

THE SPECIFIC CHARACTERISTICS OF OFFENSES RELATED TO INFORMATION AND COMMUNICATION TECHNOLOGY

DR. ASMA KELANEMER

Lecturer at the University of Algiers 1

Criminal Sciences Research Laboratory - Criminal Justice Unit

Professional Email: a.kelanemer@univ-alger.dz

Received: 04/06/2024

Accepted: 08/11/2024

Published: 03/12/2024

Abstract:

This research aims to analyze the Algerian legislator's approach to eliminating crimes related to information and communication technology, and at the same time to highlight how Algeria is striving to establish an objective punitive legislative balance in order to combat these crimes in all their manifestations and means of committing them, and to compare it as much as possible with the rapid and dangerous development of this type of contemporary crime.

Keywords: *Information and communication technology, Objective judgments, Specificity of criminalization.*

INTRODUCTION

The contemporary world is undergoing a profound transformation, commonly referred to as the "Information Age," propelled by rapid technological advancements. These innovations have had a far-reaching impact on individuals and societies globally, reshaping various facets of life. However, this remarkable progress is not without its challenges, one of which is the rise of new forms of crime facilitated through information systems and electronic communication networks.

These crimes, which are closely tied to information and communication technologies (ICT), have become a pressing concern for numerous countries, as they represent some of the most perilous transnational offenses targeting not only informational systems but also individuals, assets, and national security.

The significance of this study stems from its timely relevance and the pivotal role that information and communication technologies now occupy in our everyday lives. These technologies have substantially enhanced communication, the transfer of information, and the interactions between individuals across the globe. Furthermore, the study aims to critically assess the extent to which Algerian legislation has adapted to the rapid evolution of ICT-related crimes.

The primary objective of this research is to examine ICT-related crimes from a substantive legal standpoint, defining their scope, identifying their various forms, and analyzing the involved parties. These offenses are uniquely characterized by their distinct nature, which differentiates them from conventional crimes, primarily due to their occurrence within a digital framework and their commission through modern technological tools. Given this context, a central question arises: To what degree are the existing substantive legal provisions effective in addressing ICT-related crimes? To address this question and fulfill the study's objectives, the discussion is structured into two main sections. The first section will explore the general framework of ICT-related crimes, while the second will examine various classifications of these crimes.

First Section: General Framework of ICT-related Crimes

As ICT-related crimes are relatively novel, legal scholars have yet to reach a consensus on a standardized terminology to describe these offenses. Various terms have emerged in the academic and legal discourse: some scholars use the term "cybercrimes," others refer to them as "electronic crimes," and some favor the term "informatics crimes" or even "computer crimes," among others. In contrast, the Algerian legislator has opted to classify these offenses as "crimes related to information and communication technologies."

First: The Distinctive Characteristics of ICT-related Crimes

ICT-related crimes exhibit a set of distinctive characteristics that set them apart from both traditional and other emerging categories of crime. These features include:

1. ICT-related Crimes Are Transnational in Nature

A defining attribute of ICT-related crimes is their transnational nature, meaning they often transcend national borders and acquire a global dimension. This is largely due to their reliance on the internet and other information technologies, which are capable of bypassing traditional constraints of time and geography. In the digital realm, there are no physical borders, checkpoints, or transit hubs. A crime can be initiated in one part of the world, yet its effects can reverberate across vast distances, impacting regions thousands of kilometers away.¹

In this context, cybercriminals can perpetrate offenses without being physically present at the crime scene, leading to significant challenges, particularly when it comes to determining jurisdiction. The question of which country should have the legal authority to prosecute the crime becomes more complicated. Moreover, challenges related to the applicable law, as well as procedural complexities involved in prosecuting these crimes, further complicate the legal landscape.²

2. Difficulty in Detecting ICT-related Crimes

The digital nature of ICT-related crimes inherently makes them difficult to detect and trace. This challenge arises primarily from the absence of physical evidence left behind by the perpetrators.³ Users of information and communication technologies are not typically required to disclose their identities while using these tools, which complicates the investigative process. Consequently, many of these crimes are either discovered by chance or not until a considerable time after their commission.

