

Mechanisms Anti Crimes Electronic And its role in promoting Security Cyber

Received date: 18/04/2025**Accepted date: 19/05/2025**

KHALFALLAH Adel*
Badji Mokhtar Annaba University
Maghrebian laboratory of legal
studies

adel.khalfallah@univ-annaba.dz

MILOUD Hocine
Badji Mokhtar Annaba University
Maghrebian laboratory of legal
studies

miloud.hocine@univ-annaba.dz

Abstract:

The rapid advancement of digital technologies and the Internet has given rise to numerous criminal activities that jeopardize individuals' privacy and national security, despite being safeguarded by international and national laws concerning the collection and processing of personal data. Due to the gravity of cybercrimes and their

direct link to technological progress, the global community has recognized the need to act decisively by enacting comprehensive legislation to address these threats.

In an effort to harmonize cybersecurity-related laws, several international agreements and conventions have been established to combat cybercrimes. Among the most notable is the Budapest Convention, issued by the European Union, which stands as the first international treaty dedicated to address crimes associated with modern technology.

Keywords: (Cybersecurity; Personal Data; Cybercrime; Informatics; Cyber Threats)

Introduction:

Today, we live in an era dominated by information and communication technology, which has become the cornerstone of many aspects of life. Society has evolved from a consumer-based economy to an industrial one, and now to a digital society, largely due to the digital services offered by modern technologies, which are characterized by speed and low cost.

With the arrival of the new millennium, numerous lifestyle changes emerged, leading to a fundamental shift in the relationships between individuals and states. The advancement of communication methods, particularly the rise of social media, which has gained millions of users worldwide, brought about several challenges. Despite the numerous benefits these platforms offer, they also pose risks to individuals' privacy and security. In many cases, they can even threaten the security

* - Corresponding author.

and sovereignty of states.

We frequently hear in the media about cybercrimes and electronic offenses resulting from malicious attacks on computer devices and information systems. These incidents have prompted governments to raise the alarm and take action, either individually through national legislation aimed at combating crimes against personal data or collectively through international cooperation. This includes concluding treaties and agreements with specialized organizations to mitigate and reduce the impact of such crimes.

The significance of this study lies in the impact of cyber threats on individuals, state institutions, and entire societies. Regardless of their resources or capabilities, all countries are striving to combat cybercrime to ensure cybersecurity. Cybersecurity has become one of the most critical contemporary issues for nations due to the rapid and unprecedented advancement of modern communication technologies, which can expose countries to risks that threaten their security and sovereignty.

This study aims to analyze key international and national legislation designed to combat cybercrime and strengthen cybersecurity. It also highlights newly introduced concepts related to cybersecurity.

Accordingly, the main research question is: What mechanisms can effectively reduce cybercrime and ensure cybersecurity?

To address this question, the study is structured into two main sections. The first section examines the concepts of cybersecurity and cybercrime, while the second discusses international and national mechanisms for combating cybercrime.

The nature of the topic necessitates the use of both descriptive and analytical approaches. The analytical method is applied to review and interpret international and national legislative texts related to cybersecurity, aiming to draw meaningful conclusions. Simultaneously, the descriptive method is employed to explain key concepts and terms related to the subject, ensuring a clearer understanding and better contextualization.

Chapter I: A Conceptual Framework for Cybersecurity and Cybercrime

With the ongoing digital revolution and the rapid advancements in modern communication technologies, many nations have experienced a significant rise in electronic security threats. Cybersecurity has

emerged as one of the most pressing challenges at both national and global levels, as it poses a threat to the integrity and stability of state sovereignty

In this section, we will explore the conceptual framework by examining two key aspects: the concept of cybersecurity (first subsection) and the concept of cybercrime (second subsection).

First Subtitle: The Concept of Cybersecurity

Safeguarding users of modern technology in the digital age has become a critical necessity, particularly with the growing use of electronic networks and the associated cyber risks. Countries are making concerted efforts to protect their information systems, as cybersecurity represents a fundamental pillar of their criminal security policies.

In this context, we will first define cybersecurity (first subsection), then discuss the most significant terms related to cybersecurity (second subsection), and finally dedicate the third subsection to exploring the dimensions of cybersecurity.

