LEGAL CRIMINAL MECHANISMS FOR COMBATING CYBERCRIME IN ALGERIAN LEGISLATION

Dr. LAIDANI SIHAM[1],Dr. SLIMANI SAFIA[2]

[1]Institute of Law and Political Science, El-BayadhUniversity Center, Algeria

[2]Faculty of Law and Political Science, Department of Law, Ziane Achour University of Djelfa, Algeria

Received: 09/08/2024;Accepted:27/11/2024; Published: 16/01/2025

ABSTRACT

Recently, with technological advancements and the massive media revolution, numerous cybercrimes have emerged, such as hacking, involving various forms of attacks on electronic data. The impact of cybercrime has extended to organized crime and other offenses. To curb this phenomenon, international and regional efforts have been coordinated to combat it. Our focus here is on the criminal legal mechanisms provided by the Algerian legislator to combat cybercrime.

Keywords: *Cybercrime - Organized crime - Electronic data - Criminal protection - Hacking.*

This raises the following question:

To what extent are the criminal legal mechanisms effective in combating cybercrime in Algerian penal legislation?

INTRODUCTION

Cybercrime is among the offenses resulting from the misuse of the information and communication technology revolution. It is committed using modern technologies and has become a pressing issue at both the national and international levels, necessitating effective legal provisions from the criminal legislator to combat and deter it.

Rapid urbanization and the availability of opportunities for committing cybercrimes have contributed to their prevalence, alongside an increasing number of victims and insufficient measures to counter them. Various international and regional efforts have been made to combat cybercrime. Algeria, like other countries, is not immune to these crimes and their consequences. Social media platforms, in particular, have been targets of hacking, extortion, and defamation.

Given this grave situation, it became imperative for the Algerian legislator to intervene with practical legal mechanisms to curb the spread of this phenomenon. Among these mechanisms are the criminal legal measures designed to combat cybercrime in Algeria.

The key question remains:

How effective are the criminal legal mechanisms in combating cybercrime in Algeria?

Chapter One: The Conceptual and Substantive Framework of Cybercrime

Cybercrime is considered one of the complex crimes that are difficult to detect due to the involvement of information technologies. In light of the inadequacy of traditional mechanisms to combat cybercrime, it became necessary for the Algerian legislator to intervene with mandatory legal provisions to criminalize this phenomenon. To understand the substantive rules governing this crime, we address the following:

Section One: Definition of Cybercrime and Its Legal Nature

1. Definition of Cybercrime:

Cybercrime is the deliberate commission of a socially harmful or serious act prohibited and punishable by law. It encompasses a range of illegal actions conducted using electronic devices, equipment, or the internet, or disseminated through its content. These crimes require specialized knowledge of computer technologies and information systems to commit, investigate, or prosecute their perpetrators. [1]

2. The Legal Nature of Cybercrime:

The distinct nature of these crimes lies in the ability of information networks to simultaneously transmit and exchange personal data, facilitating the commission of the act. This is largely due to the expansion of various types of information databases. The challenge of categorizing these crimes stems from their unique nature, as traditional legal rules were not designed for these newly emerging criminal phenomena. Consequently, applying these traditional rules to such crimes raises numerous issues, including those related to evidence and tracking the offenders. Thus, it can be concluded that cybercrime possesses a unique legal nature.[2]

Section Two: Characteristics and Elements of Cybercrime

1. Characteristics of Cybercrime:

Cybercrime is characterized by several unique features, as follows:

- It leaves no tangible traces after its commission.
- Even if traces exist, it is technically challenging to preserve them.
- It requires specialized technical expertise, making it difficult for a traditional investigator to handle.
- Its execution relies on deception, misleading efforts to identify the perpetrators.
- It involves a high degree of intelligence in its commission. [3]
- Additional distinguishing features that set cybercrime apart from traditional crimes include:
- Cybercrimes are committed through the internet, which serves as a medium connecting all potential crime targets, such as banks and companies.
- These crimes are transnational in nature, as the informational society does not recognize geographical boundaries. It is an open society that operates through networks transcending time and space, which has created numerous issues related to jurisdiction, applicable laws, procedural challenges in judicial follow-ups, and other concerns typically associated with transboundary crimes. [4]
- Difficulty in proving cybercrime.
- High financial losses resulting from cybercrime.
- Underreporting of cybercrime incidents.

