



Mechanisms for Combating Cybercrime at the International and National Levels

Khaled khelif *

Badji Mokhtar University – Annaba

khaled_khelif@hotmail.fr

Received:05/07/2025

Accepted: 21/08/2025

Published: 25/09/2025

Abstract :

This article discusses cybercrime from various perspectives, starting with an overview of its definition and impact on individuals, institutions, and states. It also addresses the different types of cybercrimes, such as cyber-attacks, electronic fraud, industrial espionage, and data breaches. The article highlights the legal efforts made to combat these crimes at both international and national levels, including international agreements like the Budapest Convention of 2001 and the United Nations Convention of 2024. Additionally, it discusses national efforts through laws that criminalize cybercrimes and the establishment of the Algerian National Cybercrime Prosecutor's Office to tackle crimes related to information and communication technologies. Finally, the article touches upon the challenges related to the violation of digital privacy in the context of combating cybercrime and the need for legal safeguards to prevent the infringement of individuals' fundamental rights.

Keywords : Cybersecurity. Cybercrime. International Mechanisms .National Efforts.

* Corresponding author ☐



Introduction:

In the context of rapid technological advancement and the growing reliance on the Internet across all spheres of life, cybercrime has emerged as one of the most pressing and complex challenges confronting individuals, institutions, and states alike. With the increasing use of electronic networks and the evolution of digital communication tools, cybercrimes now pose significant threats to information security, infringe upon individual privacy, and target governmental, financial, and commercial systems in unprecedented ways.

Amid this remarkable technological development, cybercrime has evolved into a transnational threat that transcends conventional geographic boundaries. The growing dependence on the Internet and digital systems has fostered an environment in which cybercriminals can perpetrate fraud, hacking, espionage, and other illicit acts with relative impunity.

Addressing cybercrime requires a multifaceted and coordinated approach, involving collaboration among governmental bodies, security agencies, and private sector entities. Equally important is the promotion of legal and technical awareness among individuals. Key strategies to combat cybercrime include the development of specialized legal frameworks, the deployment of advanced technologies for detection and response, and the enhancement of international cooperation to pursue offenders who exploit cyberspace as a sanctuary for their criminal activities.

Given the grave implications of this phenomenon, it is imperative to reinforce cybersecurity measures and adopt proactive, preventive policies aimed at safeguarding data and digital infrastructure. Continuous legal reform and robust international cooperation are essential instruments for ensuring a secure digital environment that fosters trust in online interactions and protects the rights of individuals, communities, and nations.

This research paper seeks to explore the central question:

To what extent are international and legal efforts effective in combating cybercrime?

This primary question gives rise to several subsidiary inquiries:

- What are the main categories of cybercrime?
- What are the most significant international and national legal frameworks addressing cybercrime?
- What forms of digital privacy violations arise in the context of cybercrime prevention?

To address these questions, the study is structured around two main sections:

The first section focuses on the classification of cybercrimes, while the second examines both international and national efforts to combat this phenomenon.

Section I: Classification of Cybercrimes

Cybercrime is defined as any illegal act committed via the internet or through the use of computer systems. This includes offenses such as online fraud, system hacking, data theft, virus dissemination, as well as crimes related to defamation and cyber extortion. Due to their transnational nature, combating such crimes necessitates international cooperation and the



development of modern legal frameworks that align with the rapid advancements of the digital age.

In this context, international instruments have defined cybercrime as any unlawful act committed through the use of information technology or directed against information systems or digital data. Several international conventions have provided definitions of this type of crime.

For instance, the Budapest Convention on Cybercrime (2001) defines cybercrime as “any criminal offense committed against the confidentiality, integrity, or availability of data or computer systems, or any crime committed using information systems.” These crimes include unauthorized access to information systems (hacking), illegal interception of data, data manipulation or misuse, as well as content-related offenses such as the dissemination of illegal materials or fraud committed through information technology.¹

Considering that cybercrime refers to any criminal activity committed through computers or electronic networks targeting individuals, institutions, or states including unauthorized access, cyber fraud, identity theft, dissemination of malicious software, and cyberattacks on critical infrastructure it is evident that cybercrimes can be categorized into three main types.

