PARTICULARITY OF THE PROSECUTION IN CRIMES RELATED TO THE USE OF ICT IN ALGERIA

MEHALLEGUE JAMILLA[1]
[1] Faculty of Law and Political Sciences, Badji Mokhtar University, Annaba (Algeria).
The E-mail Author: jamillamehallegue@gmail.com
Received: 12/07/2024 Published: 29/01/2025

Abstract:
Technological development has led to the use of ICT (ICT), accompanied by a transformation in various fields of life, leading to the emergence of information crime threatening the security and safety of individuals, society and countries. Therefore, the Algerian legislator is confronting this information crime with appropriate techniques since it does not leave physical traces. Search, examination and investigation in a digital virtual environment are used to get digital evidence to prove and repress the crime which is borderless, raising the issue of conflict of laws and imposes the need to define competent jurisdiction and applicable law, as well as international judicial cooperation.
Keywords: cybercrime; ICT; prosecution; electronic guide; international judicial cooperation.

1. INTRODUCTION

There is no doubt that the world has recently witnessed a radical transformation towards establishing the features of a new world model based on the use of technology in various fields and the accompanying revolution against traditional concepts in the field of information, as the latter has become available to everyone and its positive use contributes to facilitating services and transactions and advancing human knowledge, while its negative use affects the achievement of its intended purpose. With this tremendous and rapid development in the use of technological techniques for information and communication, the commission of crime has developed through the use of modern technology as a tool in committing traditional crime, and new patterns of crimes related to ICT have emerged.

The importance of this study is in the seriousness of this new criminal phenomenon, especially since its perpetrators find it easy to implement, as it does not take a long time, as it may be done in minutes or seconds, and it does not require moving to the place, as it occurs in a virtual environment that does not leave any tangible material traces, unlike traditional crimes, which led to the difficulty of proving it due to the special nature of evidence in this type of crime, as it is not a tangible material evidence that is difficult to obtain, so it has become necessary to reconsider the old means and methods that have often revealed their shortcomings and ineffectiveness in uncovering the perpetrators of these crimes.

Crimes related to ICT also transcend national territorial borders, which raises the issue of tracking and pursuing them outside the national territory. These are crimes that require international judicial cooperation to combat them.

This study concerns and focuses on the specificity of the follow-up in crimes related to ICT?

To address this problem, we follow the analytical approach as well as the descriptive approach, which are indispensable in this research. We divide the research into two sections. The first section deals with the specificity of proof in crimes of ICT, while the second section is devoted to the specificity of judicial jurisdiction in these crimes.

2. SPECIFICITY OF CRIMINAL EVIDENCE IN CRIMES RELATED TO ICT

The emergence of a new type of crimes known as ICT crimes, which are known as information crimes, electronic crimes, or digital crimes, has led to the inadequacy and unsuitability of traditional systems in proving these crimes from the legal and technical aspects. It is imperative for the legislator to create legislation that is compatible with this type of crime, in addition to establishing specialized

technical bodies entrusted with the process of scientific and technical proof of these crimes. Accordingly, we address the definition of crimes related to ICT and clarify the most important characteristics that distinguish them from other crimes, then we explain the methods of proof in these crimes.

2.1 First requirement: What is meant by ICT crimes?

Modern ICT has been exploited to commit crimes. It differs from traditional crimes because they are crimes closely linked to technology, which relies mainly on computers and other technical devices.

We discuss the definition of ICT crimes according to the Algerian legislator through legal texts according to their chronological order as follows:

2.1.1 Penal Code:

The Algerian legislator adopted in Law No. 04-15 [1] amending the Penal Code the term "tampering with automated data processing systems" in Section 7 bis thereof under the title "tampering with automated data processing systems" which included 08 articles from Article 394 bis to Article 394 bis 7, in which it criminalized acts that affect computer systems. In 2006, the Algerian legislator added an amendment to the Penal Code pursuant to Law No. 06-23 according to Section 7 bis, in which the penalty of imprisonment and the fine prescribed for these acts only were increased without prejudice to the criminal texts contained in this section. The Algerian legislator kept pace with the development of this field and in parallel with the various legislations that developed a strategy to combat this new type of crime.

2.1.2 Law No. 09-04 on crimes related to ICT:

The Algerian legislator defined the crime related to ICT under Law No. 09-04 as crimes related to ICT [2] and defined it in Article 2 as crimes of tampering with automated data processing systems specified in the Penal Code and any other crime committed or facilitated by an information system or electronic communications system. It can be noted that the Algerian legislator has expanded the scope of criminalization by adopting several criteria, including the subject of the crime, which is crimes of tampering with automated data processing systems, as well as the means of committing the crime, which is the information system or electronic communications system.