Unlike traditional crimes, ICT-related offenses do not leave behind physical witnesses who can be questioned or tangible evidence that can be scrutinized. Additionally, victims of such crimes often contribute negatively to their detection. This may be due to personal concerns, such as reputational damage, or financial factors related to employment, which often prevent victims from reporting the crimes, thus hindering their detection.

3. Difficulty in Proving ICT-related Crimes

Given that ICT-related crimes occur within a virtual space, they do not produce the tangible evidence typically found in traditional crimes.⁴ Digital evidence can be easily erased or altered in an instant, further complicating the task of proving these offenses. These crimes do not leave physical traces, nor do they provide witnesses who can offer testimony or material evidence to be examined. As a result, proving ICT-related crimes becomes especially challenging.⁵

Moreover, to further complicate the prosecution process, cybercriminals often employ sophisticated techniques and tools designed to shield themselves after committing the offense. These methods are intended to obstruct the discovery of evidence or to delay the process, allowing the offender to evade detection. Investigating such crimes requires a specialized approach, technical expertise, and an in-depth understanding of ICT techniques to effectively retrieve electronic evidence.

¹ Mahmoud Ahmad Ababna, *Computer Crimes and Their International Dimensions*, Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 2009, p. 34.

² Ali Jaafar, *Modern Information Technology Crimes Against Individuals and Government: A Comparative Study*, 1st edition, 2013, Zen Legal and Literary Library, p. 99.

³ See also: Mariam Ahmed Masoud, *Mechanisms for Combating ICT-related Crimes in Light of Law No. 09-04*, Master's thesis, Faculty of Law, Specialization in Criminal Law, Qasdi Merbah University, Ouargla, 2012-2013, p. 8-12.

⁴ Khaled Mamdouh Ibrahim, *Cyber Crimes*, Dar Al-Fikr Al-Jami'i, Alexandria, 2009.

⁵ Hussein Tahiri, *Electronic Crimes*, Dar Al-Khaldounia, Algeria, 1st edition, 2021, p. 18.

4. The Soft Approach in Committing ICT-related Crimes

ICT-related crimes are often characterized by a "soft" approach, which differentiates them from traditional crimes that typically involve physical force, aggression, and violence. Unlike conventional offenses, such as assault, battery, or theft, which require physical exertion, ICT-related crimes are primarily carried out through knowledge and the manipulation of information systems. The cybercriminal does not rely on physical strength to perpetrate the crime; instead, they leverage their expertise in digital systems. This makes ICT-related crimes both subtle and dangerous, as they can be executed quietly and without any visible signs of physical violence.⁶

5. Committing ICT-related Crimes Using Electronic Means

To commit their crimes, cybercriminals exploit technological tools, utilizing devices such as personal computers and mobile phones to communicate, plan, and execute their offenses. These tools grant them access to the internet, allowing the criminal to engage in illegal activities such as tampering with, stealing, or downloading programs to infiltrate or monitor computer systems. Such actions constitute severe breaches of privacy and security, highlighting the vulnerability of digital infrastructure.⁷

6. The Specific Nature of Cybercriminals

Cybercriminals, also referred to as "information criminals," possess distinct characteristics that set them apart from traditional criminals. The commission and concealment of these crimes require a high level of technical skill, which is why the perpetrators must have a comprehensive understanding of computing and internet systems. In other words, cybercriminals are specialists in information technology, possessing the expertise necessary to carry out sophisticated offenses. Understanding these technical proficiencies is crucial to comprehending the behavior of cybercriminals, a topic that will be further explored in the second part of this study.⁸

In addition to these traits, ICT-related crimes are also marked by other distinctive features, such as their ease of execution, rapid implementation, the difficulty of controlling or classifying the crimes, and the frequent tendency for them to remain unreported.