These will be addressed in three subsections: the first will examine cybercrimes against individuals, the second will explore those targeting institutions, and the third will focus on cybercrimes directed against states.

A) : Crimes Against Individuals

Cybercrimes are among the most dangerous challenges facing individuals and societies in the digital age, as modern technologies are exploited to commit crimes that target individuals directly. These crimes encompass a wide range of illegal activities that affect privacy, personal security, and digital property.

1): Types of Cybercrimes Against Individuals

1- Cyber Fraud: This involves identity theft to obtain sensitive information such as banking details, and phishing attacks through fraudulent emails that deceive victims into revealing their information.

2- Cyber Extortion: This involves threatening to publish personal information or sensitive images to demand a ransom, as well as hacking into private accounts and requesting money in exchange for restoring access.

3- Defamation, Insult, and Slander Online: This involves spreading false or defamatory information about individuals via social media, and using emails or forums to circulate misleading news with the aim of damaging a person's reputation.

4- Cyber Harassment and Digital Bullying: This involves sending threatening or harassing messages online and publishing offensive content with the intention of causing psychological or social harm to others.

5- Hacking and Privacy Violations: This includes spying on electronic devices, stealing personal data, and using malicious software (Malware) to gain unauthorized access to devices and files.



6- Digital Identity Theft: This involves using the victim's information to create fake accounts, conduct illegal transactions, or hijack social media or email accounts and use them unlawfully.

7- Online Sexual Exploitation: This includes luring minors online for sexual exploitation, as well as distributing or publishing illegal content containing exploitative images or videos.²

B): Protection Methods Against Cybercrimes Targeting Individuals

A number of important measures and practical steps can be adopted to combat cybercrimes against individuals. These can be summarized in the following points:

- Use strong passwords and change them regularly.
- Avoid oversharing personal information online.
- Verify the sources of emails before opening or interacting with them.
- Update security and protection software on smart devices and computers.
- Report cybercrimes through designated legal channels.
- Raise awareness about digital risks among the community, especially children

and adolescents

B): Cybercrimes Against Institutions

Cybercrimes targeting institutions have become a serious threat facing businesses globally, as these crimes target sensitive data, systems, and digital assets of institutions. In this context, cybercrimes against institutions refer to any illegal activities conducted via the internet or digital systems that target the data, resources, or systems of a specific institution, whether it is a private or public company. Examples include data breaches and theft of sensitive business information.

1): Types of Cybercrimes Against Institutions

* Cyber Attacks : These refer to attacks using malicious software (Malware) such as viruses, Trojans, and ransomware, or Distributed Denial of Service (DDoS) attacks, which flood servers with massive requests to disrupt their operation.

* Cyber Fraud and Embezzlement:

- Theft of money through banking hacking.
- Forgery of invoices and online financial transactions.

* Industrial Espionage and Data Theft:

- Spying on companies and stealing intellectual property.
- Hacking into systems to obtain confidential information.

* Data Breaches and Information Leaks:

- Unauthorized access to databases.
- Leaking customer and employee information.

C)Section Three: Cybercrimes Against States

With the rapid technological advancements, cyberattacks have become a real threat to countries, as they target critical infrastructure, government systems, and economic sectors. These attacks vary in their objectives and methods, making them a strategic tool used in modern warfare and geopolitical conflicts.



1): Types of Cyberattacks Against States

Cyberattacks targeting states can be classified into several types, the most important of which include:

- **Disruptive Attacks :** These aim to disrupt essential government or vital services such as electricity, water, telecommunications, and all civilian life systems, causing a paralysis in the service sector.
- **Espionage Attacks :** These attacks target the theft of sensitive information from government or military institutions, and they are often organized and precise.
- **Financial Attacks :** These are used to steal money or disrupt banking and financial systems by attacking major banks and financial exchange centers.
- **Infrastructure Attacks :** These attacks focus on a country's infrastructure, particularly energy, transportation, and health systems, potentially leading to a complete shutdown of the state.³
- **Disinformation & Propaganda Attacks:** These attacks aim to spread fake news and influence public opinion on various political, economic, and social issues.