2.1.3 Criminal Procedure Code:

Pursuant to Order 21/11 amending and supplementing the Criminal Procedure Code and through paragraph 3 of Article 211 bis 22, it is noted that the Algerian legislator emphasized the definition of crimes related to ICT and expanded it to include all electronic crimes by their nature (subject matter) or traditional crimes that are committed or facilitated by the use of an information system or an electronic communications system or any other means or mechanism related to ICT, and thus the legislator has expanded the scope of criminalization to include every mechanism related to information technology.

2.2 Characteristics of crimes related to ICT

The connection of crimes related to ICT with the computer and Internet has given it a set of characteristics, the most important of which are:

2.2.1 Across countries and continents:

The information society does not recognize geographical borders. Networks are borderless in time and space. This is what criminals exploit to commit these crimes remotely, where there is distance between the perpetrator and the victim, as the criminal act may occur in one country and the criminal result is achieved in another country, and this increases difficulty in discovering it as the case with cyber terrorism, which is a crime that crosses national borders [3].

2.2.2 Committed via Internet:

These crimes are committed via Internet, which is a feature that distinguishes it from other crimes. The perpetrator uses a computer and other modern technological means that enable him to access Internet and commit the crime, regardless of its type. It is the link between the various targets of these crimes, such as industrial companies, banks, and other targets that are often victims of these crimes, which necessitated them to take precautions and strengthen their electronic security systems so that they are not exposed to these crimes or reduce their losses or be targeted [4].

2.2.3 Difficulty of detecting the crime:

These crimes are characterized by being hidden and covert because the victim does not notice them despite his presence on the network, so that the perpetrator is an expert in technical matters to carry out his crime accurately, such as sending viruses or spying on stored data.

2.2.4 Easy to commit and quick to implement:

The perpetrator usually commits these crimes alone without seeking the help of other people. He carries out his criminal plan while sitting in front of his computer at home the need for muscular effort, unlike traditional crimes such as breaking doors and locks in the crime of theft. This is what some call the characteristic of softness, and it does not cost the perpetrator to purchase weapons, ammunition, and other tools [5]. To carry out his crime, it is sufficient for him to have some technical devices and programs available, which reduces the costs of committing it, as it is usually attractive to the perpetrators, not to mention the profits it may generate for them, and it does not require a lot of time to do it.

2.2.5 The perpetrator is a person with technical experience:

In order for a computer to be used to commit or carry out a crime on Internet, this user must be very knowledgeable and have great experience in his field in order to commit his crime under cover. Therefore, we find that most of those who commit these crimes are experts in the field of computing. As is the case with electronic terrorism, it no longer requires violence or force, but rather requires a computer connected to the information network, unlike traditional terrorism [6].

2.2 Second requirement: Methods of proof in crimes related to ICT

Crimes related to ICT are among the newly emerging electronic crimes that appeared as a result of the misuse of ICT. These crimes are characterized by the difficulty of proving them and that we are dealing with a criminal phenomenon of a special nature related to the cybercriminal law [7].

2.2.1 Electronic Evidence

Due to the spread of the phenomenon of cybercrime and its resulting effects on the level of criminalization, punishment and criminal procedures, cybercrime is a special type of crime that is developing rapidly and continuously, which has created the problem of the difficulty of searching for evidence and following up on the perpetrators of this advanced crime, as it is not a tangible, visible evidence. It has the following features [8]:

- Electronic evidence is a scientific and technical evidence.
- Electronic evidence is difficult to get rid of.
- Electronic evidence can be copied.

The Algerian legislator has authorized copying and emptying data onto an electronic storage medium that can be seized, such as: a hard disk, a CD, or a flash memory, etc., in accordance with the text of Article 06 of Law 09-04.

2.2.2 Procedures for extracting electronic evidence

The Algerian legislator worked to find modern mechanisms and methods to combat electronic crime and the electronic criminal, through amendments to the level of the Code of Criminal Procedure and special laws.

a. Procedures included in the Code of Criminal Procedure

- **Gathering information** [9].
- **Special investigation procedures:** The development of crime prompted the legislator to create new means to combat it, through Law 06/22 dated 12/22/2006 amending and supplementing the Code of Criminal Procedure, in Articles 65 bis 5 to bis 18 thereof.
- **The infiltration process:** Among these means, we find the infiltration that the Algerian legislator has organized through Articles 65 bis 11 to bis 18 of the Code of Criminal Procedure. Given the seriousness of this procedure and the violation of the privacy of the accused that may occur in it, the legislator has restricted it to a set of guarantees that must be observed during the investigation and inquiry, and they are of two types:
  - Formal conditions.
  - Objective conditions.
- **Intercepting electronic correspondence:** Personal communications in general and electronic communications in particular are among the most important issues related to a basic human right,

namely the right to personal privacy, which has been emphasized and protected by many international charters and agreements [10]. The Algerian legislator did not provide for a specific definition of the process of intercepting correspondence. Through the text of Article 65 bis 5 of the Criminal Code, we find that intercepting correspondence means capturing, recording or copying correspondence that takes place through wired and wireless communication channels or means [11].