A) The Legislative and Jurisprudential Definition of Legal Security

International and national legislations, along with jurisprudence, have varied in their attempts to establish a unified definition of cybersecurity. Therefore, we will examine the most significant legislative and jurisprudential definitions:

1- Legislative Definitions of Cybersecurity

The International Telecommunication Union (ITU) defined cybersecurity in its 2010-2011 report on trends in telecommunication reform, which serves as a consensus framework for various intellectual and professional perspectives. According to the ITU, cybersecurity is: "A set of tasks, including the collection of resources, policies, security procedures, guidelines, risk management approaches, training, best practices, and techniques aimed at protecting the cyber environment and the assets of institutions and users."⁽¹⁾

The regulation No. 2019/881, issued by the European Parliament and Council, relates to cybersecurity. According to the first paragraph of its second article, it defines cybersecurity as: "Measures necessary to protect networks, information systems, their users, and other individuals exposed to cyber threats."⁽²⁾

At the national level, the Algerian legislator defined cybersecurity in



Article 10, paragraph 3 of Law No. 18/04, which outlines the general rules regarding mail and electronic communications. It is defined as: "The collection of tools, data, security concepts, mechanisms, guidelines, risk management methods, practices, training, guarantees, and technologies that can be used to protect electronic communications from any event that could affect the availability and integrity of stored, processed, or transmitted data."⁽³⁾

2- The Jurisprudential Definition of Cybersecurity

Jurisprudence has not reached a consensus on a unified definition of cybersecurity. This is due to the nature of cybercrime, which cannot be confined to specific actions, as it evolves in response to rapid technological advancements. Therefore, we will examine the most significant jurisprudential definitions:

It is a collection of technical, organizational, and administrative measures used to prevent unauthorized access and misuse, recover electronic information, communications, and information systems, enhance the protection, confidentiality, and privacy of personal data, and implement necessary actions to protect citizens and consumers from risks in cyberspace⁽⁴⁾.

Cybersecurity is also defined as the measures and procedures used to protect both civil and military cyberspaces from threats that could harm the information infrastructure⁽⁵⁾.

Based on the previous definitions, cybersecurity can be defined as the technologies used to protect devices and software from digital attacks that may threaten the confidentiality, integrity, and accuracy of the data being processed.

B) Key Terms Related to Cybersecurity

There are numerous concepts and terms associated with cybersecurity, and the most important are:

1- Cyberspace: It refers to the environment defined by the use of electronic systems and the electromagnetic spectrum to store, modify, and exchange data through internet networks and their associated infrastructure⁽⁶⁾.

2- Cyber Threats: These are attacks and risks carried out using the mechanisms and networks of the Internet and computers, aimed at damaging information systems and electronic networks connected to the Internet. The nature of these threats varies from one country to another, depending on its level of technological development⁽⁷⁾.

3- Cybercrime: This refers to illegal activities conducted using electronic devices, where the digital offender gains material or moral benefits. These crimes are typically carried out through hacking or breaching information systems⁽⁸⁾.

4- Cyber Deterrence: This refers to preventing harmful actions against national assets in cyberspace and the assets that support cyberspace operations. It is based on three key pillars in the defense field: the credibility of defense, the availability of backup information systems, and the ability to respond effectively⁽⁹⁾.

5- Cyber Attack: These are actions taken by a state to target the enemy's information systems in order to disrupt or influence them, while also defending the attacking state's own information systems⁽¹⁰⁾.

C) Dimensions of Cybersecurity

Cybersecurity has become a crucial component of national security policies, as it is interconnected with various fields. As a result, countries strive to enhance their security systems to keep pace with the rapid technological advancements in communication and media while addressing potential cyber threats. Cybersecurity encompasses several dimensions, including:

1- The Legal Dimension: Technological advancements in society require corresponding updates in legal frameworks. This is achieved by establishing laws to define legal and illegal actions. However, there is generally a gap in the legal system governing cybercrimes. This deficiency may be attributed to the nature of these crimes, the difficulty in identifying their perpetrators, and their ability to transcend national borders⁽¹¹⁾.

2- The Economic Dimension: This is considered one of the most crucial aspects of cybersecurity, as many state institutions and companies rely heavily on digital systems. Governments must implement all necessary measures to protect their data, information, applications, and users from economic crimes that cross national borders, such as money laundering, piracy, tax evasion, and other illegal activities that impact national economies. The relationship between the economic dimension and cybersecurity is strong, as ensuring security fosters trust and ensures the continuity of economic institutions and businesses. This, in turn, supports the growth of digital trade and mitigates the negative effects of cybercrimes⁽¹²⁾.

3- The Social Dimension: Social networks, in particular, play a

significant role in allowing individuals to express their political goals and social aspirations in various ways. The involvement of all segments of society contributes to social development by providing opportunities to access information and share ideas. A society's openness to others also fosters the exchange of experiences and ideas, laying the foundation for cooperation and integration⁽¹³⁾.

4- The military dimension: highlights the significant advantage of cyber power in connecting military units through networks in cyberspace. This capability facilitates the seamless exchange and flow of information, enhances speed in issuing military orders, and enables remote targeting and destruction of objectives. However, if the electronic networks employed for these purposes are not adequately secured, this strength could become a vulnerability. Such networks may be susceptible to hacking, potentially undermining the state's ability to rapidly deploy its resources and forces⁽¹⁴⁾.