Section II : Legal Efforts to Combat Cybercrimes

National and international legislations aim to combat cybercrimes by establishing various systems, procedures, and measures at both national and international levels. However, these measures can impact the enjoyment of the right to digital privacy for individuals and societies.

Therefore, in this section, we will highlight international efforts to combat cybercrimes in the first part, then discuss national efforts to combat cybercrime, and finally, we will focus on certain violations that affect the right to digital privacy in the name of combating cybercrime in the third part.

A) : International Efforts to Combat Cybercrimes

In response to the increasing global cyberattacks, the international community has sought to establish international conventions between the parties of the international community to combat these crimes. Perhaps the most notable of these conventions is the Budapest Convention of 2001, as well as the United Nations Convention on the Prevention and Combating of Cybercrime, which was established in 2024.

1): The Budapest Convention of 2001

With the increasing reliance on digital technology, the urgent need to establish international legal frameworks to combat cybercrimes emerged. The Budapest Convention of 2001 is considered one of the most important international treaties in this field, as it aims to harmonize national legislations and enhance international cooperation to combat crimes committed over the internet.



*** Substantive Rules in the Budapest Convention of 2001**

The convention includes a set of substantive rules that obligate member states to criminalize specific acts in their national legislations. These substantive rules include:

- Crimes Related to the Confidentiality and Integrity of Data:

These involve unauthorized access to, or tampering with, computer systems or data, as well as illegal interception, destruction, modification, or disruption of data without authorization.

- Crimes Related to Content : This includes crimes related to child exploitation in pornography, such as the production, distribution, provision, acquisition, or possession of child pornography.⁴

- Crimes Related to Intellectual Property Rights : Violations of copyright and related rights through the unauthorized copying, distribution, broadcasting, or making available of protected works.

*** Measures and Sanctions in the Budapest Convention of 2001**

The convention outlines several sanctions and measures aimed at ensuring that each state party adopts the necessary legislative and other measures to guarantee that the crimes specified in Articles 2 to 11 are subject to effective, proportionate, and deterrent penalties, including custodial sentences.⁵

Furthermore, the convention ensures that each state party holds legal persons accountable in accordance with Article 12 of the convention text, subjecting them to effective, proportionate, and deterrent sanctions or measures, whether they are criminal or non-criminal, including financial penalties.

2): The United Nations Convention on the Prevention and Combating of Cybercrime (2024)

The United Nations Convention on Cybercrime aims to prevent and combat cybercrimes more efficiently and effectively, including through enhanced international cooperation, technical assistance, and capacity-building support, particularly for developing countries.

The United Nations Office on Drugs and Crime (UNODC) stated in a press release after the adoption of the convention that it acted as the secretariat for the negotiations. The convention represents the first comprehensive international treaty on cybercrime in 20 years and is considered a critical step forward in addressing crimes such as online child sexual abuse, complex online fraud, and money laundering.

The convention will be opened for signature at an official ceremony hosted by Vietnam in 2025, and it will enter into force 90 days after being ratified by the fortieth signatory state.

The United Nations Convention on the Prevention and Combating of Cybercrime (2024) consists of several key sections aimed at enhancing international efforts to confront cyber threats. Its main contents can be summarized as follows:



1- General Provisions : These provisions define the scope of the convention and provide definitions for key terms used within it, such as "cybercrime" and "information system." Essentially, the convention outlines the conceptual framework for cybercrime.

2- Criminalization : The convention obligates member states to criminalize a range of acts related to cybercrime, including:

- Unauthorized Access: Unauthorized entry into computer systems or networks.
- Illegal Data Interception: Eavesdropping or obtaining data during transmission without authorization.
- Data or System Damage: Destroying, modifying, or disabling data or computer systems.
- Misuse of Devices: Producing or distributing tools used to commit cybercrimes.

