relating to information about processing, access to personal data, correction, and requests for destruction under the conditions

[(103)] Kingdom of Saudi Arabia, Anti-Cyber Crime Law, op. cit., Art. 13.
[(104)] Kingdom of Saudi Arabia, Personal Data Protection Law, Royal Decree No. M/19, dated 1443 AH, as amended by Royal Decree No. M/148, dated 1444 AH, Art. 1.

established by law, meanwhile Article 5 establishes a general consent requirement, subject to the statutory exceptions, while Article 6 identifies circumstances in which processing may take place without the consent otherwise contemplated under Article 5 [105].

The legal significance of these provisions is that valid processing cannot be assessed solely by determining whether express consent has been obtained. Instead, the legality of the conduct depends on the applicable legal basis and the requirements governing that basis.

Article 15 additionally regulates the circumstances in which personal data may be disclosed [106]. These provisions establish a framework for controlling the collection, use, and disclosure of personal information beyond the criminalization of specific cybercrimes.

3. Data Security and Breach Notification:

The Personal Data Protection Law also contains preventive obligations concerning the security of personal information. Article 19 requires controllers to implement appropriate organizational, administrative, and technical measures to protect personal data.

Article 20 establishes requirements relating to notification of personal data breaches, subject to the conditions prescribed by the Law and its implementing regulations [107].

These provisions are significant because their purpose extends beyond responding to privacy violations after they occur. They require relevant organizations to adopt measures intended to reduce security risks and address incidents affecting personal information.

4. Criminal Protection of Sensitive Personal Data:

Article 35 of the Personal Data Protection Law establishes a specific criminal offence concerning the disclosure or publication of sensitive personal data in violation of the Law where the conduct is committed with the intention of harming the data subject or obtaining a personal benefit. The provision establishes a maximum penalty of two years' imprisonment and a fine not exceeding SAR 3 million, or either penalty [108].

The additional intention prescribed by the provision is essential to the offence. It would therefore be inaccurate to describe every unlawful disclosure of personal information as automatically constituting the criminal offence established under Article 35.

Article 40 also recognizes the right to claim compensation for material or moral harm resulting from violations within the scope of the Law [109]. Accordingly, the legislative framework distinguishes criminal punishment from regulatory enforcement and compensation.

[105] Kingdom of Saudi Arabia, Personal Data Protection Law, op. cit., Arts. 4, 5, 6.
[106] Kingdom of Saudi Arabia, Personal Data Protection Law, op. cit., Art. 15.
[107] Kingdom of Saudi Arabia, Personal Data Protection Law, op. cit., Arts. 19, 20.
[108] Kingdom of Saudi Arabia, Personal Data Protection Law, op. cit., Art. 35.
[109] Kingdom of Saudi Arabia, Personal Data Protection Law, op. cit., Arts. 36, 40.

5. National Cybersecurity Measures:

The protection of private information also depends on the security of the systems through which that information is processed. The National Cybersecurity Authority has issued the Essential Cybersecurity Controls (ECC 2-2024), which establish cybersecurity requirements designed to strengthen protection of information and technological assets within their applicable scope [(110)].

These controls support the protection of electronic systems by establishing organizational and technical security requirements. Cybersecurity measures are particularly relevant to privacy protection because weaknesses in electronic systems may facilitate unauthorized access to personal information.

Nevertheless, cybersecurity requirements must be distinguished from criminal prohibitions. The existence of a technical weakness does not itself establish that a criminal offence has occurred, and an allegation of criminal interference must still be assessed according to the applicable statutory requirements.

6. The Relationship between Criminal and Regulatory Protection:

The Anti-Cyber Crime Law and the Personal Data Protection Law perform complementary functions. The former addresses specified prohibited activities involving electronic devices, information systems, and networks. While the latter regulates the lawful collection, use, disclosure, and protection of personal information.

These frameworks may become relevant to the same factual circumstances, but they do not necessarily establish identical forms of liability. For example, unauthorized disclosure of personal information may raise issues concerning data protection obligations, while the method used to obtain the information may separately require examination under the Anti-Cyber Crime Law.

Accurate legal analysis therefore requires identification of the relevant conduct, the protected interest, and the conditions governing each form of responsibility.