Second Subtitle: Understanding the concept of cybercrimes

The widespread use of modern information and communication technology in the digital age has led to a rise in cybercrimes, also known as information crimes. Therefore, in the first section, we will explore the definition of cybercrime. The characteristics of cybercrime will be discussed in the second section, while the third section will focus on the elements of cybercrime

A) Definition of Cybercrime

Cybercrime has been defined in various ways, but these definitions are not confined to specific actions. This is largely due to the rapid and ongoing advancements in technology, which have made it challenging to establish a single, universally accepted definition

1- The Legislative Definition of Cybercrime

According to Article 2 of Law No. 09/04, which outlines specific rules for preventing and combating crimes associated with information and communication technologies, cybercrimes are defined as "offenses that impact automated data processing systems specified in the Penal Code, as well as any other crimes committed or facilitated through the use of an information system or electronic communications system⁽¹⁵⁾."

The Algerian legislator used the term crimes related to information and communication technologies to refer to electronic or information crime.

At the International Level, the Organization for Economic Co-



operation and Development (OECD) defines cybercrime as any action or omission that could harm material or moral property, either directly or indirectly, through the use of information technology. Similarly, during the Tenth United Nations Congress on the Prevention of Crime and the Punishment of Offenders in 2006, cybercrime was defined as “any offense that can be carried out using a computer system or network, or within a computer system.” This definition broadly encompasses all crimes that can occur in an electronic environment⁽¹⁶⁾.

2-The jurisprudential definition of cybercrime

Jurisprudence has differed in finding a unified definition of cybercrime. This is due to the standard adopted by each jurist in defining it. Among the most important jurisprudential definitions we find:

It refers to any attack on individuals, property, or private or public rights through the use of modern electronic computers, targeting cyber systems, networks, data, or electronic applications⁽¹⁷⁾.

It refers to any action or failure to act by an individual that damages computer components or communication networks protected under the Penal Code, which prescribes penalties for such attacks⁽¹⁸⁾.

It is any criminal activity in which electronic technology is used directly or indirectly as a means to carry out the targeted criminal act⁽¹⁹⁾.

B) Characteristics of Cybercrime

Cybercrime is distinguished from traditional crime by several characteristics, whether related to the perpetrator, the environment in which the crime was committed, or the means used when committing the crime. Among the most important distinguishing characteristics of cybercrime, we mention:

1-Global: Cybercrime surpasses national borders, making it a transcontinental crime⁽²⁰⁾. It is classified as a non-national crime due to the electronic environment in which it occurs. This environment relies on electronic connections between computers, whether within a single country or across multiple countries, through electronic networks such as the Internet⁽²¹⁾.

2-A New Type of Crime: Cybercrime is one of the most prominent emerging forms of crime, posing significant risks in the era of globalization.⁽²²⁾ It leverages advancements in modern technology,



scientific methods, and technical innovation throughout all stages of planning, preparation, and execution.⁽²³⁾

3-Difficulty of Proof: A key characteristic of cybercrimes is their difficulty to detect and prove compared with traditional crimes. Often referred to as hidden crimes, they are committed in secrecy, making it challenging to apprehend the perpetrators. Additionally, these offenders are typically highly intelligent and skilled professionals⁽²⁴⁾.

4-The Perpetrator's privacy: Unlike traditional crimes, which are generally not influenced by the offender's level of education, cybercrimes are fundamentally different. Cybercriminals are typically specialized and possess significant knowledge in the field of information technology⁽²⁵⁾.

C) Elements of Electronic Crimes

Cybercrime is based on three pillars. It differs from traditional crimes only in its location. The pillars of cybercrime are:

1- The material element

The material element of a cybercrime comprises the criminal act, the outcome, and the causal link between them. Notably, the material element can exist even if the intended result is not achieved, such as when the crime is reported before its consequences materialize. In cybercrime, the material element varies depending on the specific positive act committed. For example, in the case of electronic espionage, directly obtaining the electronic medium containing the confidential information or secrets constitutes the material element of the crime⁽²⁶⁾.

2- The Moral Aspect

The moral element of cybercrime is generally tied to the psychological state of the perpetrator. It encompasses the presence of criminal intent, where the offender is fully aware of all elements of the crime they are committing. The perpetrator understands that their actions target an automated data processing system, including the information and programs it contains, recognizing these as subjects of a legally protected right⁽²⁷⁾.

3- The Legal Pillar

The legal pillar refers to the legislator's acknowledgment and explicit provision for the criminalization of a specific act, based on the principle that no crime or punishment exists without legal text. The Algerian legislator established a dedicated section in the Penal Code

under Chapter Three, Section Seven Bis, addressing felonies and misdemeanors against property. This section specifically focuses on crimes involving tampering with automated data processing systems⁽²⁸⁾.

Chapter II: Mechanisms for Combating Cybercrime:

Cybercrime is a global threat that transcends continents and borders. It can be carried out by anyone with sufficient expertise in planning and executing such crimes, even while remaining physically distant and avoiding direct surveillance or prosecution. The rapid evolution and innovation of cybercrime patterns have made it increasingly difficult to track and combat locally and internationally.