Elements of Cybercrime

Cybercrime is based on two pillars: the material element and the moral element. Therefore, cybercrime must include a material element embodied in an act that reflects the will of the perpetrator, and a moral element embodied in an act that reflects the will of the cybercriminal.

- **The Material Element of Cybercrime**

The material element is an act or omission that can be proven. This element varies depending on the classification of the act, and thus, cybercrime cannot be confined to a single characterization.

The material element of cybercrime consists of three components: criminal behavior, the outcome, and the causal relationship. It is worth noting that the material element can be established without the outcome occurring, such as reporting the crime before its result is achieved (e.g., creating a website to defame a specific person without publishing it online, yet the perpetrator must still be punished).

- **The Moral Element of Cybercrime**

The moral element of cybercrime consists of two components: knowledge and intent.

- **Knowledge:** The perpetrator's awareness of the circumstances.
- **Intent:** The direction of the criminal behavior towards achieving the outcome.

According to established principles in criminal law, criminal intent may be general or specific.

- **General Criminal Intent:** Refers to the direct aim of the criminal behavior, confined to committing the act itself.
- **Specific Criminal Intent:** Required in certain crimes but not others, it involves achieving the intended outcome.

General criminal intent is present in all cybercrimes, while specific criminal intent applies to certain crimes, such as defamation via the internet and spreading viruses through the network.

Section Three: Procedural Rules Governing Cybercrime

Amendments to the Code of Criminal Procedure have introduced several procedural rules to address cybercrime. The legislator has established specific procedures for these crimes, covering every stage from investigation and inquiry to trial. The particularity of cybercrime lies in the following:

Extension of Local Jurisdiction: The local jurisdiction of judicial police officers, investigating judges, and public prosecutors has been extended under Article 37 of the Code of Criminal Procedure for organized crimes and data-related offenses. The adoption of extended territorial jurisdiction represents an effective approach for addressing certain categories of serious organized crimes. Although it deviates from the original jurisdiction standards, which are based on the location of the crime, it serves as an effective means for tackling complex cybercrimes.

New Provisions in Law 09/04 (dated August 5, 2009): The Algerian legislator introduced specific provisions on jurisdiction in the field of information technology, aligning with the developments in cybercrime. For example, Article 3 outlines new measures required for investigations and inquiries, including technical arrangements.

Additionally, Article 15 of Law 09/04 stipulates:"In addition to the jurisdiction rules outlined in the Code of Criminal Procedure, Algerian courts have jurisdiction over crimes related to information and communication technologies committed outside the national territory when the perpetrator is a foreigner, and the crime targets Algerian state institutions, national defense, or the strategic interests of the national economy."

2. Special Investigation Methods:

The importance of the judicial police in uncovering cybercrimes and identifying cybercriminals has led the Algerian legislator to introduce specific procedures tailored to the new nature of criminality. These measures allow the judiciary and police to adapt to this evolving form of crime, drawing their legitimacy from international agreements ratified by Algeria, particularly Article 20 of the Palermo Convention on combating organized crime, which includes cybercrime. This method is authorized only for certain crimes, as stipulated in Article 14, such as intercepting communications conducted through wired and wireless means. [5]

- **Search and Seizure:**

Cybercrime differs from other crimes in its complexity and difficulty to prove. Therefore, the Algerian legislator permits searches of information systems for any crime that is likely to occur, reducing the usual safeguards required in other crimes due to the speed at which cybercrimes are committed and their transnational effects. [6]

Paragraph 4 of Article 47 of the Code of Criminal Procedure provides for the possibility of searching and seizing intangible computer components, stating:"If the crime involves data processing systems, the investigating judge may conduct any search or seizure operations, day or night, anywhere across the national territory or authorize a judicial police officer to do so."

- **Preventive Detention:**

One of the newly introduced measures to combat cybercrime in Algerian legislation is the extension of preventive detention by judicial police officers, as stipulated in Article 51, Paragraph 5 of Ordinance 15/02 dated July 23, 2015. This measure allows an officer to detain any person against whom strong evidence of committing a cybercrime exists. However, the duration of preventive detention must not exceed 48 hours, except in certain serious crimes for which the legislator has provided specific exceptions.