The Algerian legislator has established legal guarantees that prevent abuse by public authorities and preserve individual freedom, the most important of which are:

- Licensing and monitoring of the judicial authority.
- Benefits of lawful interception in revealing the truth.
- Lawful interception period.

b. Procedures contained in Law 09/04.

Law 09/04, which contains special rules for the prevention of crimes related to ICT, includes a set of procedures to enhance the effectiveness and speed of investigations onto these crimes, which are represented in monitoring electronic communications, inspection of an information system, and seizure or detention.

- Monitoring electronic communications.
- Inspection of an information system.
- Seizure (reservation of information data).

3. SPECIFICITY OF JUDICIAL JURISDICTION IN CRIMES OF ICT

In the context of combating crimes related to ICT, the legislator has created legal mechanisms that are consistent with the specificity of these crimes, by creating the sixth chapter in the Code of Criminal Procedure pursuant to Order 21/11 amending and supplementing the Code of Criminal Procedure, which includes the creation of a specialized criminal pole to combat crimes related to ICT. These crimes are also considered organized crimes that cross borders, which raises the issue of conflict of jurisdiction, which requires the combination of national and international efforts to combat them.

3.1 The first requirement: national jurisdiction

Given the novelty of crimes related to media and communication technologies, we consider they are new to developing societies compared to developed countries, and the inability of traditional penal procedures to combat these crimes, the legislator has required the need for the penal legislative system to keep pace with technological development, through the introduction of many penal and procedural legal texts, most notably Order 21/ 11, amending and supplementing the Code of Criminal Procedure, which includes the creation of a specialized penal center to combat crimes related to ICT. How effective is the national criminal pole in combating crimes related to ICT?

3.1.1 Rules of Jurisdiction of the National Criminal Pole

Is the national penal pole subject to the same rules of jurisdiction as regular courts, or is it distinguished by special rules?

1. Territorial jurisdiction

The national jurisdiction for crimes of automated data processing, or what is known as crimes related to information technology or electronic crimes, is defined in two stages:

- Stage of expanding the jurisdiction of some courts (criminal poles) [12, 13].
- Stage of establishing the national penal pole [14,15].

2. Subject-matter jurisdiction of the National Criminal Pole

The subject-matter jurisdiction of the criminal courts is determined on the basis of the type of crime and the penalty prescribed for it. The specialized National Criminal Pole is responsible for following up, investigating and ruling on the crimes specified in accordance with the aforementioned Order 21/11, as follows:

- **Special jurisdiction**

The jurisdiction of the National Criminal Pole to combat crimes related to ICT is determined by Article 211 bis 22 of the Criminal Procedure Code. The special jurisdiction of the National Criminal Pole is determined by two criteria: the first relates to the type of crime (crimes related to ICT and crimes

associated with them), and the second relates to the legal classification of the crime, that it is competent to rule on misdemeanors only.

It is noted that the legislator, on one hand, has expanded the jurisdiction of the penal pole to follow up and investigate crimes related to ICT, as well as crimes associated with them. On the other hand, we find that he has narrowed the ruling, as the national penal pole is not competent to rule on them except as misdemeanors, while felonies are subject to the general rules of jurisdiction and the ruling on them is assigned to the criminal court of first instance. This raises the question of the usefulness of establishing the national penal pole to combat crimes related to ICT? It would have been more appropriate if it were subject to the same specialized penal pole and that a criminal court of first instance and appeal be formed in the same pole, and their composition would be made up of specialized judges without jurors, so that we can actually move towards combating this new and constantly evolving type of crime.

- **Exclusive jurisdiction**

Articles 211 bis 24 and 25 bis of the Criminal Procedure Code include the exclusive jurisdiction of the National Criminal Pole, in two cases:

- Crimes related to ICT mentioned in Article 211 bis 24, as well as crimes associated with them.
- Crimes related to ICT mentioned in Article 211 bis 25 and related crimes.

- **Joint jurisdiction**

The National Criminal Pole for Combating Crimes Related to ICT has joint jurisdiction with the jurisdiction resulting from the application of Articles 37, 40 and 329 of the Criminal Procedure Code with regard to crimes related to ICT and crimes associated with them, taking into account the provisions of Articles 211 bis 24 and 25 bis of the Criminal Procedure Code, meaning that the National Criminal Pole has jurisdiction over crimes related to ICT and crimes associated with them with joint jurisdiction with the competent local judicial authorities (local jurisdiction is established at the place of commission of the crime or the place of residence of the suspect or the place of arrest of the suspect) with the possibility of extending jurisdiction to the district of other courts in the following crimes: drug crimes, transnational organized crime, crimes affecting automated data processing systems, money laundering and terrorism crimes and crimes related to exchange legislation in addition to corruption crimes and smuggling crimes [16], which are outside the exclusive jurisdiction of this pole.