In this section, we will try to address the international mechanisms for combating cybercrimes in the first section, then the national mechanisms for combating cybercrimes in the second section.

First Subtitle: Mechanisms for Combating Cybercrime through International Instruments

Numerous international agreements have been established to address the issue of cybercrime. These agreements focus on combating cybercrimes and the development of information systems and technologies. Recognizing the threat posed by cybercrime, many countries have signed international treaties and conventions. Cybercrime is a borderless issue, where the perpetrator may reside in one country while the harm occurs in another one and a third country may be involved as a service provider or the host of the site from which the crime originates. This raises complex challenges in applying criminal law across borders.

Therefore, in this section, we will examine the key international instruments and frameworks that address the issue of combating cybercrime.

A) Mechanisms for Combating Cybercrime in United Nations Resolutions

The United Nations addressed computer crimes in its resolution during the Eighth Havana Congress in 1990, focused on the Prevention of Crime and the Treatment of Prisoners. This decision reflected the efforts of the United Nations and called on member countries to intensify their efforts to combat the misuse of computer devices. It urged nations to criminalize actions related to cybercrime and to strengthen measures against these offenses⁽²⁹⁾.

Through which it requested countries to take the following

measures⁽³⁰⁾:

-A review of penalties, current laws, investigative authorities, and judicial procedures is necessary to ensure their applicability to modern cybercrimes. This may require changes to existing laws when needed. The text regarding crimes, penalties, investigations, and evidence should be updated to address the new and complex nature of cybercriminal activities. The absence of suitable laws to cover these evolving crimes calls for urgent action. Additionally, the United Nations encourages member countries to intensify their efforts in combating computer-related crimes and to participate in treaties related to this issue.

-The decision encourages member countries to focus on improving their legislation related to the delivery of criminals and the exchange of assistance in criminal matters. It emphasizes the need for countries to ensure that their legal frameworks apply to all forms of new crimes, such as cybercrimes, and to take specific steps to enhance investigations in this area. The goal is to strengthen international cooperation and effectively address these evolving criminal activities.

This also includes the vision regarding information crime in general, which requires continuous development or to develop the following⁽³¹⁾:

- International Criteria for Data Security Treatment Mechanisms.*
- Take appropriate measures to address the judicial challenges posed by cybercrimes, which transcend borders or share similar international characteristics.*
- International agreements involve texts that organize and regulate procedures, as well as adjust to the realities of cross-border issues related to information systems. These agreements also include various forms of mutual assistance, ensuring the protection of individuals' rights and freedoms, while safeguarding the sovereignty of states.*

b) Mechanisms for Combating Cybercrimes in the Decisions and Recommendations of the International Criminal Law Commission

This committee held its 15th conference in 1994 in Brazil, where it outlined the illegal acts that fall within the scope of cybercrimes. These include fraud, computer damage, data deletion, and actions related to information technology forgery. The scope also covers damage to and deletion of programs and data, disabling computer operations and communication systems (networks), and unauthorized access that violates security protocols.

Regarding the procedural aspect, the decision made during the 15th International Conference of the International Association for Penal Law includes rules for the procedural environment of cybercrimes. These rules emphasize conducting inspections and adjustments in the information technology environment, as well as inspecting automated computer networks. The decision also highlights the importance of effective cooperation between victims, witnesses, and other parties involved. It stresses the need for the availability of information for judicial purposes, the regulation of communication within automated computer systems, and the practice of oversight and control over such systems⁽³²⁾.

C) Mechanisms for Combating Cybercrimes in International Agreements

Two agreements have been concluded in this regard: the first is the Berne Convention for the Protection of Literary and Artistic Works, and the second is the Budapest Convention on Combating Cybercrime, established in 2001. Additionally, there is an Arabic convention aimed at combating information technology crimes.

1- Mechanisms for combating Electronic Crimes in "Bern" agreement related to the protection of literary, artistic works and technical classifications

With the aim of protecting authors' rights over their literary works more effectively, the "Berne" Agreement was initially concluded on September 9, 1886. It was later supplemented in Paris in 1896, modified in Berlin on September 13, 1908, supplemented again in Bern on March 20, 1914, and modified in Brome in June 1928. Further modifications occurred in Brussels in 1948, Stockholm in July 1967, and Paris in July 1971. The countries that are parties to this agreement form a union to protect the rights of authors over their literary and artistic works. According to the "Berne" Agreement, automated computer software, regardless of whether it is in source or in machine language, is also protected as literary work⁽³³⁾.

Referring to Article 2, paragraph 1 of this agreement, the phrase "literary and artistic works" encompasses all productions in the literary, scientific, and artistic fields, regardless of the method or form of expression. This includes works such as books, brochures, lectures, and other written materials, which are listed as examples, not limitations. Therefore, digital works resulting from rapid technological

advancements are also covered under this scope. However, this does not eliminate the need for additional agreements and treaties to regulate these developments. This necessity led to the creation of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), as well as the efforts of the World Intellectual Property Organization (WIPO). Notably, the WIPO Copyright Treaty and the Internet Treaty have played a significant role in the protection of computer software⁽³⁴⁾.