Chapter Two: Criminal Protection of Information Systems in Algerian Legislation

In this chapter, we address the aspects of the Algerian legislator's efforts to combat cybercrime by examining the role of intellectual property laws from a criminal perspective, as well as general criminal laws in combating cybercrime, as follows:

Section One: Criminal Protection of Information Systems Through Intellectual Property Laws

Cybercrime can be classified under violations of the moral rights of authors; in this context, it falls under the concept of "paternity rights." Among the moral rights granted to authors over their works is the right to ensure their work is respected and remains intact, as well as the right to oppose any modification or distortion made to it, especially if such changes affect their interests or reputation. Accordingly, we explore the protective measures provided under Algerian law regarding copyright.

By analyzing the provisions of Ordinance 97/10, amended and supplemented by Ordinance 03/05 on Copyright and Neighboring Rights, the following points can be deduced:

- The list of protected works has been expanded to include computer applications as original works under Article 4, referred to as databases and computer programs.

- The duration of protection is set between **25 years and 50 years** after the creator's death, aligning with the Berne Convention, which specifies a 50-year protection period. This duration also applies to computer-related works, as stipulated in Article 58 of Ordinance 03/05.

- **Increased penalties** for violating authors' rights, particularly those of creators of computer-related works, are stipulated under Article 153 of Ordinance 03/05.

- The **WIPO Copyright Treaty** of June 20, 1996, in Article 4, recognizes computer programs as literary works under Article 2 of the Berne Convention. This protection applies to computer programs regardless of their form or mode of expression.

- Article 5 adds that collections of data or other materials are protected as such, regardless of their form, if they are deemed artistic innovations due to their selection or arrangement. However, this protection does not extend to the data or materials themselves.

- Article 25 of Ordinance 03/05 stipulates:“The author has the right to demand the integrity of their work be respected and to object to any modification, distortion, or corruption that may harm their reputation as an author, their honor, or their legitimate interests.” [7]

- Articles 52 and 53 of the same law specify acts considered legitimate in the context of using works, such as reproduction, translation, adaptation, and modification. Any reproduction or use of a work outside these provisions constitutes counterfeiting, punishable by imprisonment and fines as outlined in Articles 151 to 153 of the same law.

- As outlined earlier, the law on copyright and neighboring rights provides criminal protection for computer-related works after explicitly incorporating them into the list of protected works. This aligns with the provisions of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) as part of efforts to join the World Trade Organization.

- Accordingly, computer programs fall under the umbrella of criminal protection afforded to copyright. This necessitates the examination of offenses related to the counterfeiting of computer-related works and the penalties prescribed for such acts.

Counterfeiting of Electronic Works:

The law in various legislations has criminalized infringements on the literary and artistic rights of authors. Crimes against authors' rights are referred to as counterfeiting offenses. The Algerian legislator, in Article 151 of the 2003 Copyright Law, states:"A person committing an act of counterfeiting is guilty of a misdemeanor."

A. Elements of the Crime of Counterfeiting

1. The Material Element:

According to Articles 151 to 155, the legislator has criminalized all infringements on the moral or material rights of authors. The Algerian legislator has classified several actions as counterfeiting, even if they are not technically or theoretically considered counterfeiting, including:

- **Unauthorized disclosure of a work:** For example, screening a film without the owner's permission or publishing a book in the press without the author's consent.
- **Presenting a work under a false name.**
- **Reproduction without the author's permission.**
- **Illegally communicating the work to the public.**
- **Importing or exporting counterfeit copies.**
- **Selling, renting, or generally distributing the work without permission.**
- **Refusing to pay the compensation due to the author.**

The law does not penalize attempted counterfeiting. [8]

B. The Moral Element:

The occurrence of an infringement alone is not sufficient to establish the crime of counterfeiting. The presence of a moral element, represented by criminal intent, is required. This crime cannot be based on negligence or error.