Second: The Parties Involved in ICT-related Crimes

The global proliferation of electronic devices has undoubtedly brought numerous benefits to individuals and societies alike. However, it has also paved the way for a new class of criminals. In this context, particular attention is given to the figure of the "information criminal."

1. The Information Criminal

The information criminal is considered one of the most dangerous types of offenders, characterized by a distinct set of traits that differentiate them from traditional criminals.

A. Defining the Information Criminal in ICT-related Crimes

The information criminal is a specialist in their field, with a professional approach to executing their offenses. Committing ICT-related crimes requires bypassing advanced protective measures within computer systems, a skill set that sets these criminals apart from their traditional counterparts.

Unlike conventional offenders, the information criminal does not rely on physical violence. Instead, they typically possess high intelligence, sophisticated technical skills, and a deep cultural awareness of their area of expertise.⁹

⁶ Abdel Nour Bichane, *Substantive Aspects of Handling Information Crimes*, Doctoral thesis in Criminal Law and Criminology, Faculty of Law, University of Algiers 1, 2017-2018, p. 65.

⁷ Mohamed Khalifa, *Criminal Protection of Computer Data in Algerian and Comparative Law*, Dar Al-Jamia Al-Jadida, Alexandria, Egypt, 2008, p. 36-37.

⁸ Adham Basel Nimer Baghdadi, *Investigation and Inquiry Techniques in Cybercrimes*, Master's thesis in Law, Graduate Studies, An-Najah National University, Nablus, Palestine, 2018, p. 12.

⁹ Nabila Hiba Harwal, *Procedural Aspects of Internet Crimes During the Collection of Evidence*, Comparative Study, Dar Al-Fikr Al-Jami'i, Alexandria, 1st edition, 2006, p. 37.

B. Common Traits Among Cybercriminals Involved in ICT-related Crimes

1. Intelligence

Intelligence is perhaps the most critical trait of individuals committing ICT-related crimes, as these offenses require advanced technical knowledge, especially when it comes to gaining unauthorized access to computer systems for theft, fraud, and other illicit activities. Cybercriminals must possess a high level of expertise to effectively execute these crimes.

A study conducted in the United Kingdom suggests that children who spend significant amounts of time in front of computers tend to exhibit higher levels of intelligence compared to their peers who engage less with technology.¹⁰

The importance of intelligence in these crimes lies in the fact that perpetrators do not need to resort to physical violence to carry out their activities. For instance, a cybercriminal can transfer millions of dollars from one bank account to another without ever leaving their home.

2. Experience and Skill

Cybercriminals typically possess extensive experience and expertise in using computers and the internet. Those who engage in ICT-related crimes are often specialists in information technology, as these crimes require a high degree of technical skill.

Unlike traditional criminals who may rely on physical force, cybercriminals are often categorized as "criminals of intelligence," as their offenses are largely based on their knowledge and understanding of digital systems.¹¹

It is important to note that not all computer-related crimes qualify as ICT-related crimes. Specifically, crimes involving "soft destruction techniques", such as hacking, data manipulation, or surveillance, fall within this category. For individuals with limited technical expertise, their criminal activities might involve simple actions, such as deleting or copying data. In contrast, those with more advanced skills can hack into computer systems, steal money, engage in fraud, or even conduct espionage, all of which require higher levels of expertise.¹²

3. Social Identity of the Cybercriminal

The intelligence of a cybercriminal often enables them to integrate into society in ways that remain undetected or unrecognized. Intelligence is closely tied to adaptability¹³, which can manifest in the formation of groups that share similar ideologies. These groups encourage their members to plan and execute crimes both domestically and internationally.

Social isolation also plays a key role in facilitating cybercriminal activities, as it allows the individual to focus on honing their technical abilities without interference from the outside world. In some cases, these crimes may stem from a desire to demonstrate superiority over electronic systems or serve as a form of self-expression.¹⁴

2. The Victim in ICT-related Crimes

In this section, we will define the victim of ICT-related crimes and explore the various types of individuals or entities that fall victim to these offenses.