Therefore, the Berne Convention has a positive impact on the development of cybersecurity by safeguarding copyright and promoting international cooperation in the fight against cybercrimes that target protected content.

2- Mechanisms for Combating Electronic Crimes in the Budapest Agreement related to combating cybercrimes and establishing procedures for international cooperation in addressing these crimes.

Recognizing the seriousness of cybercrimes as transnational offenses, many countries sought to sign the Budapest Convention. The agreement was adopted in the Hungarian capital, Budapest, with thirty nations initially signing, including EU member states, Canada, Japan, South Africa, and the United States. The purpose of this agreement was to address the challenges posed by international cybercrimes, transcending national borders to facilitate collaboration among nations in combating these crimes. The agreement aims to assist countries in fighting cybercrimes, tracking offenders, enabling prosecution, and apprehending perpetrators. It also outlines the best practices for investigations into internet-based crimes. Signatory countries committed to close cooperation to counter these offenses.

The Budapest Convention provides substantive criminal law provisions, defining various types of cybercrimes, including terrorism, credit card fraud, copyright infringement, and others. It is regarded as one of the most comprehensive efforts to coordinate new legal frameworks across multiple countries to combat the illegal use of information networks. Notably, the agreement resulted from extensive consultations among governments, law enforcement agencies, and the computer industry, with input from legal experts under the Council of Europe, supported by other nations⁽³⁵⁾.

The agreement comprises 48 articles divided into four sections:

- First Section: Definitions and use of terminology.



- **Second Section:** Measures to be implemented at the national level.
- **Third Section:** Judicial processes and international cooperation.
- **Fourth Section:** Final provisions.

3- Mechanisms for Combating Cybercrimes in the Arab Convention on Combating Information Technology Crimes

The agreement aims to strengthen and support cooperation among Arab countries in combating information technology crimes. It seeks to mitigate the dangers posed by these crimes to protect the security of Arab nations, safeguard their interests, and ensure the safety of their societies and citizens⁽³⁶⁾.

It can be concluded from this agreement that, in addition to the electronic crimes covered by international conventions related to computers and communication systems, it also addresses several crimes related to pornography for instance: Article 12 states that any activity aimed at producing pornography is considered a crime. This includes offering, distributing, providing, publishing, buying, selling, or importing pornographic materials or materials that violate public decency using information technology. Similarly, Article 13 includes crimes related to pornography, such as those associated with gambling and sexual exploitation⁽³⁷⁾.

The agreement calls for stricter punishments for crimes related to child pornography, including emphasizing the possession of child pornography materials and other indecent materials involving children, particularly those stored or distributed using information technology or electronic media. Regarding the scope of application, the convention requires the States Parties to adopt internal legislation and necessary procedures to establish powers and processes as outlined in Chapter Three of the agreement⁽³⁸⁾.

As for legal and judicial cooperation Article 30 of the agreement requires all member states to implement necessary measures to address crimes outlined in Chapter II of the agreement. These measures apply when a crime occurs entirely or partially within the territory of a member state on a vessel or aircraft registered under a member state's laws by a citizen of a member state or if it took place outside the jurisdiction of any state⁽³⁹⁾.

National legislation also played a major role in combating cybercrimes, especially Arab legislation such as Algerian national legislation, and this will be discussed in the next section.



Second Subtitle: National mechanisms to combat cybercrime

Similar to international legislation, Algeria has made significant efforts to combat cybercrime, recognizing cybersecurity as a key pillar in protecting networks and digital systems from cyber threats. To address these risks, the Algerian legislator has issued various legal texts aimed at strengthening cybersecurity. The legislator's strategy for tackling the phenomenon of cybercrime has led to the enactment of several laws, the most prominent are:

The Penal Code, which has been amended multiple times, along with Law No. 18-07 on the protection of individuals in the processing of personal data and Law No. 18-05 on electronic commerce, will be discussed in the following sections.

A) Penal Law:

To address the rapid technological advancements and the growing challenges posed by digital crimes, the Algerian legislator has introduced numerous amendments to the Penal Code. These amendments aim to fill the legal void in the realm of cybercrime and adapt to societal changes.

One of the most notable amendments is Law No. 04-15, which introduced a dedicated section titled "Crimes Related to Automated Data Processing Systems." This section outlines a set of legal provisions that define actions considered violations and specifies the corresponding penalties⁽⁴⁰⁾.

Some of the key crimes related to automated data processing systems, as stipulated in the Penal Code, include:

-Crime of Unauthorized Access or Entry: This crime occurs when someone gains access to a system without authorization. This crime also includes cases where an individual fraudulently remains in all or part of an information system or attempts to gain such access.