However, the legislator has excluded, in the case of joint jurisdiction of the National Criminal Pole for ICT, two cases in which jurisdiction is mandatory for one judicial authority and not the other, as follows:

- The mandatory jurisdiction of the Economic and Financial Penal Pole.
- The mandatory jurisdiction of the court of the headquarters of the Algiers Judicial Council.

It can be concluded from the above that the joint jurisdiction of the National Criminal Pole for Combating Crimes Related to ICT is concerned with three crimes: crimes against automated data processing systems, crimes related to ICT, drug crimes, and transnational organized crime with a misdemeanor character, while the aforementioned crimes with a criminal character are excluded from the scope of jurisdiction and are subject to expanded judicial jurisdiction through regulation.

It is noted that the legislator sometimes considers organized crime to be subject to the exclusive jurisdiction of the pole if it requires the use of special investigative means or specialized technical expertise or resorting to international judicial cooperation (Article 211 bis 25 of the Criminal Procedure Code), and sometimes subjects it to the joint jurisdiction of the pole (Article 211 bis 27 of the Criminal Procedure Code). The legislator should have settled this issue and made it subject to the exclusive jurisdiction of the pole if it was committed using electronic means or mechanisms.

3.1.2 Procedures specific to the National Criminal Pole

Is the national penal pole subject to the same rules of jurisdiction as regular courts, or is it distinguished by special rules?

Referring to the provisions of Articles 211 bis 22 to 29 bis of the Criminal Procedure Code relating to the newly established criminal pole, we find that the legislator has provided for the follow-up, investigation and ruling in crimes related to ICT and crimes associated with them, without referring

to the search and investigation of these crimes; which indicates that they are subject to the search and investigation procedures assigned to judicial police officers according to Articles 15 and 16 of the Criminal Procedure Code in accordance with the rules of expanded territorial jurisdiction, as well as judicial police officers belonging to the National Authority for the Prevention of Crimes Related to ICT [17].

As for the procedural rules followed before the National Criminal Pole, the legislator referred to them within the provisions of Articles 211 bis 26 and 27 bis of the Criminal Procedure Code, as follows:

1. Case of exclusive jurisdiction pole

In Article 211 bis 26 of the Criminal Procedure Code, the legislator referred to the procedures stipulated in Articles 211 bis 19 to 21 bis of the Criminal Procedure Code, as follows:

- If the case is in the investigation and inquiry phase, the reports and minutes must be sent by the judicial police officers directly to the public prosecutor at the competent national criminal pole, and the judicial police officers receive instructions from him directly, and in the event of opening a judicial investigation, they receive judicial commissions from the investigating judge at the pole.
- If the Public Prosecutor finds that the facts reported to him do not fall within his jurisdiction, he shall issue a decision to relinquish the case in favor of the competent Public Prosecutor.
- If the investigating judge finds that the facts notified do not fall within his jurisdiction, he shall issue an order of lack of jurisdiction, either automatically after obtaining the opinion of the Public Prosecutor or based on the Public Prosecutor's requests.
- The file of the proceedings shall be transferred, upon the request of the Public Prosecutor, to the regionally competent Public Prosecution Office when the decision of the investigating judge becomes final.
- The arrest or detention orders issued by the investigating judge remain in effect.
- The follow-up and investigation procedures, as well as the formal procedures taken before the issuance of the order of lack of jurisdiction, shall not be renewed.

2. Case of joint jurisdiction pole

Regarding the procedures followed before the National Criminal Pole, the legislator referred in Article 211 bis 27 of the Criminal Procedure Code to the procedures stipulated in Articles 211 bis 4 to bis 15 of the Criminal Procedure Code, as follows:

- **Case of joint jurisdiction with national courts:** If the case file is located at the level of one of the national courts with regional jurisdiction, with the exception of the court of the headquarters of the Algiers Judicial Council, the newly created penal pole is connected to the case file.
- **Case of joint jurisdiction with the criminal poles:** If the request for the file by the Public Prosecutor at the newly created criminal pole coincides with the request for it by the Public Prosecutor at the judicial authorities with expanded territorial jurisdiction, with the exception of the economic and financial criminal pole, then the jurisdiction shall necessarily be transferred to the Public Prosecutor at the newly created criminal pole. The file shall be relinquished, whether at the stage of investigation and inquiry, follow-up or judicial investigation, in favor of the Public Prosecutor at the newly created criminal pole, and the judicial police shall be placed under the authority and management of the Public Prosecutor at the newly created pole and the requests of the investigating judge at the newly created criminal pole shall be implemented.
- **Case of joint jurisdiction with the Economic and Financial Pole or with the court of the headquarters of the Algiers Judicial Council:** we distinguish between two cases as follows:
  - If the jurisdiction of the National Criminal Pole for Combating ICT coincides with the jurisdiction of the Economic and Financial Criminal Pole, then jurisdiction shall necessarily be transferred to the Economic and Financial Criminal Pole. The newly created criminal pole must relinquish the case file, whether at the stage of investigation and inquiry, follow-up or judicial investigation, in favor of the Economic and Financial Criminal Pole.
  - If the jurisdiction of the National Penal Pole for Combating ICT coincides with the jurisdiction of the court at the headquarters of the Algiers Judicial Council, jurisdiction shall necessarily be transferred to the court at the headquarters of the Council, by following the same previous procedures (renunciation).

3.2 Second requirement: Conflict of jurisdiction in ICT crimes

Crimes related to ICT have acquired an international character, as they are considered transnational crimes, exceeding the borders of a single country as a result of the amazing progress in means of communication and transportation. They raise the problem of judicial jurisdiction and the applicable law, as well as the procedures for prosecution and investigation [18]; but in reality, they are internal crimes punishable by national penal law in addition to the relevant international agreements, and they require international judicial cooperation [19].

3.2.1 Principles of internal jurisdiction

To determine the applicable law in crimes related to ICT, it is necessary to determine the place where they were committed. They may be committed in more than one country and by one or more persons of different nationalities, and they may affect the basic interests of many countries, which raises the question of which law should be applied?

1. Principle of territoriality

The principle of territoriality of the criminal text is the application of the penal code to all crimes, regardless of their type and regardless of the nationality of the perpetrator, which is included in Article 3 of the Penal Code. One of its most important justifications is that it is an aspect of the state's sovereignty over its territory, by applying the law of the place where the crime was committed, which is the most appropriate because it is the place where evidence is available. This principle also establishes the idea of general deterrence of criminal punishment. The interest of the accused lies in applying the law of the country in which his crime was committed, assuming that he is aware of this law, which achieves the purpose of the principle of criminal legality [20].

The Algerian legislator adopted the principle of territoriality of criminal law, whereby a crime is considered to have been committed in Algerian territory if one of the acts constituting one of its elements was committed in Algeria. The question arises when the elements of the crime are distributed in more than one territory, so that more than one state has jurisdiction to consider this crime, which requires the necessity of determining the bases according to which the jurisdiction of states is determined to consider the crime, and to resort to some other complementary principles.

2. Principles complementary to the principle of territoriality

With the development of the world and its transformation into a small village, the principle of territoriality alone has become insufficient to confront the criminal phenomenon, which necessitated the need to resort to some complementary principles to confront crime and prevent impunity, through the following principles:

- **Principle of the character of the criminal text:** The first complementary principle to the principle of territoriality is the application of the criminal text to every offender who holds the nationality of the state, regardless of the territory in which the crime was committed, as stipulated by the Algerian legislator in Articles 582 and 583 of the Code.
- **Principle of the specificity of the criminal text:** It is the second principle complementary to the principle of territoriality and means applying Algerian national law to all crimes committed abroad that affect the basic interests of the state related to its sovereignty and economy, such as counterfeiting money or banknotes in circulation in Algeria at the time of committing the crime, in accordance with the provisions of Article 588 of the Penal Code; Thus, the Algerian legislator has expanded the scope of local jurisdiction of Algerian courts to consider crimes related to ICT if they are committed outside Algerian territory by foreigners and target Algerian state institutions, national defense, or the strategic economic interests of the national economy, through Article 15 of Law 09/04 containing the special rules for the prevention of crimes related to ICT.
- **Principle of universality:** The Algerian legislator did not explicitly stipulate this principle, and it means that the national criminal law applies to all crimes of a global or international nature when the perpetrator is arrested or apprehended in Algeria, regardless of the nationality of this person, i.e. that neither the perpetrator nor the victim are Algerian nationals, and regardless of the place where the crime was committed, provided that it is not Algeria.

3.2.2 Aspects of International Judicial Cooperation

The phenomenon of transnational crime, especially crimes related to ICT, in light of the ease of obliterating evidence and the shortcomings of domestic criminal legislation in combating them. The

importance of international judicial cooperation to combat cybercrimes is due to the shortcomings of domestic legislation and the resulting procedural difficulties in confronting these crimes in order to create integration and resolve the difficulties resulting from conflicts in the application of laws, as well as achieving speed and effectiveness in prosecuting and punishing the perpetrators of these crimes [21].