Section Three: Judicial Applications

Judicial applications provide practical illustrations of the manner in which privacy-related provisions have been applied to particular circumstances.

The following two cases appeared in the original research and are retained as examples of Saudi judicial practice. Their significance must be assessed in light of the legislation and judicial procedures applicable at the time of the decisions.

1. Unauthorized Publication of Personal Photographs:

The first case concerned the publication of photographs of a young woman through a social media platform without her authorization. According to the judicial record cited in the original research, the

[(110)] National Cybersecurity Authority (NCA), Essential Cybersecurity Controls (ECC 2-2024), Saudi Arabia, 2024.

defendant admitted the conduct attributed to her. The court considered circumstances including her age, the absence of previous convictions, and her acknowledgment of responsibility.

The court imposed a sentence of one month's imprisonment and ordered confiscation of the mobile phone and SIM card involved, destruction of the photographs submitted during the proceedings, and closure of the social media page used to publish them. The judgment was subsequently upheld on appeal [111].

The importance of this case lies in the judicial treatment of unauthorized dissemination of personal images and the assessment of circumstances relevant to sentencing. It also illustrates the possible application of ancillary measures to electronic devices used in prohibited conduct. Nevertheless, this decision should not be treated as establishing a uniform penalty for every contemporary case involving unauthorized publication of photographs.

2. Photographing and Publishing Images of a Minor:

The second case concerned an individual who photographed a minor at the place where he worked and subsequently published her images. According to the judicial record cited in the original research, the defendant admitted the allegations, and the court considered the conduct established during the proceedings.

The original judgment imposed imprisonment, a financial penalty, a discretionary corporal punishment under the legal framework applied at the time, and confiscation of the mobile phone involved [112].

For the purposes of this study, the relevance of the case concerns the treatment of recording and publication of a minor's image without authorization. The case also illustrates the importance of examining the circumstances of the recording and the subsequent use of the images.

However, the sanctions imposed must be understood within their legal context at the time of the decision and should not be presented as necessarily representative of contemporary sentencing practice.

3. Evaluation of the Judicial Applications:

The two cases demonstrate that the unauthorized use of electronic recording technologies may give rise to criminal proceedings where the statutory requirements are satisfied. They also illustrate the judicial consideration of the surrounding circumstances and the potential availability of confiscation or other measures affecting devices used in committing prohibited conduct.

[111] Ministry of Justice, Kingdom of Saudi Arabia, Collection of Judicial Judgments for the Year 1434 AH, Research Centre, Vol. 24, Case No. 34278231, judgment dated 26 Jumada II 1434 AH, p. 160.
[112] Ministry of Justice, Kingdom of Saudi Arabia, Collection of Judicial Judgments for the Year 1435 AH, Research Centre, Vol. 13, Case No. 35165932, 1435 AH, p. 295.

Nevertheless, the cases should not be interpreted as establishing that all recording or publication of an individual's image automatically constitutes a criminal offence. Rather, their legal significance depends on the specific facts, the statutory provisions applied, and the findings established by the competent courts.

Furthermore, these two decisions alone do not establish uniform contemporary judicial practice. A comprehensive assessment of recent sentencing patterns would require examination of additional published judgments.

Concluding Observations

Saudi Arabia's legal framework for addressing privacy-related cybercrimes combines criminal legislation, personal data protection, and preventive cybersecurity measures.

The Anti-Cyber Crime Law establishes criminal protection against specified forms of unauthorized interception, misuse of electronic devices, unlawful access, and interference with private information.

The Personal Data Protection Law complements this framework by regulating the processing and security of personal information and establishing distinct mechanisms of criminal, regulatory, and civil responsibility. National cybersecurity requirements further support the protection of information systems through preventive security measures.

Judicial applications demonstrate the importance of examining the statutory elements of the offence and the circumstances of the particular case.

Accordingly, the effectiveness of privacy protection depends on accurate application of the relevant legal provisions and continued consideration of technological developments within the principles governing criminal liability.

Conclusion

The protection of privacy in the context of cybercrime has become an increasingly significant area of legal analysis, particularly as technological developments continue to transform the methods through which private information may be accessed, monitored, manipulated, and disclosed. This research has examined the legal foundations of the right to privacy, the constituent elements of privacy-related cybercrimes, their common forms, and the legal measures adopted to address such conduct in Saudi Arabia.