-Crime of Information Forgery: This crime involves the act of falsifying or altering information within a system.

-Crime of Data Theft: This crime involves the unlawful theft or unauthorized acquisition of data.

-Crime of Data Destruction and Damage: it involves the unlawful destruction or alteration of data, causing harm to the system or information.

- Cyber Fraud Crime⁽⁴¹⁾.

To strengthen penalties for cybercrimes, the Algerian legislator

introduced new amendments through Law No. 06-23, related to protection of individuals and institutions from cyber threats while raising awareness about the seriousness of such crimes. Additionally, to align national legislation with emerging forms of crime and enhance cybersecurity efforts, the legislator enacted Law No. 24-06. This law includes provisions that impose strict penalties for offenses committed using information and communication technology.

b) Combating Electronic Crimes Under Law No. 18-07

Law No. 18-07 establishes general provisions aimed at protecting natural persons in the context of processing personal data, ensuring respect for human dignity, privacy, and fundamental freedoms. The law emphasizes safeguarding individuals' rights, honor, and reputation⁽⁴²⁾ in alignment with the principles of the Algerian Constitution, which upholds the rule of law.

According to the law, personal data may only be processed with the explicit consent of the individual, who retains the right to withdraw consent at any time. Exceptions to this rule are outlined in Article 06 of the law, which permits the processing of personal data by a natural person for purposes limited to personal or family use, provided the data is not shared with or disclosed to others⁽⁴³⁾.

To ensure protection mechanisms aligned with international legislation, the Algerian legislator addressed key issues in Article 03 of Law No. 18-07. This article clarifies various definitions related to technology and legal concepts, recognizing the necessity of precisely defining these terms for their effective application in the law. Additionally, the Algerian legislator, similar to comparative legislation, permits the processing of personal data as a general principle, except in cases where exceptions are explicitly provided. Certain types of data, particularly sensitive data, are excluded from processing due to their nature and the level of risks associated with their handling. These measures aim to safeguard the rights and fundamental freedoms of individuals while balancing the state's responsibility to fulfill its duties in the public interest⁽⁴⁴⁾.

Therefore, the Personal Data Protection Law reflects the state's commitment to protecting individuals' rights in the digital space. This law is also considered a fundamental tool in strengthening cybersecurity and combating electronic crimes.



C) Combating Electronic Crimes Under Law No. 18-05

The growing interest in electronic commerce and the widespread use of the internet globally have significantly contributed to the digital economy, generating substantial profits for many advanced countries and global companies active in this field. One of the defining features of the digital economy, particularly electronic commerce, is the shift from a supply-centred approach to a demand-driven model. This shift prioritizes operational processes and anticipates customer needs, allowing companies to tailor their offerings to meet demand effectively.

This flexibility and abundance in the variety of available products and services are key characteristics of the digital economy, however, despite its advantages and the expanding scope of e-commerce worldwide, certain challenges, including rare occurrences of specific demands, persist⁽⁴⁵⁾.

There are various definitions of electronic commerce. The Algerian legislator, in Article 06 of Law No. 18-05 dated May 10, 2018, defines it as: "An activity through which an electronic supplier offers or ensures the delivery of goods and services remotely to an electronic consumer using electronic communication methods⁽⁴⁶⁾."

Regarding the mechanisms for combating e-commerce crimes, the Algerian legislator has established various measures to protect electronic consumers. These mechanisms aim to address all forms of crimes that may be committed against them, including:

Protecting the Electronic Consumer from Misleading Advertising While Law No. 18-05 does not explicitly address misleading advertising in e-commerce, the Algerian legislator has established several conditions in Chapter VII that electronic suppliers must follow when conducting electronic advertising. Among these provisions is Article 22, which states: "Without prejudice to the legislative and regulatory provisions in force in this field, any advertising, promotion, or message of a commercial nature or purpose carried out through electronic communications must meet the following requirements: ⁽⁴⁷⁾"

- It must be clearly identified as a commercial or advertising message.*
- to allow identification of the person for whom the message was designed.*
- It must not violate public morals or public order.*
- It must clearly specify whether the business purpose includes a*

discount, rewards, or gifts in the event of a purchase, and whether the offer is commercial, competitive, or promotional.

- to ensure that all conditions required to benefit from the commercial offer are clear, not misleading, and not ambiguous.

Regarding the protection of electronic consumers from arbitrary terms, the Algerian legislator did not explicitly address arbitrary conditions in Law No. 18-05 on electronic commerce. However, it referred to the application of relevant legislation and regulations concerning commercial practices and consumer protection in the first chapter of the third section. Specifically, Article 29 of Law No. 04-02, which governs commercial practices, prohibits arbitrary conditions, and these provisions can also be applied to electronic commercial practices⁽⁴⁸⁾.

This law also mandates that the electronic supplier ensure the security of information systems and maintain the confidentiality of data. It further stipulates that only the data necessary to complete electronic commercial transactions should be collected⁽⁴⁹⁾. Therefore, it is required to take all appropriate security measures to protect systems from cyber threats and attacks.