Judicial cooperation is a set of legal means by which one country provides assistance to its public authority or judicial institutions to the investigating, ruling or executing authority in another country [22]. International judicial assistance is defined as any judicial procedure undertaken by a country that facilitates the task of prosecuting a crime in another country [23].

Therefore, the Algerian legislator addressed in Law 09/04, which includes special rules for the prevention of crimes related to ICT, through Chapter Six on international judicial cooperation and assistance, which is as follows:

1. Forms of international judicial assistance

They can be presented in several forms, including the following:

- **Exchange of information and taking precautionary measures:** The Algerian legislator adopted the technology of exchanging information and taking precautionary measures within the framework of international judicial assistance through Article 17 of Law 09/04 due to the importance of information in combating crime, especially cybercrime, within the framework of relevant international agreements, bilateral international agreements and the principle of reciprocity.
- **International judicial delegation:** International judicial delegation is one of the forms of judicial assistance for international cooperation. It is defined as a request for a judicial procedure by the judicial authorities of a country to a foreign judicial authority to carry out, on its behalf and in its territory, a specific procedure or group of procedures that it is unable to carry out on its own [24].
- **Extradition of criminals:** It is the abandonment by one country to another of a person who has committed a crime in order to prosecute him for it or to implement the sentence issued by the courts because the country requesting extradition has the natural jurisdiction or is the first to try and punish him, provided that the extradition takes place within the framework of the conditions agreed upon in agreements between countries [25].

2. Restrictions on international judicial assistance

The Algerian legislator has restricted the conditions for accepting international judicial assistance through Law 09/04, which includes special rules for preventing crimes related to ICT, through Articles 16 and 18 thereof. In cases of urgency and taking into account international agreements and the principle of reciprocity, it has permitted the acceptance of requests for judicial assistance if they are received via rapid means of communication, including fax machines or e-mail, to the extent that these means provide sufficient security conditions to ensure their validity. In return, the acceptance of international judicial assistance has been restricted by conditions, which are:

- Not to prejudice national sovereignty or public order,
- Maintaining the confidentiality of information.
-

3. Conclusions and suggestions

Crimes related to ICT have become the most serious crimes due to the adoption of information technology and communication technologies in all areas of life. They are in rapid and continuous development, until our era became known as the information age. Their use is not limited to individuals only, but has extended to their use by governmental and non-governmental institutions. E-governments, E-commerce, E-contracts, E-Learning, remote litigation have emerged.... etc. However, these modern technologies are a double-edged sword. As much as they contribute to the speed of transactions, processing and storage, they also negatively affect their deviant use and the commission of crimes related to ICT; which requires the combination of national efforts through a legislative arsenal that is in line with technological development, especially the trend towards electronic follow-up, relying on modern technological techniques in research, investigation and inquiry into these crimes due to their specificity and transnational nature, not to mention a

specialized judiciary capable of confronting cybercrime by all standards. This can be observed through the Algerian legislator issuing a set of national laws, not to mention the need for international judicial cooperation. Through this research, we reached a set of results and recommendations:

- The legislator has moved towards special investigation procedures under Law 06/22 amending and supplementing the Code of Criminal Procedure, through Articles 65 bis 5 to bis 18, which allowed the interception of correspondence, recording of voices, taking photographs and infiltration according to conditions within the framework of the procedural legitimacy of investigation and inquiry into serious crimes exclusively, including crimes affecting automated data processing systems.
- Issuance of Law 09/04, which includes special rules for the prevention of crimes related to ICT, through which the term crimes related to ICT was adopted; the legislator also adopted through its investigation methods specific to ICT, electronic monitoring, inspection of an information system, and then the adoption of electronic evidence as proof.
- The difficulty of monitoring electronic evidence, whether in terms of seizing it, obtaining it, and transferring it from the virtual world to the physical world, as well as the difficulty of assessing the extent of the validity of electronic evidence in criminal proof.
- The legislator has moved towards judicial specialization to combat crimes related to ICT, which are known as crimes affecting automated data processing systems under Law 04/14 dated 11/10/2004 amending and supplementing the Code of Criminal Procedure, which established judicial bodies with expanded territorial jurisdiction to combat serious crimes exclusively.
- Then, issuance of Order 21/11 dated August 25, 2021 amending and supplementing the Code of Criminal Procedure, which reorganized crimes related to ICT to include crimes affecting automated data processing systems and other crimes committed or facilitated by ICT, thus the legislator has expanded the scope of criminalization to include all crimes related to ICT in the future.
- The legislator also created, by virtue of the aforementioned Order 21/11, the National Criminal Pole specializing in crimes related to ICT, which indicates that the Algerian legislator has become aware of the seriousness of crimes related to ICT, especially since ICT has become a way that facilitates the commission of crimes not only related to information technology but also traditional crimes, which requires the inevitability of judicial specialization in order to confront electronic crimes.
- The legislator has moved towards international judicial cooperation to combat cybercrime, given the cross-border nature of cybercrime.