A. Definition of the Victim (the Injured Party):

¹⁰ Rahima Nmadili, *The Specificity of Electronic Crime in Algerian and Comparative Law*, Proceedings of the 14th International Conference on Cybercrime, Jil Research Center, Tripoli, Lebanon, March 24-25, 2017, p. 101.

¹¹ Khaled Mamdouh Ibrahim, *Op. Cit.*, p. 133.

¹² Mourad Yermekh, *The Specificity of Electronic Crime*, Doctoral Thesis in Private Law, Intellectual Property Branch, Faculty of Law, University of Algiers 1, Ben Youssef Ben Khedda, 2020-2021, p. 45-47.

¹³ Mourad Yermekh, *Op. Cit.*, p. 135.

¹⁴ Nahla Abdelkader Al-Momani, *Cybercrimes*, Master's in Information Criminal Law, Dar Al-Thaqafa for Publishing and Distribution, 2012, p. 77.

In ICT-related crimes, the victim is anyone who suffers material or moral damage as a result of the unauthorized use of digital technologies. This category encompasses a wide array of individuals or entities whose personal data, financial assets, or privacy have been compromised through illegal technological means.¹⁵

B. Types of Victims in ICT-related Crimes:

- **Natural Persons (Individuals):**

Natural persons are among the most vulnerable to cybercrime, particularly those crimes perpetrated via the internet. The continuous growth in the number of internet users has broadened the reach of cybercriminals, extending their activities beyond the financial and military sectors. As a result, many individuals now fall victim to crimes such as fraud, identity theft, data theft, and data destruction. Millions of personal secrets, whether belonging to ordinary individuals or people in specific positions, are now accessible to anyone capable of breaching digital networks.¹⁶

One of the most prevalent crimes against individuals is credit card theft, along with data destruction via viruses sent through email. Hackers often gain unauthorized access to personal computers through such methods.¹⁷

- **Financial Institutions and Government Bodies:**

These crimes also target legal entities, both public and private. Public institutions, such as state agencies, are at risk from cybercriminals who seek to steal sensitive projects or state secrets. Private institutions, particularly financial organizations such as banks, financial companies, and stock exchanges, are also frequent targets. These entities are attractive to cybercriminals because of the wealth they control and the critical financial data they hold. The primary objective of such crimes is typically to gain access to funds, followed by the acquisition of sensitive information, which is crucial for maintaining a competitive edge in the market economy.

- **Military Institutions:**

The impact of the information revolution extends well beyond the civilian sector, encompassing the development of modern warfare systems and giving rise to what is now known as information warfare. In today's world, the country that controls superior information is often considered the strongest. As a result, military intelligence has become a central focus, and satellite technology, particularly in the hands of military entities, has become integral to the development of modern military equipment.

This shift has led to the emergence of a new form of warfare, information warfare, which is now a global concern. The mechanisms of information warfare are heavily reliant on computer networks for transmitting data via networks and satellites. This dependence has amplified the role of armed forces and information systems within military arsenals. The storage, rapid processing, and presentation of data in a usable format are crucial for decision-makers, enabling them to make well-informed choices based on the significance of the information at hand.

Second Section: Examples of Major Classifications of ICT-related Crimes

According to Algerian law, specifically Article 2, Paragraph 2 of Law No. 09-04, which governs ICT-related crimes and their prevention, an information system is defined as: *"An independent system or a collection of interconnected systems, one or more of which process data automatically as part of a specific program."*

¹⁵ Abdel Nour Bichane, Op. Cit., p. 114-115.

¹⁶ Mustafa Mohamed Mousa, Criminal Investigation in Cybercrimes, Dar Al-Nahda Al-Arabia, Egypt, 2008, p. 159.