The study demonstrates that the effective protection of privacy requires more than the recognition of privacy as a fundamental right. It also requires clear identification of the conduct prohibited by law, careful examination of the elements establishing criminal liability, and an understanding of the relationship between criminal legislation and complementary regulatory measures. These considerations are particularly important where emerging technologies create new forms of interference that may not correspond precisely to traditional classifications of unlawful conduct.

The examination of the Saudi legal framework further demonstrates the complementary roles of the Anti-Cyber Crime Law, the Personal Data Protection Law, and national cybersecurity measures. Although these frameworks contribute to the protection of privacy, they perform different legal functions and must be interpreted according to their respective purposes and requirements.

On the basis of the preceding analysis, the research presents the following findings and recommendations.

Research Findings

1. The right to privacy is a fundamental personal right closely associated with human dignity and individual autonomy. Its scope has evolved from the protection of physical spaces and private correspondence to encompass personal information and activities conducted within digital environments.
2. Privacy-related cybercrimes are distinguished by the nature of the prohibited conduct and the legally protected interest, rather than merely by the technological means employed. Accordingly, the use of electronic devices does not, in itself, establish criminal liability.
3. The establishment of criminal liability requires proof of the constituent elements of the relevant offence, including Actus Reus (The Material Element) and Mens Rea (The Mental Element). Where a particular criminal intention or purpose is required by law, it must be established in accordance with the applicable statutory provisions.
4. Privacy-related cybercrimes may involve violations of image rights, electronic surveillance, unauthorized access to information systems, unlawful interference with personal data, and violations of private communications. Although these activities may overlap, their legal classification depends on the specific conduct and statutory requirements involved.
5. Technological developments, particularly synthetic media, artificial intelligence-assisted impersonation, and sophisticated methods of electronic deception, have introduced additional challenges to privacy protection and the application of existing criminal provisions.
6. The Saudi Anti-Cyber Crime Law establishes criminal protection against specified forms of unauthorized interception, misuse of camera-equipped devices, unlawful access, and interference with private information. These offences are subject to distinct statutory elements and penalties.
7. The Personal Data Protection Law complements criminal legislation by regulating the lawful collection, processing, disclosure, and protection of personal information, while distinguishing criminal offences from violations subject to regulatory sanctions or civil remedies.
8. National cybersecurity measures contribute to privacy protection by strengthening information security and supporting the prevention and management of cybersecurity risks. Their preventive role remains distinct from the establishment of criminal liability.

9. The Saudi judicial applications examined in this research illustrate the importance of considering the circumstances of each offence, particularly in cases involving unauthorized recording and publication of personal images. However, the selected decisions do not provide a sufficient basis for general conclusions regarding contemporary judicial practice.
10. Effective privacy protection requires complementary criminal, regulatory, preventive, and judicial mechanisms, together with a clear distinction between the different forms of legal responsibility.

Recommendations

1. Promoting the continued development of legal frameworks to keep pace with emerging technological advancements, particularly those involving synthetic media, artificial intelligence-assisted impersonation, and digital manipulation, while preserving the principles of legality and legal certainty.
2. Public awareness initiatives should be strengthened to clarify the legal consequences of privacy-related cybercrimes, the protection afforded to personal information and private communications, and the importance of responsible digital practices, particularly among young people.
3. Universities and legal education institutions should incorporate contemporary issues relating to cybercrime, digital privacy, personal data protection, and emerging technologies into relevant academic programs.
4. Specialized training should be developed for judges, prosecutors, investigators, and legal practitioners to strengthen their understanding of digital evidence, the constituent elements of cybercrimes, and the distinctions between criminal and regulatory liability.
5. The publication and systematic classification of judicial decisions concerning privacy-related cybercrimes should be encouraged to facilitate legal research and improve understanding of the practical application of relevant statutory provisions, subject to appropriate privacy safeguards.
6. Greater awareness of the obligations established under the Personal Data Protection Law should be promoted among organizations processing personal information, particularly regarding lawful processing, information security, disclosure, and breach notification.
7. Coordination among competent criminal enforcement, data protection, and cybersecurity authorities should be strengthened within their respective legal mandates to support effective responses to incidents involving privacy violations.
8. Public guidance concerning official reporting procedures and the preservation of digital evidence should be improved to encourage lawful reporting and support the investigation of suspected privacy-related cybercrimes.