3- Procedural Measures : These include mechanisms for investigation and prosecution, such as:

- Data Retention : Requiring service providers to retain data for a specific period to support investigations.
- Search and Seizure : Granting authorities the power to search devices and seize digital evidence.
- Access to Stored Data : Enabling authorities to access data stored in systems.

4- International Cooperation : The convention emphasizes the importance of cooperation between countries through:

- Mutual Legal Assistance : The exchange of information and evidence between states for investigations and prosecutions.
- Extradition of Offenders : Establishing mechanisms for the extradition of individuals accused of committing cybercrimes.
- Training and Capacity-Building : Providing technical support and training to developing countries to enhance their capabilities in combating cybercrime.

5- Human Rights Protection : The convention underscores the need to respect human rights and fundamental freedoms while implementing measures to combat cybercrime, including the protection of privacy and freedom of expression.

B): National Efforts to Combat Cybercrime

The Algerian legislator amended the Penal Code through Law No. 04-15, which aims to protect information processing systems from cybercrimes. This law criminalizes acts such as unauthorized access to information systems, data destruction, and the use of systems for harmful purposes.

In addition, Law No. 09-04 was issued regarding the special rules for preventing and combating crimes related to information and communication technology. This law aims to establish a comprehensive legal framework for preventing and combating cybercrimes, with a focus on the necessary preventive and procedural measures.⁶



1): The National Specialized Pole for Combating Cybercrime

The pole is a specialized body responsible for investigating and prosecuting cybercrimes, thereby enhancing the effectiveness of applying these laws in response to the increasing number of cybercrimes and their impact on the security and stability of society. Algeria established the "National Judicial Pole for Combating Crimes Related to Information and Communication Technologies" under Order No. 21-11 dated August 25, 2021, which amends and supplements the Criminal Procedure Law.

This pole has expanded jurisdiction, both in terms of subject matter and territorial reach, covering the entire national territory. Its aim is to improve the efficiency of the judicial system in dealing with crimes associated with modern technology.

Referring to the provisions of Article 211 bis 22 of Order No. 21-11, the newly established pole is responsible for handling crimes related to information and communication technologies, as well as crimes associated with them, whether during the prosecution stage by the public prosecutor, the judicial investigation stage by investigating judges, or the trial stage.⁷

The pole is exclusively responsible, throughout the national territory, for addressing crimes related to information and communication technologies, as listed exhaustively. Article 211 bis 24 defines these crimes as follows:

- Crimes affecting national security or national defense.
- Crimes related to spreading and promoting false news among the public that could harm security, public order, or societal stability.
- Crimes related to the dissemination and promotion of malicious information that undermines public order and security, with a systematic or transnational nature.⁸
- Crimes affecting automated data processing systems related to public administrations and institutions.
- Crimes related to human trafficking, organ trafficking, or migrant smuggling.
- Crimes of discrimination and hate speech.⁹

Thus, the role of the National Judicial Pole includes monitoring and investigating cybercrimes, as well as issuing rulings in misdemeanors related to these crimes. This judicial specialization is considered an important step in enhancing the justice system's capacity to combat this type of crime.

C): Forms of Violation of the Right to Digital Privacy in Light of Cybercrime Combat

The fight against cybercrime in the interconnected digital world has many dimensions. As countries, institutions, organizations, or even individuals strive to protect national security and combat cybercrime, numerous violations can occur under the guise of national security protection. These violations take various forms, and they can be summarized as follows:

1) Unlawful Collection and Storage of Personal Data

There are instances where security agencies conduct search operations for virtual suspects without seeking judicial authorization to track and monitor individuals. In such cases, we are confronted with clear violations of individuals' right to privacy.



Some of these methods include:¹⁰

- Monitoring, intercepting, and extracting messages exchanged via email.
- Secretly connecting wires to computers where the targeted data is stored in order to seize it.