¹⁷ Mohamed Mohamed Sheta, The Concept of Criminal Protection for Computer Programs, Dar Al-Jamia Al-Jadida, Egypt, 2001, p. 94.

In this section, we will address two types of crimes: unauthorized access or staying fraudulently within an automated data processing system, and fraudulent manipulation of data within an automated data processing system.

First: The Crime of Unauthorized Access or Staying Fraudulently within an Automated Data Processing System

This crime is based on three essential elements: the legal, material, and mental elements.

- **The Legal Element**

Under Algerian law, specifically the Penal Code, the crimes of unauthorized access and staying fraudulently within a system are classified under Article 394 bis, in Section 7, which deals with felonies and misdemeanors against property.¹⁸

- **The Material Element**

The material element of this crime consists of three components: the criminal act, the criminal result, and the causal link between the act and the result¹⁹. If all these elements are present, the crime is considered complete.

A. The Criminal Act:

The criminal act refers to the unauthorized intervention by the cybercriminal in the external world, as per the legal principle "No crime without a wrongful act." There are two types of criminal actions: an active action (such as unauthorized access) and a passive action (such as remaining within the system without permission).²⁰

Unauthorized access occurs when a person enters the system without authorization or by deceit. This action becomes illegal when it is not authorized by the system administrator, or when access is granted but exceeded in scope.²¹

Fraudulent staying refers to remaining within the system against the will of the authorized individual controlling that system. While Algerian law does not explicitly define this act, it is understood within the legal community to be the act of unauthorized presence within a system after initial access.²²

B. Place of the Criminal Activity:

Algerian law places a significant emphasis on protecting the automated data processing system. This is evident in the extension of the material element to include not only access or staying within the system but also the handling of data at various stages: processing, storage, and retrieval. The system and its networks, along with any data transmitted through them, form the basis of the criminal act. These crimes can target all elements of the system, as their primary goal is to disrupt the automated data processing systems, including information networks.²³

C. The Criminal Result:

To establish a complete crime, the criminal result must occur. If the result is absent, the offense would be considered an attempt rather than a completed crime.

¹⁸ Op. Cit., p. 14.

¹⁹ Law No. 04-15, dated 27 Ramadan 1425 (November 10, 2004), amending and supplementing Ordinance No. 66-156 of the Penal Code, Official Journal No. 71.

²⁰ Ahssen Bouski'a, *The Brief Explanation of Special Penal Law*, 1st edition, Volume 1, Dar Houma, Algeria, 2012, p. 12.

²¹ Rachida Boker, *Crimes Against Automated Processing Systems in Algerian Comparative Legislation*, 1st edition, Halabi Legal Publishing, Lebanon, 2012, p. 175.

²² Op. Cit., p. 179.

²³ Ali Abdelkader Al-Qahouji, *Criminal Protection of Computer Programs*, Dar Al-Jamia Al-Jadida, Alexandria, 1999, p. 133.

There are two scenarios for the criminal result in cases of unauthorized access or staying fraudulently within a system:

- **No result occurs:** According to Paragraph 1 of Article 394 bis, the crime is committed whether or not the act results in any tangible outcome. The mere act of access or staying within the system is considered an infringement of a protected legal right, and legal protection is afforded immediately upon the commission of the act.
- **A criminal result occurs:** According to Paragraph 2 of Article 394 bis, the penalty is heightened if the unauthorized access or fraudulent stay results in one of the following outcomes:
 - Deletion or alteration of data within the system.
 - Destruction or disruption of the system's operation.

3. The Mental Element

The mental element, or *mens rea*, refers to the criminal intent underlying the crime. Without this mental element, criminal liability for the information crime would not be established.

In the case of both unauthorized access and staying fraudulently within a system, these are considered intentional crimes, meaning the general criminal intent is required for their commission. This intent consists of two components: knowledge and will. The perpetrator must be aware that they are accessing or remaining within a system to which they are not authorized. They must also intentionally remain within the system even after their authorized access has expired, even if the initial access was legitimate.