9. Further legal research should examine the application of existing criminal provisions to emerging technologies, particularly artificial intelligence-generated intimate imagery and synthetic impersonation, with emphasis on the requirements of Actus Reus and Mens Rea.

References

Primary Sources and Legislation:

1. The Holy Qur'an.
2. Kingdom of Saudi Arabia. Anti-Cyber Crime Law .Council of Ministers Resolution No. 79, 1428 AH, promulgated by Royal Decree No. M/17, 1428 AH.
3. Kingdom of Saudi Arabia. Copyright Law. Royal Decree No. M/41, 1424 AH, as amended.
4. Kingdom of Saudi Arabia. Criminal Procedure Law. Royal Decree No. M/2, 1435 AH.
5. Kingdom of Saudi Arabia. Personal Data Protection Law. Royal Decree No. M/19, 1443 AH, as amended by Royal Decree No. M/148, dated 5 Ramadan 1444 AH.
6. Kingdom of Saudi Arabia. Regulations Governing Photography in Public Places. Issued in 1427 AH.
7. Ministry of Justice, Kingdom of Saudi Arabia. Collection of Judicial Judgments for the Year 1434 AH .Research Centre, Vol. 24, Case No. 34278231, p. 160.
8. Ministry of Justice, Kingdom of Saudi Arabia. Collection of Judicial Judgments for the Year 1435 AH. Research Centre, Vol. 13, Case No. 35165932, p. 295.

Books:

1. Al-Ghathbar, Khaled bin Sulaiman, and Mohammed bin Abdullah Al-Qahtani .Information Security in Simple Language. Centre of Excellence in Information Assurance, Riyadh, Saudi Arabia, 1st ed., 1429 AH/2009.
2. Al-Hait, Adel Azzam Saqf. Crimes of Defamation, Slander and Insult Committed through Electronic Media: A Comparative Legal Study. Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 1432 AH/2011.
3. Al-Jarallah, Abdulaziz bin Gharmallah. Internet Crimes and Their Penalties under the Saudi Anti-Cyber Crime Law: A Comparative Study. Dar Al-Kitab Al-Jami'i, Riyadh, Saudi Arabia, 1st ed., 1438 AH/2017.
4. Al-Mawash, Dirgham Jaber Atoush. The Crime of Information Espionage: A Comparative Study. Arab Centre for Studies and Scientific Research, Cairo, Egypt, 1st ed., 1438 AH/2017.
5. Al-Shawabkeh, Mohammed Amin. Computer and Internet Crimes. Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 4th ed., 1432 AH/2011.

6. Al-Zaidi, Taha Ahmed. Provisions Governing Information Crimes in Islamic Jurisprudence and Law. Dar Al-Fajr for Printing and Publishing, Baghdad, Iraq, 1st ed., 1438 AH/2017.
7. Al-Zuhairi, Ashjan Khalis, and Linda Mohammed Nais. Commentary on the Saudi Criminal Law: General Part. Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 1st ed., 1438 AH/2017.
8. Al-Dairabi, Ismail. Cybercrimes: A Comparative Legal and Judicial Study. National Centre for Legal Publications, Cairo, Egypt, 1st ed., 2012.
9. Al-Duaimi, Mohammed Rakan. Protection of Private Life in Islamic Law. Dar Al-Salamah, Cairo, Egypt, 1st ed., 1405 AH/1985.
10. Fuzay, Nabil. Criminal Protection of the Right to One's Image under Egyptian Law .Dar Mahmoud Publishing, Cairo, Egypt, 1st ed., 2016.
11. Ibrahim, Khaled Mamdouh. Cybercrimes. Dar Al-Fikr Al-Jami'i, Alexandria, Egypt, 1st ed., 2009.
12. Ibrahim, Khaled Mamdouh. Internet Governance. Dar Al-Fikr Al-Jami'i, Alexandria, Egypt, 1st ed., 2011.
13. Mansour, Salman, and Jamal Awad. Email with Windows. Dar Al-Bashir, Amman, Jordan, 1st ed., 1416 AH/1996.
14. Minshawi, Mohammed Abdullah. The Internet: Its Definition, Origins and Common Crimes . Minshawi Centre for Studies and Research, Makkah, Saudi Arabia, 1423 AH.
15. Sadik, Dalal, and Hamid Nasser Al-Fattal. Information Security. Dar Al-Yazouri Scientific Publishing, Amman, Jordan, 1st ed., 2008.
16. Yassin, Saad Ghaleb. Fundamentals of Management Information Systems and Information Technology. Dar Al-Manahij for Publishing and Distribution, Amman, Jordan, 1st ed., 1433 AH/2012.