Some legal scholars argue that the intent required for this crime is specific intent, where the perpetrator's aim is to harm the author.[9] However, the Algerian legislator does not require specific intent but suffices with general intent. This general intent consists of the perpetrator's awareness of their act, meaning their deliberate engagement in the material aspects of the crime with the intent to achieve the crime.

For instance, the perpetrator must know that the work is legally protected. If the perpetrator believes the work has entered the public domain, the crime is not established.

C. Penalty for the Crime of Counterfeiting:

The Algerian legislator classified counterfeiting as a misdemeanor and prescribed penalties according to Article 153: imprisonment from 6 months to 3 years and a fine ranging from 500,000 DZD to 1,000,000 DZD. The legislator combined imprisonment with fines and did not allow the judge the discretion to impose only one of the two penalties. The legislator also adopted a recidivism system by doubling the penalty.

The Algerian legislator also stipulated complementary penalties, including the temporary closure of the establishment where the counterfeiting occurred for 6 months or permanent closure, confiscation of equipment, counterfeit items, and financial proceeds. The confiscated funds go to the author and not to the state, as stated in general rules. The court may also order the publication of the judgment as an additional penalty.

3. Crimes Related to Computers and Databases:

In addition to the general rules for criminalizing infringements on works, the Algerian legislator has established specific provisions for computer programs and databases in the general Penal Code. The Penal Code was amended in 2004, and Articles 394 bis 1 and 394 bis 2 criminalize the following acts:

- Fraudulent alteration of data in an automated data processing system.
- Fraudulent removal or modification of data.
- Designing, researching, assembling, providing, managing, or trafficking intellectual data processed or transmitted via an information system.
- Possessing, acquiring, disseminating, or using data obtained from the aforementioned crimes.

Moral Element:

The Algerian legislator established these crimes based on specific intent, namely committing the act fraudulently. However, regarding the possession and use of data obtained from the aforementioned crimes, these are based on general intent.

- **Penalty:**The legislator prescribed a penalty of imprisonment ranging from **6 months to 3 years** and a fine ranging from **500,000 DZD to 5,000,000 DZD.**

Section Two: Criminal Protection of Information Systems Under the Penal Code

1. Attacks on Information Systems:

The Algerian Penal Code, through its most recent amendment, supplemented Chapter Three of Part Two of Book Three of Ordinance 66/156 by adding Section Seven Bis under the title "Attacks on Automated Data Processing Systems." This section includes eight articles, from Article 394 bis to Article 394 bis 7. Additionally, Law 09/04, dated August 5, 2009, establishes specific rules for preventing and combating crimes related to information and communication technology.

Components of Automated Data Processing Systems:

An automated data processing system consists of both physical and intangible components that form the system, such as memory, software, data, and connecting devices. These components are not exhaustive, leaving room for new elements necessitated by technological advancements. [10]

Second: Elements of Crimes Against Information Systems

A. Material Element: Unauthorized Access and Presence in an Automated Data Processing System

This is stipulated in Article 2 of the International Convention on Cybercrime, as well as Article 394 bis of the Algerian Penal Code, which states:**"Anyone who fraudulently accesses or remains in all or part of an automated data processing system, or attempts to do so, shall be punished with imprisonment from 3 months to 1 year and a fine ranging from 50,000 DZD to 100,000 DZD. The penalty is doubled if the act results in the deletion or alteration of system data. If the acts mentioned above lead to the destruction of the system's operation, the penalty shall be imprisonment from 6 months to 2 years and a fine ranging from 50,000 DZD to 150,000 DZD."**

It is noteworthy that the legislator did not specify the means of access or the method by which the system is entered. Thus, the crime is established regardless of the means or method used to gain access, whether direct or indirect. [11]

The aggravated form of the punishment, as provided in Articles 394 bis 2 and 394 bis 3, states: **"The penalty shall be imprisonment from 6 months to 2 years and a fine ranging from 50,000 DZD to 150,000 DZD."**

From this, it can be concluded that there are two circumstances under which the penalty for unauthorized access and presence in the system is aggravated. These circumstances are linked by a causal relationship between the unauthorized access or presence and the harmful result, even if the latter was unintended.