If the perpetrator lacks this awareness, that is, they are unaware of the risks of accessing the system, or they do not intentionally engage in the act of entering or staying, the mental element of criminal intent is absent. According to Article 394 bis of the Penal Code: "*Anyone who enters or stays within a system by fraudulent means*" does not require the specific criminal intent to achieve the result of the crime, but only the general criminal intent.²⁴

Second: The Crime of Fraudulent Manipulation of Data within an Automated Data Processing System

For this crime to be complete, certain essential elements must be present:

1. The Legal Element

The Algerian legislature has criminalized the fraudulent manipulation of data within an automated data processing system under Article 394 bis 1 of the Penal Code.

2. The Material Element

The material element of the crime involves three components:

A. The Criminal Act

The criminal act is realized when the offender engages in one of the activities outlined in Article 394 bis 1 of the Penal Code, specifically:

- **Inputting fraudulent data into the system:** This involves entering data or a program designed to deceive or mislead in order to commit a crime.
- **Removing or altering system data:** This refers to the intentional act of the cybercriminal, after gaining unauthorized access to the system, either removing or modifying data, whether partially or fully, with the goal of disrupting the system, regardless of whether the initial access was authorized or not.

B. The Subject of the Criminal Act

The focus of the criminal activity is on the information within the system. The protection offered under the law extends to data being processed automatically, data in the process of being

²⁴ Rachida Boker, Op. Cit., p. 223-224.

processed, or data that has been processed but is being reintroduced into the system. This also includes data stored in the system's memory, whether in an ongoing or separated state.²⁵

C. The Criminal Result

Algerian law classifies fraudulent manipulation of data as a "dangerous" crime, meaning it does not require a specific material outcome for the crime to be complete. Even if the intended result is not achieved, the crime is still considered complete. If the result occurs as a direct consequence of the perpetrator's actions, or if it fails to occur due to external factors, the crime is considered committed.²⁶

C. The Mental Element

Since fraudulent manipulation of data is an intentional crime, the perpetrator must possess general criminal intent, meaning they are fully aware of the fraudulent actions they are performing (i.e., inserting, removing, or altering data) within an automated data processing system.

The intent to carry out these actions is a critical aspect of the crime, as outlined in Article 394 bis 1: *"Anyone who fraudulently enters data into the system, or removes or alters data within the system"* must have a clear intention to commit these actions and achieve the intended result.

Third: Penalties for Crimes Affecting Automated Data Processing Systems

The legal penalties imposed on offenders in relation to crimes affecting automated data processing systems serve both as a deterrent and a means of accountability. These penalties, as outlined in the Algerian Penal Code, encompass both primary and supplementary sanctions. They apply to both legal entities (corporations or organizations) and natural persons (individuals). The punishments also address participation in and attempts to commit these crimes, as stipulated in Articles 394 bis to 394 bis 7 of the Penal Code.²⁷

1. Penalties for Natural Persons

The Algerian Penal Code specifies both primary and supplementary penalties for crimes affecting the system, as outlined below:

A. Primary Penalties:

The law stipulates primary penalties for each crime, which can include imprisonment and fines. These penalties can be either simple or aggravated, depending on whether the crime is committed under aggravating circumstances.²⁸

• Simple Penalties:

For crimes such as unauthorized access or fraudulent stay within an automated data processing system, the punishment includes imprisonment from 3 months to 1 year and a fine ranging from 50,000 DZD to 100,000 DZD, according to Article 394 bis, Paragraph 1 of the Penal Code.²⁹

For crimes of fraudulent manipulation of data within an automated system, the penalty is imprisonment ranging from 6 months to 3 years and a fine ranging from 500,000 DZD to 2,000,000 DZD, as per Article 394 bis 1.

²⁵ Fatiha Mehri, The Crime of Unauthorized Access to Automated Data Processing Systems, Supplementary Master's Thesis, Specialization in Criminal Business Law, Faculty of Law and Political Science, Arab Ben Mehidi University, Oum El-Bouaghi, 2015-2016, p. 43-42.