Conclusion:

As a result of the discussion, it is evident that cybercrimes have reached a level of severity that has prompted the international community to take significant action to combat them and put an end to their spread. These crimes have become a serious threat to global peace and cybersecurity. In light of this, we propose several suggestions that could support the efforts of both international and national legislators in combating cybercrimes:

- The Algerian national legislator must ratify the United Nations agreements and recommendations related to combating cybercrimes, considering the advanced and effective mechanisms they offer in this area.

- The national government should work to join international committees focused on combating cybercrimes in order to enhance its cybersecurity efforts.

- Efforts should be made to raise awareness and promote electronic consumer culture among both consumers and suppliers by organizing training courses, strengthening the role of consumer protection associations, and involving civil society institutions in this area.

Additionally, electronic commerce should be included in school curricula.

- National legislation should be adapted to keep pace with the continuous advancements in information and communication technologies.

- There is a need for more punitive and procedural legislation to address these increasingly dangerous crimes, along with stronger controls to confront them.

- Penalties for cybercrime perpetrators should be tightened.

- Support should be provided for innovation and scientific research in cybersecurity, particularly to confront advanced and rapidly evolving threats. Investment in the development of new techniques and tools for detecting and preventing cybercrimes should also be prioritized.

- Awareness campaigns about cyber threats should be conducted through various media platforms, including social media.

Referrals and References:

⁽¹⁾- Bouazdia Djamel, *Algerian Strategy in the face of cybercrime "Challenges and future prospects"*, Journal of Legal Political Sciences, university Algeria 3, Volume 10, number 01, April 2019, P.1267.

⁽²⁾- Regulation UE 2019/881 European Parliament and Council on 17 April 2019 comply with ENISA the European Union agency for cybersecurity and on information and communications technology cybersecurity certification and repealing regulation UE n° 526/2013 cybersecurity Act, JO, n° L151/15 du 06/07/2019.

⁽³⁾- Article 10, Paragraph 03 of Law No. 18-04, *Included rules general related by mail and communications electronic*, dated May 10, 2018, published in the Algerian Official Journal, No. 27, dated May 13, 2018.

⁽⁴⁾- Guettaf Slimane, Bougrine abd el halim, *Objective and procedural Mechanisms used to achieve cyber Security Algeria as a model*, Governance Journal and Economic Law, university of Batna 1, Algeria, Volume 03, Number 02, July 2023, P.82.

⁽⁵⁾- Katarzna Chatubinska, Jentkiewicz and Others, *Cybersecurity in Poland: Legal Aspects*, Springer Nature, Switzerland, 2022, P.30.

⁽⁶⁾- Iman abd el kader, *The impact of cyberspace on Arab national security during the period from 2011 to 2023*, National Security and Strategy, academy Military For studies The Supreme and strategy, Egypt, Volume 02, Number 03, January 2024, P.107.

⁽⁷⁾- Abd allah Jaafari, *Cyber Threats and their impact on Algerian National Security*, African Journal of Legal and political studies, university of Adrar, Algeria, Volume 06, Number 02, December 2022, P.247.

⁽⁸⁾- Kadri Nour el Houda, *Cybercrime and mechanisms combat it-Facing cyber security Challenges -*, Algerian Journal of Law political Sciences, university of Sidi Bel Abbas, Algeria, Volume 08, Number 01, June 2023, P.04.

⁽⁹⁾- Guettaf Slimane, Bougrine abd el halim, *Cybersecurity and its related Conceptual implications*, TOBNA Journal For Academic scientific studies, university center Si EL-Hawas, Batna, Algeria, Volume 05, Number 02, August 2022, P.48.

⁽¹⁰⁾- Sediki Samia, *International responsibility for the cyber attack in the perspective of international law*, Journal of Legal and Economic Research, university of Aflou, Algeria, Volume 06, Number 01, January 2023, P.823.

⁽¹¹⁾- Idris Atia, *The Status of Cybersecurity in Algeria's National Security System*, Misdakia Journal, Higher Military School of information and communication, Algeria, Volume 01, Number 01, September 2019, P.106.

⁽¹²⁾- Salah el Chahat abd el Latif el Zaouaoui, *Security Cyber And its application on data theft study Jurisprudence comparison*, Egyptian house "El Iftaa" Journal, Egypt, Volume 16, Number 58, July 2024, P.195.

⁽¹³⁾- Guettaf Slimane, Bougrine abd el halim, *the patient Mechanisms Objectivity And procedural Followed To achieve Security Cyber Algeria Model*, Op.cit, P.84.

⁽¹⁴⁾- Idris Atia, Op.cit, P. 105.

⁽¹⁵⁾- Article 02 of law No.09/04 Included Private Rules For preventing and combating Crimes related to communication technologies and Media, dated August 05, 2009, published in the Algerian Official Journal, No. 47, dated August 16, 2009.