Intentional Disruption of the Operation of an Automated Data Processing System:

This type of attack is addressed in Articles 5 and 8 of the International Convention on Cybercrime. However, the Algerian legislator did not include a specific provision for intentional disruption of the system's operation. Instead, it addressed attacks on the data within the system.

This can be attributed to the fact that the Algerian legislator, through Paragraph C of Article 2 of Law 09/04, considered that programs governing the operation of automated data processing systems fall under the category of informational data. [12]

Manifestations of Intentional Disruption of System Operation:

The intentional disruption of a system’s operation takes two forms:

First Act: Disruption or hindrance, which requires a positive act. The legislator does not require the disruption to occur through a specific means, whether by:

- Physical means, such as breaking the physical devices of the system or damaging a disk.
- Non-physical means, such as targeting the logical components of the system (e.g., programs and data) by employing techniques used in this field, like introducing a viral program, using timed logic bombs, or slowing down the system’s performance.

Second Act: Corruption, which occurs through any act that does not necessarily disable the automated data processing system but renders it unsuitable for proper use, resulting in outcomes different from those that should have been achieved.

B. Moral Element:

For the moral element to be established, the perpetrator's intent must be directed toward the act of unauthorized access or presence in the system, with the knowledge that they do not have the right to access or remain in the system.

Thus, the moral element is not present if the perpetrator's access was permitted or legitimate. When criminal intent, comprising both knowledge and intent, is established, the motive behind the access or presence does not affect the crime, even if the motive was to demonstrate skill or to challenge the system. [13]

3. Sanctions for Crimes Against Information Systems:

The International Convention on Cybercrime states in Article 13 that penalties for committing cybercrimes must be deterrent and include imprisonment. It also requires sanctions for legal entities based on the principle of corporate liability, as stated in Article 12 of the convention.

A. Sanctions for Natural Persons

- According to Article 394 bis of the Penal Code, the penalty for the crime of unauthorized access, presence, or fraud in its simplified form is imprisonment from **3 months to 1 year** and a fine ranging from **50,000 DZD to 100,000 DZD.**
- Aggravated penalties under Articles 394 bis 2 and 394 bis 3 include doubled penalties if these acts result in the deletion or alteration of system data. The penalty is imprisonment from **6 months to 2 years** and a fine ranging from **50,000 DZD to 150,000 DZD** if unauthorized access or presence leads to the destruction of the operating system.
- For the crime of intentional data manipulation, Article 398 bis 2 stipulates a penalty of imprisonment from **2 months to 3 years** and a fine ranging from **1,000,000 DZD to 5,000,000 DZD** for intentional or fraudulent manipulation of data within the system.

In addition to the primary penalties, the Algerian legislator has provided for **supplementary penalties** under Article 394 bis 6, including:

- **Confiscation:** This supplementary penalty involves seizing devices, software, and tools used in committing crimes against information systems, while respecting the rights of third parties acting in good faith.
- **Website Closure:** Closing websites that serve as the subject of crimes against information systems.
- **Closure of Premises:** Shutting down establishments or exploitation sites where crimes were committed, provided the owner was aware of the illegal activities. For example, closing an internet café where crimes were committed, contingent upon the owner's knowledge of these activities.

The penalties are further aggravated under Article 394 bis. [14]

B. Sanctions for Legal Entities:

It is worth noting that the Algerian legislator, in the amendment to the Penal Code under Article 18 bis of Law 04/15, addressed penalties applicable to legal entities.

CONCLUSION

Cybercrime is one of the most dangerous forms of crime. The Algerian legislator has taken steps to strengthen the legal system with various measures to prevent and combat cybercrime. However, it is essential to further enhance legal mechanisms to mitigate the risks posed by cybercrime. Among the proposed recommendations are the following:

- Establishing cooperative mechanisms between various stakeholders, including the government, civil society, and the private sector, as part of Algeria's strategic collaboration with academics and research institutions.
- Prioritizing the fight against cybercrime.
- Utilizing media outlets and social media platforms to raise awareness about the impact and risks of cybercrime across cultural, social, and political dimensions.
- Ensuring the involvement of mobile phone operators in awareness campaigns by dedicating spaces on their platforms to inform customers and subscribers about potential cyber threats

(preventive measures), securing their devices, and emphasizing the confidentiality of personal data.