2) Electronic Espionage on Private Life

This refers to obtaining instant access to an individual's private life, such as obtaining their bank balance, commissions,¹¹ travel ticket dates, and social security number. Matters become even more complicated when official entities eavesdrop on emails for the sake of protecting national security or maintaining public order.¹²

For instance, the U.S. wiretapping law allows the U.S. intelligence agency to monitor phone calls and emails of foreigners and residents in the U.S. without judicial authorization, granting U.S. authorities the right to spy on all conversations.¹³

3): Unlawful Disclosure and Misuse of Data

Some government agencies in many countries unlawfully disclose digital data of numerous individuals. In these cases, personal data may be collected, stored, and processed legally, but it is then unlawfully disclosed or misused by those responsible for its storage. This includes situations where the individuals who have access to the data either disclose it improperly or misuse it in some form.

4): Failure to Adhere to Procedural Rules in Collecting, Processing, and Publishing Personal Data

Governments may sometimes resort to other economic or administrative sectors that have the authority to process personal digital data of citizens or non-citizens.¹⁴ These entities may collect, store, and process such data even when the law requires prior authorization for these activities. Failure to comply with the laws related to privacy and personal data will be considered a gross violation of individuals' and communities' privacy rights.¹⁵

5): Electronic Intrusion

Some countries, under the pretext of national security protection, infiltrate the data of public and private sector companies and institutions, extracting personal information that impacts the lives of employees and workers, and accessing their files without authorization.¹⁶

This includes, for example, direct eavesdropping on the essential communication infrastructure, breaching it, or exercising regulatory control over a third party that physically controls the data. This also involves copying all digital and informational data from these companies and institutions, using it for security or intelligence research operations.¹⁷

In this context, it is important to note that the impact of the right to privacy, due to national security protection measures, has further implications on collective rights that go beyond the commonly recognized ones, such as the right to digital communication, the collection of personal data, and others. These implications extend to violations of other rights, such as the right to freedom of opinion and expression, the right to access, receive, and disseminate information, the right to peaceful assembly and association, and the right to family life—rights that are all closely tied to the right to privacy. Therefore, if the value of the right to privacy



Mechanisms for Combating Cybercrime at the International and National Levels

requires its limitation for national security reasons, it should be done in accordance with clear conditions and specific standards, which can be summarized as follows:

- The electronic surveillance should be based on a law with clear specifications. This means the need for legal guarantees to define the surveillance system, along with oversight and retroactive remedies, to ensure that the system is not misused.¹⁸

- It must be authorized by a competent authority.

The authorization for national security protection should be handled by a judicial body or an administratively empowered authority, with confidentiality rights preserved. Governments have the right to secure their territories and protect their national security.¹⁹

- It should not violate international human rights law:

This is outlined in the UN General Assembly Resolution 167/68 of 2013 on the right to privacy in the digital age, which relied on the 2014 report from the UN High Commissioner for Human Rights on the right to privacy in the digital era.²⁰

- The surveillance should be temporary:

The period of personal electronic surveillance should not exceed the legally specified time limit or the duration determined by a judicial authority.²¹

- There should be no discrimination among those being surveilled:

Electronic surveillance that violates the right to privacy should not be directed based on political beliefs,²² specific ideological thought, religion, or any other form of legally and ethically unacceptable discrimination.²³

Conclusion:

Cybercrime is considered one of the most serious challenges facing the modern world, as it poses a direct threat to the security of individuals, institutions, and states. With the rapid technological advancements and the increasing reliance on the digital space across all aspects of life, cybercrimes have taken on increasingly complex and sophisticated forms that are difficult to detect and confront through traditional means. This reality necessitates the establishment of effective legal and regulatory frameworks, in addition to the development of advanced security and technological mechanisms to address these crimes.

This research has explored the various types of cybercrimes, whether those targeting individuals such as cyber extortion and identity theft or those directed at institutions and companies, like attacks on databases and information systems. It also addressed crimes that threaten national security, such as information warfare and cyber espionage. Furthermore, it examined national and international efforts to combat these crimes in pursuit of a safe and sustainable digital environment.

Despite the multiplicity of initiatives and legal frameworks, many challenges remain. Chief among these are the rapid evolution of cybercrime techniques, the difficulty of tracing perpetrators due to their use of advanced anonymity and encryption technologies, and the lack of legal harmonization among countries, which complicates judicial cooperation and prosecution.