⁽¹⁶⁾- Ben malek Ismahan, *Characteristics of the information crime and the reasons for its commission*, El-Biban Journal of Legal and political Studie, university of Bordj Bou Arreridj, Algeria, Volume 04, Number 01, June 2019, P.104.

⁽¹⁷⁾- Salah el Chahat abd el Latif el Zaouaoui, Op.cit, P.233.

⁽¹⁸⁾- Derrar abd el Hadi, *Mechanisms to fight digital crime in Algerian legislation*, Modern Journal of Legal studies, university Ram Allah, Palestine, Volume 01, Number 02, 2023, P.250.

⁽¹⁹⁾- Ben alia Ben djedou, *Cybersecurity Challenges To face cybercrime*, Algerian Review of Human Security, university of Batna 1, Algeria, Volume 07, Number 02, March 2022, P.304.

⁽²⁰⁾- Tala Lamia, kahina salam, *Cybercrime: a new dimension to the concept of crime Across social media platforms*, Erriwak Journal of Social and Human Studies, university of Ghilizan, Volume 06, Number 02, December 2020, P.75.

⁽²¹⁾- Ben malek Ismahan, Op.cit, P.116.

⁽²²⁾- Mahdaoui Hanane, *Legal regulation of cybercrime in Algerian legislation*, Journal of Legal and Political Thought, university of setif, Algeria, Volume 06, Number 02, 2022, P.1063.

⁽²³⁾- Balaid Ilhem, *New Crimes*, EL BAHITH for Academic Studies, university of Batna 01, Algeria, Volume 09, Number 02, June 2022, P.519

⁽²⁴⁾- Ben malek Ismahan, Op.cit, P.114.

⁽²⁵⁾- Mahdaoui Hanane, Op.cit, P.1063.

⁽²⁶⁾- Derrar Abd el hadi, Op.cit, P.257.

⁽²⁷⁾- Bader eddine khellaf, *Legal Regulation of Cyber-Crime in Algeria*, Journal of legal and social studies, university of kenchla, Algeria, Volume 06, Number 02, 2021, P.337.

⁽²⁸⁾- Tala Lamia, kahina salam, Op.cit, P.69.



- (29)- Abd el fatah Mourad, to explain Crimes Computer and the Internet, without house to publish, P.382.
- (30)- Ibid, P.237.
- (31)- Abd el fatah byoumi Hijazi, Proof Criminal in Crimes Computer And the Internet, house Books Legal, 2007, P.190.
- (32)- Abd el fatah Mourad, Op.cit, P.280.
- (33)- Mohammed Abdou Allah about baker salama, encyclopedia Crimes Informatics "Crimes Computer and the Internet", The office Arabic Hadith Alexandria, 2006, P.14.
- (34)- Yasrefhadj, Legal Protection of Computer programs According to author's rights rules, Human Sciences Journal, University of Oran, Volume 5, Number 2, 2015, P.275.
- (35)- The Budapest convention on Cybercrime, Council of Europe, European Treaty Series, opened for signature 23 november 2001, Entered into force 01 July 2004, N°.185.
- (36)- Presidential Decree No.14-252, dated September 8, 2014, Including the ratification of the arab convontion to combat the crimes of information technology, Issued in Cairo on 21-12-2010, published in the Algerian Official Journal, No. 57, dated September 28, 2014.
- (37)- Articles 12 and 13 of Presidential Decree No.14-252, Ibid.
- (38)- Article 13 of Presidential Decree No.14-252, Ibid.
- (39)- Article 30 of Presidential Decree No.14-252, Ibid.
- (40)- Law No. 04-15, dated November 10, 2004, amending and supplementing Ordinance No. 66-156 concerning the Penal Code, published in the Algerian Official Journal, No. 71, dated November 10, 2004.
- (41)- Ben Alia Ben djedou, Op.cit, P.314.
- (42)- Articles 1 and 2 of law No. 18-07 Related to protection of natural persons in field of processing personal Data, dated June 10, 2018, published in the Algerian Official Journal, No. 44, dated June 10, 2018.
- (43)- Zergini Radia, Protection Penal For data Character, thesis PhD, specialty law general, college rights, university The valley, Algeria, 2021-2022, P.03.
- (44)- Ibid, P.15.
- (45)- Atik Ali, Combating E-Commerce Risks in Algeria, An article published on the Al-Mizan website <https://www.elmizaine.com/2021/03/blog-post-21.html#google-vignette>, Consulted on 25/12/2024 at 11: 35
- (46)- Article 6 of Law No 18-05 on e-commerce, dated May 05, 2018, published in the Algerian Official Journal, No. 28, dated May 16, 2018.
- (47)- Article 22 of Law No 18-05, Ibid.
- (48)- Article 29 of Law No 18-05, Ibid.
- (49)- Article 26 of Law No 18-05, Ibid.