- Creating and protecting unsecured information.
- Establishing specialized programs in higher education institutions focused on information security and cybercrime, including developing and updating graduate-level programs to align with the demands of the information society. These programs should aim to build expertise for future use and include courses on "Internet Ethics" within university curricula.

References

Books:

1. Abdel Fattah Mourad, Explanation of Computer and Internet Crimes, Dar Al-KutubwalWatha'iq, n.d.
2. Mohamed Zaki Abu Amer, Abdelkader Al-Qahwaji, Criminal Law, Special Section, Dar Al-Nahda Al-Arabiya, Cairo, 1993.
3. Paul Goldstein, Copyright Rights, Egyptian Association for Global Culture Publishing, 1st ed., 1990.
4. Omar Mohamed Abu Bakr bin Younes, Crimes Arising from Internet Use, n.d., Dar Al-Nahda Al-Arabiya, 2004.

Scientific Articles:

1. Naja Abbawi, Legal Issues in Criminalizing Attacks on Information Systems, Political and Legal Notebooks, Issue 16, Faculty of Law and Political Science, Mohamed Tahri University, Bechar, Algeria, January 2017.

Electronic Resources:

1. Mohamed Abdullah Al-Menshawi, Internet Crimes from a Legal and Sharia Perspective, International Association of Translators, website: www.wata.cc.

Theses and Dissertations:

1. Fatiha Ressa'a, Criminal Protection of Information on the Internet, Master's Thesis in Public Law, Faculty of Law and Political Science, Abou Bekr Belkaid University, Tlemcen, 2011-2012.
2. Noura Trashi, Combating Information Crimes, Master's Thesis in Criminal Law, Faculty of Law, University of Algiers 1, 2011-2012.

Legislation:

1. Ordinance 03-05 dated 23/07/2003 on Copyright and Neighboring Rights.
2. Algerian Copyright and Neighboring Rights Law of 2003.
3. Ordinance 66-156 dated 08/07/1966 containing the Penal Code, amended and supplemented, Official Gazette No. 49 of 1966.

ENDNOTES

[1]Abdel Fattah Mourad, Explanation of Computer and Internet Crimes, Dar Al-Kutub wal Watha'iq, n.d., p. 38.

[2]Mohamed Zaki Abu Amer & Abdelkader Al-Qahwaji, Criminal Law, Special Section, Dar Al-Nahda Al-Arabiya, Cairo, 1993, p. 9.

[3]Mohamed Abdullah Al-Menshawi, Internet Crimes from a Legal and Sharia Perspective, International Association of Translators, website: www.wata.cc.

[4]Fatiha Ressa'a, Criminal Protection of Information on the Internet, Master's Thesis in Public Law, Faculty of Law and Political Science, Abou Bekr Belkaid University, Tlemcen, 2011-2012, p. 43.

[5]Abdel Hakim Rasheed Touba, Information Technology Crimes, 1st ed., Dar Al-Mustaqbal for Publishing and Distribution, Amman, 2009, p. 39.

[6]Naja Abbawi, Legal Issues in Criminalizing Attacks on Information Systems, Political and Legal Notebooks, Issue 16, Faculty of Law and Political Science, Mohamed Tahri University, Bechar, Algeria, January 2017, p. 288.

[7]Article 25 of Ordinance 03-05 dated 23/07/2003 on Copyright and Neighboring Rights.

[8]Algerian Copyright and Neighboring Rights Law of 2003, previously cited reference.

[9]Paul Goldstein, Copyright Rights, Egyptian Association for Global Culture Publishing, 1st ed., 1990, p. 256.

[10]Omar Mohamed Abu Bakr bin Younes, Crimes Arising from Internet Use, n.d., Dar Al-Nahda Al-Arabiya, 2004, p. 192.

[11]Abdelkader Al-Qahwaji, previously cited reference, p. 121.

[12]Article 2 of Law 09/04, previously cited reference.

[13]Abdelkader Al-Qahwaji, previously cited reference, pp. 136-137.

[14]Noura Trashi, Combating Information Crimes, Master's Thesis in Criminal Law, Faculty of Law, University of Algiers 1, 2011-2012, p. 131