Despite the Algerian legislator's move towards combating crimes related to media and communication technologies, it remains unable to confront what technology produces and the development of artificial intelligence. We offer some suggestions:

- The necessity of raising awareness among civil society about the seriousness of using technology and communication networks, and exercising caution when using them, and activating the policy of reporting these crimes.
- The legislator's tendency towards judicial specialization by establishing a national criminal pole at the level of the Algiers Judicial Court makes it insufficient in combating crimes related to ICT, either because the criminal pole is far from the citizen, as it is located at the level of the capital, or because a single criminal pole cannot accommodate all electronic crimes. It would be preferable if the legislator created regional criminal poles specialized in crimes related to ICT.
- The jurisdiction of the National Criminal Pole is to consider only misdemeanors and not felonies. What is the benefit of judicial specialization? This is a shortcoming in the legislation. The legislator should include felonies under the jurisdiction of the National Criminal Pole by creating a criminal court specializing in crimes related to ICT.
-

4. REFERENCES:

1. Abdel Aal Al-Dreibi, Muhammad Sadiq Ismail, previous reference.
2. Abdel Fattah Mohamed Seraj, General Theory of Extradition of Criminals, An Analytical and Original Study, PhD Thesis, Mansoura University, 1999.

3. Abdul Hakim Rashid Toba, Information Technology Crimes, First Edition, Dar Al-Mustaqbal for Publishing and Distribution, Jordan, 2009.
4. Aisha Bin Qara Mustafa, the previous reference.
5. Amour Khadija, Rules of Jurisdiction of Criminal Poles to Consider Corruption Crimes, Journal of Studies in Public Service, No. 2, University of Jijel, 2014.
6. Article 14 of Law 09/04 relating to the rules specific to ICT.
7. Article 2/A, Article 15 of Law 09/04.
8. Badji Abdel Nour, Malek Nasima, Electronic Terrorism, Between the Globalization of Crime and the Necessity of Combating It, Journal of Legal Studies and Research, Faculty of Law and Political Science, University of M'sila, Volume 7, Issue 2, 2022.
9. Ben Hamidouche Nour El Din, Rahmouni Abdel Razzaq, The Status of Electronic Evidence in Criminal Evidence, Journal of Legal Studies and Research, Faculty of Law and Political Science, University of M'sila, Volume 04, Issue 02, pp: 193-203.
10. Ben Mohamed Mohamed, Conflict of Jurisdiction in Electronic Crimes, Politics and Law Notebooks, Faculty of Law and Political Science, University of Kasdi Merbah, Ouargla, Issue 2, January 2010.
11. Ben Turki Laili, General Theory of Crime and Criminal Punishment, Lectures Print, Private Law Department 2023.
12. Hassanein Obeid, International Criminal Justice, Dar Al-Nahda Al-Arabiya, Cairo, 1977.
13. Hoda Hamed Qashqoush, Computer Crimes in Comparative Legislation, Dar Al-Nahda Al-Arabiya, Cairo, Egypt, 1992.
14. Jaafar Hassan Jassim Al-Taie, Information Technology Crimes, First Edition, Dar Al-Bidaya Publishers and Distributors, Jordan, 2010.
15. Jaddi Sabrina, Criminal Protection of Privacy in the Electronic Environment, PhD Thesis in Criminal Law, Faculty of Law and Political Science, University of Badji Mokhtar, Annaba, Algeria, 2015-2016.
16. Law 09/04 dated August 5, 2009 containing special rules for the prevention and combating of crimes related to ICT, Official Journal of the Algerian Republic, No. 47.
17. Law 20/04 dated August 30, 2020 amending and supplementing the Code of Criminal Procedure.
18. Law No. 04-15 dated November 10, 2004, amending and supplementing the Penal Code, Official Journal of the Algerian Republic, No. 71, dated November 10, 2004.
19. Nabil Saqr, Computer Crimes in Algerian Legislation, Dar Al-Hilal for Media Services, Algeria, 2005.
20. Nabil Saqr, Computer Crimes in Algerian Legislation, Dar Al-Hilal for Media Services, Algeria, 2005.
21. Order 05/06 of August 23, 2005 relating to fight against smuggling, edition n° 59.
22. Rami Metwally Al-Qadi, Combating Cybercrimes in Comparative Legislation and in Light of International Agreements and Covenants, 1st ed., Dar Al-Nahda Al-Arabiya, Cairo, 2011.
23. See for example: Articles 1, 5, 12 of the Universal Declaration of Human Rights of 1948, Article 17 of the Arab Charter on Human Rights of 2004, Article 8 of the European Convention on Human Rights and Fundamental Freedoms of 1950, and Article 11 of the American Convention for the Protection of Human Rights of 1960.
24. This concerns the Sidi Mohamed Court of Algiers, Constantine Court, Oran Court, Ouargla Court.
25. Yazid Bouhlit, Electronic Crimes and Prevention in Algerian Law, Dar Al-Jamia Al-Jadida, Alexandria, 2019.