Based on these considerations, combating cybercrime requires adopting a comprehensive vision that integrates the development of national legislation in line with



technological advancements, enhancing international cooperation and the exchange of information and expertise, and raising digital awareness among individuals and institutions regarding protection methods and how to confront cyber threats.

In this context, there is a pressing need to establish specialized cybersecurity units within governmental and military bodies, develop advanced protection systems based on artificial intelligence and machine learning technologies, and activate international treaties and agreements aimed at limiting cross-border cyberattacks. Moreover, public education on cybercrime and prevention tools remains a fundamental pillar in reinforcing digital resilience at the level of nations and societies.

conditions :

¹ - United Nations General Assembly Resolution 55/63 of 2000 defined cybercrime as attacks on the integrity and security of information systems, and fraudulent or malicious activities carried out over the Internet.

² - Mahdi Reda, Cybercrime and Means of Combating It in Algerian Legislation, Eliza Journal of Research and Studies, Issue 6, 2021, p. 115

³ -Mahdi Reda, Cybercrime and Means of Combating It in Algerian Legislation, Eliza Journal of Research and Studies, Issue 6, 2021, p. 116

⁴ -Qataf Suleiman and Bougrine Abdelhalim, Objective Legal Mechanisms for Combating Cybercrime in Light of the Budapest Convention and Algerian Legislation, Academic Journal of Legal and Political Research, Issue 1, Volume 6, 2022, pp. 340-341

⁵ - See the text of Chapter Five: Additional Liability and Penalties from the 2001 Budapest Convention on Cybercrime

⁶ - -Souad Ouajatout, Combating Cybercrime at the National Level, Journal of Scientific Research Notebooks, Volume 12, Issue 2, 2024, p. 424

⁷ - Bouguera Jamal and Anan Jamal Eddine, National Penal Pole for Combating Related Crimes In Information and Communication Technologies, Al-Ustadh Al-Baheth Journal for Legal and Political Studies, Volume 7, Issue 1, 2022, p. 1677

⁸ -Bouguerra Jamal and Anan Jamal Al-Din, The National Penal Pole for Combating Crimes Related to Information and Communication Technologies, Al-Ustadh Al-Baheth Journal for Legal and Political Studies, Volume 7, Issue 1, 2022, p. 1685

⁹ - Suad Wajtout, Combating Cybercrime at the National Level, Scientific Research Notebooks Journal, Volume 12, Issue 2, 2024, p. 423

¹⁰ - -Barq Muntadhar Abdul Wahab, The Crime of Violation of Privacy Through Electronic Means in Jordanian Legislation, Master's Thesis, Middle East University, 2017, p. 113

¹¹ - -Susan Adnan and Safaa Otani, Violation of the Sanctity of Private Life via the Internet: A Comparative Study, Damascus University Journal for Legal and Economic Sciences, Volume 29, Issue 3, 2013, p. 435



¹² - Ibrahim bin Daoud Ashraf Shaat, Access to Electronic Mail between the Requirements of Public Order and the Right to Confidentiality of Correspondence, Politics and Law Notebooks, Issue 16, January 2017, p. 29.

¹³ - Barq Muntadhar Bad Al-Wahhab, The Crime of Violating Privacy Through Electronic Means in Jordanian Legislation, Master's Thesis, Middle East University, 2017, p. 115

¹⁴ - Barq Muntadhar Bad Al-Wahhab, The Crime of Violating Privacy Through Electronic Means in Jordanian Legislation, Master's Thesis, Middle East University, 2017, p. 116

¹⁵ - Example: The French Law on the Electronic Processing of Personal Data issued in 1978 stipulates in Article 41 that:

"Anyone who conducts or undertakes the electronic processing of personal data without a license from the competent committee shall be punished by imprisonment from six months to three years and a fine of 14,000 francs, or one of these two penalties." According to the same law, the court may order the publication of the entire judgment or a summary thereof in one or more newspapers, under the conditions specified in the judgment

¹⁶ - Susan Adnan, Safaa Ontli, The Crime of Violating Privacy via the Internet: A Comparative Study, Damascus University Journal of Legal and Economic Sciences, Volume 29, Issue 3, 2013, p. 436.