Theses and Dissertations:

1. Abdelrazzaq, Moussa. Criminal Protection of Internet Users .Master's Thesis, Faculty of Law and Political Science, Larbi Tebessi University, Tebessa, Algeria, 2015–2016.
2. Al-Hait, Sama Saqf. The Right to One's Image: An Aspect of the Right to Privacy or an Independent Right ?Master's Thesis, Faculty of Law and Public Administration, Birzeit University, Palestine, 2017.
3. Al-Nasser, Mohammed Qasim. The Right to Confidentiality of Correspondence in Certain Constitutional Systems. Master's Thesis, College of Law, University of Babylon, Iraq, 1422 AH/2002.

4. Ben Haida, Mohammed. Protection of the Right to Privacy under Algerian Legislation. Doctoral Dissertation, Faculty of Law and Political Science, Abou Bekr Belkaid University, Tlemcen, Algeria, 2016–2017.
5. Ben Saeed, Sabriya. Protection of the Right to Privacy in the Age of Information and Communication Technology. Doctoral Dissertation, Faculty of Law and Political Science, Hadj Lakhdar University, Batna, Algeria, 2014–2015.
6. Bouchala, Ramzi. Interception of Telephone Calls and Taking Photographs: Between Criminalization and Permissibility .Master's Thesis, Faculty of Law and Political Science, Larbi Ben M'hidi University, Oum El Bouaghi, Algeria, 2014–2015.
7. Jallad, Salim. The Right to Privacy between Safeguards and Restrictions under Algerian Legislation and Islamic Jurisprudence. Doctoral Dissertation, Faculty of Humanities and Islamic Civilization, University of Oran, Algeria, 2013.
8. Lami, Bareq Montazer Abdulwahab. The Crime of Privacy Violation through Electronic Means under Jordanian Legislation: A Comparative Study. Master's Thesis, Faculty of Law, Middle East University, Amman, Jordan, 2017.
9. Marneez, Fatima. Infringement of the Right to Privacy through the Internet .Doctoral Dissertation, Faculty of Law and Political Science, Abou Bekr Belkaid University, Tlemcen, Algeria, 2012–2013.
10. Rabhi, Aziza. Information Secrets and Their Criminal Protection .Doctoral Dissertation, Faculty of Law and Political Science, Abou Bekr Belkaid University, Tlemcen, Algeria, 2017–2018.
11. Raddad, Simaa Jabbar. The Legal Nature of the Right to One's Image. Master's Thesis, College of Law, University of Al-Qadisiyah, Al-Diwaniyah, Iraq, 2017.
12. Rassaa, Fatiha. Criminal Protection of Information on the Internet. Master's Thesis, Faculty of Law and Political Science, Abou Bekr Belkaid University, Tlemcen, Algeria, 2011–2012.
13. Sassi, Boubaker. Criminal Protection of Private Life through the Internet. Master's Thesis, Faculty of Law and Political Science, Abderrahmane Mira University, Bejaia, Algeria, 2012–2013.
14. Salim, Al-Jaida, Bouzidi, and Hamitoush. Infringement of the Right to One's Image in the Context of Modern Technological Developments. Master's Thesis, Faculty of Law and Political Science, Abderrahmane Mira University, Bejaia, Algeria, 2015–2016.
15. Saghir, Youssef .Crime Committed through the Internet. Master's Thesis, Faculty of Law and Political Science, Mouloud Mammeri University, Tizi Ouzou, Algeria, 2013.
16. Al-Sulami, Mansour bin Saleh. Civil Liability for Privacy Violations under the Saudi Anti-Cyber Crime Law .Master's Thesis, College of Graduate Studies, Naif Arab University for Security

Sciences, Riyadh, Saudi Arabia, 1431 AH/2010.