²⁶ Zayba Zidan, Information Crime in Algerian and International Legislation, Dar Al-Huda, Algeria, 2011, p. 55.

²⁷ Rachida Boker, Op. Cit., p. 257.

²⁸ Zeina Hamzaoui, Crimes Related to Information and Communication Technologies in Algerian Legislation, Master's Thesis, Specialization in Crime and Public Security, Faculty of Law and Political Science, University of El-Tebessi, 2020-2021, p. 34.

²⁹ Rachida Boker, Op. Cit., p. 317.

- **Aggravated Penalties:**

Article 394 bis 3 states that: "*Penalties shall be doubled if the crime targets national defense or public institutions governed by public law, without prejudice to the application of more severe penalties.*"³⁰

Moreover, Article 394 bis, Paragraph 2 adds that the penalty shall be aggravated if the crime results in the deletion or alteration of system data³¹. Additionally, Article 394 bis, Paragraph 3 stipulates: "*If the actions result in damage to the operational system of the system, the punishment shall be imprisonment from 6 months to 2 years, along with a fine ranging from 50,000 DZD to 150,000 DZD.*"³²

- **B. Supplementary Penalties:**

In addition to primary penalties, the legislator has provided for supplementary penalties, which include confiscation and closure. These measures are specified under Article 394 bis 6 of the Penal Code.³³

- **C. Penalties for Legal Persons (Entities)**

The Algerian legislator has established criminal responsibility for legal persons under Article 51 bis of the Penal Code, which states: "*A legal person shall be criminally responsible for offenses committed on its behalf by its agents or legal representatives when the law so provides.*"

According to Article 394 bis 4, a legal person convicted of committing any of the crimes outlined in this section shall be fined an amount equal to five times the maximum fine imposed on a natural person.³⁴

CONCLUSION:

Through our examination of the substantive provisions regarding crimes related to information and communication technologies (ICT), several critical conclusions have emerged:

- Crimes related to ICT have undergone significant transformation in recent years. Not only has the profile of the offenders evolved, but so too have the methods and technologies employed to commit these offenses. Modern cybercriminals are now exploiting the latest advancements in technical and technological sciences to perpetrate their crimes.
- These crimes, with their diverse forms and the high level of expertise of their perpetrators, whether targeting information systems directly or using them as tools for illegal activities, pose substantial threats to the safety and security of individuals and society at large. Additionally, they are often marked by ambiguity, making both the investigation and prosecution of such offenses particularly challenging. This complexity places a considerable burden on law enforcement and the judiciary.
- In response to the growing threat of cybercrime, the Algerian legislator has, like many other nations, sought to combat these offenses by amending the Penal Code through Law No. 04/15. This legislation now criminalizes unauthorized access to and fraudulent stay within information systems, as well as tampering with data within those systems. Furthermore, Algeria has taken steps to address procedural gaps with the enactment of Law No. 09/04, which introduces both procedural and preventative measures.

Based on these findings, we propose several recommendations:

³⁰ Law No. 04-15, as previously mentioned.

³¹ Law No. 04-15, as previously mentioned.

³² Ibid.

³³ Ibid.

³⁴ Rachida Boker, Op. Cit., p. 327.

– There is a need to review the curricula at law schools, particularly by introducing new subjects related to emerging technologies. This could include incorporating cybercrime into criminal law courses, e-government in administrative law courses, and electronic courts in criminal procedure law courses.

– We urge the Algerian legislator to refrain from blindly adopting foreign laws and instead to make greater use of local Algerian expertise. There are many qualified Algerian professionals whose knowledge should be leveraged to draft national legislation.

– Algeria should benefit from international experiences in the field of ICT-related crimes to develop the necessary skills and expertise to combat these offenses effectively.

– It is crucial for Algeria to join international and Arab conventions aimed at combating cybercrime. This would enable Algeria to engage in collaborative efforts with other countries in the fight against cyber threats.