5. Endnotes:

[1] Law No. 04-15 dated November 10, 2004, amending and supplementing the Penal Code, Official Journal of the Algerian Republic, No. 71, dated November 10, 2004.

[2] Law 09/04 dated August 5, 2009 containing special rules for the prevention and combating of crimes related to ICT, Official Journal of the Algerian Republic, No. 47.

[3] Badji Abdel Nour, Malek Nasima, Electronic Terrorism, Between the Globalization of Crime and the Necessity of Combating It, Journal of Legal Studies and Research, Faculty of Law and Political Science, University of M'sila, Volume 7, Issue 2, 2022, pp. 64-84, p. 72

[4] Jaafar Hassan Jassim Al-Taie, Information Technology Crimes, First Edition, Dar Al-Bidaya Publishers and Distributors, Jordan, 2010, p. 140.

[5] Abdel Aal Al-Dreibi, Muhammad Sadiq Ismail, previous reference, p. 56.

[6] Ben Hamidouche Nour El Din, Rahmouni Abdel Razzaq, The Status of Electronic Evidence in Criminal Evidence, Journal of Legal Studies and Research, Faculty of Law and Political Science, University of M'sila, Volume 04, Issue 02, pp: 193-203, p. 196.

[5] Abdul Hakim Rashid Toba, Information Technology Crimes, First Edition, Dar Al-Mustaqbal for Publishing and Distribution, Jordan, 2009, pp. 140-141.
[7] Hoda Hamed Qashqoush, Computer Crimes in Comparative Legislation, Dar Al-Nahda Al-Arabiya, Cairo, Egypt, 1992, p. 5.
[8] Yazid Bouhlit, Electronic Crimes and Prevention in Algerian Law, Dar Al-Jamia Al-Jadida, Alexandria, 2019, p. 399.
[9] Aisha Bin Qara Mustafa, the previous reference, pp. 86-87.
[10] See for example: Articles 1, 5, 12 of the Universal Declaration of Human Rights of 1948, Article 17 of the Arab Charter on Human Rights of 2004, Article 8 of the European Convention on Human Rights and Fundamental Freedoms of 1950, and Article 11 of the American Convention for the Protection of Human Rights of 1960.
[11] Jaddi Sabrina, Criminal Protection of Privacy in the Electronic Environment, PhD Thesis in Criminal Law, Faculty of Law and Political Science, University of Badji Mokhtar, Annaba, Algeria, 2015-2016, p. 403.
[12] This concerns the Sidi Mohamed Court of Algiers, Constantine Court, Oran Court, Ouargla Court.
[13] Article 2/A, Article 15 of Law 09/04.
[14] Law 20/04 dated August 30, 2020 amending and supplementing the Code of Criminal Procedure.
[15] Amour Khadija, Rules of Jurisdiction of Criminal Poles to Consider Corruption Crimes, Journal of Studies in Public Service, No. 2, University of Jijel, 2014, p. 134.
[16] Order 05/06 of August 23, 2005 relating to fight against smuggling, edition n° 59.
[17] Article 14 of Law 09/04 relating to the rules specific to ICT.
[18] Nabil Saqr, Computer Crimes in Algerian Legislation, Dar Al-Hilal for Media Services, Algeria, 2005, p. 160.
[19] Nabil Saqr, Computer Crimes in Algerian Legislation, Dar Al-Hilal for Media Services, Algeria, 2005, p. 160.
[20] Ben Turki Laili, General Theory of Crime and Criminal Punishment, Lectures Print, Private Law Department, p. 56.,2023
[21] Rami Metwally Al-Qadi, Combating Cybercrimes in Comparative Legislation and in Light of International Agreements and Covenants, 1st ed., Dar Al-Nahda Al-Arabiya, Cairo, 2011, p. 132.
[22] Rami Metwally Al-Qadi, previous reference, p. 133.
[23] Hassanein Obeid, International Criminal Justice, Dar Al-Nahda Al-Arabiya, Cairo, 1977, p. 99.
[24] Ben Mohamed Mohamed, Conflict of Jurisdiction in Electronic Crimes, Politics and Law Notebooks, Faculty of Law and Political Science, University of Kasdi Merbah, Ouargla, Issue 2, January 2010, p. 156.
[25] Abdel Fattah Mohamed Seraj, General Theory of Extradition of Criminals, An Analytical and Original Study, PhD Thesis, Mansoura University, 1999, p. 65.