Academic Journal Articles:

1. Abdelkader, Omaimer. "Criminal Protection of the Right to Privacy in the Digital Environment ". Journal of Law and Business, Hassan I University, Morocco, No. 20, 2018.
2. Al-Obaidi, Osama bin Ghanem. "Protection of the Right to Privacy against Computer and Internet Crimes". Arab Journal for Security Studies and Training, Riyadh, Saudi Arabia, No. 47, 1429 AH.
3. Al-Shukri, Adel Youssef. "Cybercrime and the Crisis of Criminal Legality". Journal of the Kufa Studies Centre, University of Kufa, Iraq, No. 7, 2008.
4. Al-Hawamdeh, Lawrence Saeed. "Cybercrimes: Their Constituent Elements and Methods of Combating Them". Al-Mizan Journal for Islamic and Legal Studies ,Jordan, No. 1, 2016–2017.
5. Al-Daihany, Fahed Mohsen. "The Legal Nature of the Right to One's Image and Its Civil Protection under Kuwaiti Law". Arab Journal for Security Studies and Training ,Naif Arab University for Security Sciences, Saudi Arabia, No. 56, 2017.
6. Al-Khasawneh, Al-Momani, Alaa Al-Din Abdullah Fawaz, and Bashar Talal. "The Legal Framework of Photographs: Associated Rights and Legal Protection ".Journal of Sharia and Law, United Arab Emirates University, No. 53, 2013.
7. Ben Dawood, Shat, Ibrahim, and Ashraf. "Access to Electronic Mail". Dafater Al-Siyasa wa Al-Qanun, Djillali Liabes University, Algeria, No. 16, 2017.
8. Ghayeb, Mahrous Nassar. "Cybercrime". Al-Taqani Journal ,Technical Education Authority, Iraq, No. 9, 2011.
9. Ghoneim, Riham Asim. "Personal Information Available on the Web". Recent Trends in Libraries and Information, Cairo, Egypt, No. 37, 2012.
10. Gharib, Majeda, and Hassan Al-Amir. "Awareness among Young People of the Saudi Cybercrime Penalty System". Arab International Journal of Informatics, Saudi Arabia, No. 9, 2017.
11. Hadi, Uday Jaber. "Criminal Protection of Email". Risalat Al-Huquq Journal, Iraq, No. 3, 2010.
12. Khalfi, Abdelrahman. "The Right to Private Life under Algerian Criminal Legislation". Journal of Communication in Economics, Administration and Law, University of Bejaia, Algeria, No. 45, 2016.
13. Maashi, Samira. "The Concept of Cybercrime". Legal Forum Journal, University of Biskra, Algeria, No. 7, 2010.

14. Naima, Majadi. "Criminal Protection of the Right to One's Image". Journal of Legal Studies and Research, University of M'sila, Algeria, No. 7, 2017.
15. Rabee, Ziad Mohammed. "Infringement of the Inviolability of Private Life under Cybercrime Law". Journal of Legal and Political Sciences, Algeria, No. 1, 2016.
16. Salman, Ouda Youssef. "Crimes Violating the Right to Privacy through Modern Information Technology". Journal of Law, Iraq, Nos. 29–30, 2017.
17. Zawawi, Chenna. "Legal Protection of an Individual's Right to Their Image". Dafater Al-Siyasa wa Al-Qanun, Djillali Liabes University, Algeria, No. 13, 2015.

Official Reports and Electronic Sources:

1. Chandra, Bilva, Jesse Dunietz, Kathleen Roberts, Yooyoung Lee, Peter Fontana, and George Awad. Reducing Risks Posed by Synthetic Content: An Overview of Technical Approaches to Digital Content Transparency. NIST AI 100-4, National Institute of Standards and Technology, United States, 2024.
2. Computer Emergency Response Team for the EU Institutions, Bodies and Agencies (CERT-EU). Threat Landscape Report 2025: A Year in Review. European Union, 2026.
3. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2026. European Union, 2026.
4. National Cybersecurity Authority (NCA). Essential Cybersecurity Controls (ECC 2-2024). Kingdom of Saudi Arabia, 2024.