List of Sources and References:

Sources:

- Law No. 04-15, dated 27 Ramadan 1425 AH (November 10, 2004), amending and supplementing Ordinance No. 66-156 concerning the Penal Code, Official Gazette No. 71.


References:

1. Books:

- a. Ahssan Bousqiaa, *"Al-Wajez fi Sharh al-Qanoun al-Jaza'i al-Khass"*, First Edition, Volume 1, Dar Houma, Algeria, 2012, p. 12.
- b. Rachida Bouker, *"Crimes of Attacks on Automated Data Processing Systems in Algerian Comparative Legislation"*, First Edition, Halabi Legal Publications, Lebanon, 2012, p. 175.
- c. Ali Abdelkader Al-Qahouji, *"Criminal Protection of Computer Programs"*, Dar Al-Jami'ah for Publishing and Distribution, Alexandria, 1999, p. 133.
- d. Mahmoud Ahmed Ababneh, *"Computer Crimes and Their International Dimensions"*, Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 2009.
- e. Ali Jaafar, *"Modern Information Technology Crimes Affecting Individuals and Government: A Comparative Study"*, First Edition, 2013, Zain Legal and Literary Library.
- f. Khaled Mamdouh Ibrahim, *"Cybercrimes"*, Dar Fikr Al-Jami'ah, Alexandria, 2009.
- g. Hussein Tahiri, *"Electronic Crimes"*, Dar Al-Khaldounia, Algeria, First Edition, 2021.
- h. Mohamed Khalifa, *"Criminal Protection of Computer Data in Algerian and Comparative Law"*, Dar Al-Jami'ah Al-Jadida, Alexandria, Egypt, 2008.
- i. Rahima Nmadili, *"The Specificity of Cybercrime in Algerian and Comparative Law"*, Proceedings of the 14th International Conference on Cybercrime, Center for Scientific Research, Tripoli, Lebanon, March 24-25, 2017.
- j. Zibha Zidan, *"Cybercrime in Algerian and International Legislation"*, Dar Al-Huda, Algeria, 2011.
- k. Nabila Hiba Harwal, *"Procedural Aspects of Internet Crimes in the Stage of Gathering Evidence: A Comparative Study"*, Dar Fikr Al-Jami'ah, Alexandria, First Edition, 2006.
- l. Mustafa Mohamed Mousa, *"Criminal Investigation in Cybercrimes"*, Dar Al-Nahda Al-Arabiya, Egypt, 2008.
- m. Mohamed Mohamed Sheta, *"The Concept of Criminal Protection of Computer Programs"*, Dar Al-Jami'ah Al-Jadida, Egypt, 2001.

2. Doctoral Theses:

3. Abdel Nour Bechan, *"Substantive Aspects of Cybercrime: A Thesis for the Doctorate in Criminal Law and Criminology"*, Faculty of Law, University of Algiers 1, 2017-2018.
4. Mourad Yarmesh, *"The Specificity of Cybercrime"*, Thesis for the Doctorate in Private Law, Specializing in Intellectual Property, Faculty of Law, University of Algiers 1, Ben Yousef Ben Kheda, 2020-2021.

- 
5. Nahla Abdelkader Al-Momani, *"Cybercrimes"*, Master's Degree in Information Law, Dar Al-Thaqafa for Publishing and Distribution, 2012.
 6. Adham Basim Nimir Baghdadi, *"Research and Investigation Methods for Cybercrimes"*, Master's Thesis in Law, Faculty of Graduate Studies, An-Najah National University, Nablus, Palestine, 2018.
 7. Fatiha Mehri, *"Crime of Access and Staying in Automated Data Processing Systems"*, Supplementary Memoir for a Master's Degree, Specializing in Criminal Law for Business, Faculty of Law and Political Science, Department of Law, University of Arabic Ben Mehidi, Um El-Bouaki, 2015-2016.