¹⁷ - Report of the Office of the High Commissioner for Human Rights, The Right to Privacy in the Digital Age, page 6, paragraph 14, document number A/HRC/27/37

¹⁸ - Report of the Office of the High Commissioner for Human Rights, Summary of the Panel Discussion on the Right to Privacy, dated December 19, 2014, page 10, paragraph 27, document number A/HRC/28/39

¹⁹ - Report of the Office of the High Commissioner for Human Rights, Summary of a Panel Discussion on the Right to Privacy, dated 19 December 2014, pp. 5, paras. 9 and 10, document no. A/HRC/28/39

²⁰ - Report of the Office of the High Commissioner for Human Rights, Summary of a Panel Discussion on the Right to Privacy, dated 19 December 2014, page 5, paragraph 12, document number A/HRC/28/39.

²¹ - Brahim Ben Daoud, Ashraf Shaat, Access to Email: Between the Requirements of Public Order and the Right to Confidentiality of Correspondence, Journals of Politics and Law, issue 16, January 2017, page 38.

²² - Report of the Office of the High Commissioner for Human Rights, Summary of a Panel Discussion on the Right to Privacy, dated 19 December 2014, p. 5, para. 10, document no. A/HRC/28/39

²³ - As stated in the OHCHR report: "International human rights law permits interference with an individual's right to privacy only if such interference is neither arbitrary nor unlawful. The Human Rights Committee clarified in its General Comment No. 11 that the term "unlawful" means that interference may only occur "in cases provided for by law. Interference authorized by States may only occur on the basis of law, which must itself be consistent with the provisions, aims, and objectives of the Covenant".



Bibliography List setting:

1: Legal Texts

- United Nations General Assembly, Resolution 55/63 on Combating the Criminal Misuse of Information Technologies, 2000.
- Budapest Convention on Cybercrime, Council of Europe, 2001, Chapter Five: Additional Liability and Penalties.
- French Law on the Electronic Processing of Personal Data, Law No. 78-17 of 6 January 1978, Article 41.

2: Memory (Theses and Dissertations)

- Barq, Muntadhar Abdul Wahab, The Crime of Violation of Privacy Through Electronic Means in Jordanian Legislation, Master's Thesis, Middle East University, 2017

3: Articles

- Mahdi, Reda, Cybercrime and Means of Combating It in Algerian Legislation, Eliza Journal of Research and Studies, Issue 6, 2021
- Qataf, Suleiman and Bougrine, Abdelhalim, Objective Legal Mechanisms for Combating Cybercrime in Light of the Budapest Convention and Algerian Legislation, Academic Journal of Legal and Political Research, Vol. 6, No. 1, 2022
- Ouajatout, Souad, Combating Cybercrime at the National Level, Journal of Scientific Research Notebooks, Vol. 12, No. 2, 2024
- Bouguera, Jamal and Anan, Jamal Eddine, National Penal Pole for Combating Crimes Related to Information and Communication Technologies, Al-Ustadh Al-Baheth Journal for Legal and Political Studies, Vol. 7, No. 1, 2022
- Adnan, Susan and Otani, Safaa, Violation of the Sanctity of Private Life via the Internet: A Comparative Study, Damascus University Journal for Legal and Economic Sciences, Vol. 29, No. 3, 2013
- Shaat, Ibrahim bin Daoud Ashraf, Access to Electronic Mail between the Requirements of Public Order and the Right to Confidentiality of Correspondence, Politics and Law Notebooks, Issue 16, January 2017

4: Websites / Electronic Sources

- Office of the High Commissioner for Human Rights (OHCHR), The Right to Privacy in the Digital Age, UN Doc. A/HRC/27/37, 2014
- OHCHR, Summary of the Panel Discussion on the Right to Privacy, 19 December 2014, UN Doc. A/HRC/28/39
- OHCHR Report: "International human rights law permits interference with an individual's right to privacy only if such interference is neither arbitrary nor unlawful...", General Comment No. 11.