

**Crimes related to information and communication technologies, any
role of the criminal justice in combating them, in the light of Law No.
25-14 of the Code of Criminal Procedure**

Dr. Remal Amine^{1*}

¹ University of Tlemcen (Algeria), remal.amine16@gmail.com

Received: 28./10/2025

Accepted: 05./11/2025

Published:04./12/2025

Abstract:

Crimes related to information and communication technologies are one of the most widespread crimes due to the comprehensive use of technology in all fields, as these crimes have become a threat to the information security of the state through threats and penetrations that affect the official data and information of countries and their destruction by cybercrime professionals, such as financial institutions, sensitive ministerial sectors.

in addition to attacks that affect the private lives of officials or individuals, especially on social networking sites, where cybercrimes have become or in the face of these threats and attacks, the state has worked to address these crimes through the creation of the National Authority for the Prevention of Crimes Related to Information and Communication Technologies, in addition to the National Penal Pole to Combat Crimes Related to Information and Communication Technologies.

Keywords: Cybercrime; Cyber Threats, Data Destruction, Criminal Pole.

1. INTRODUCTION

In the face of the emergence of the digital society today, which has made the world a small village that expresses its behaviors with the latest technologies in the field of information and communication, whether at the level of the state, individuals or organizations, especially in light of the use of artificial intelligence and the resulting negative consequences that affect the state and individuals, such as the use of drones by terrorist groups or transnational criminal organizations, whether in the smuggling of migrants illegally or in the photography of sensitive sites of the state and others. Cybercrimes committed through modern technologies, on the other hand, have facilitated services as they have become easily provided in a short period as a result of the digitization of the state's public utilities, in the face of the challenges facing the state in order to enhance the status of the citizen through his right to obtain information and high-quality public service.

On the other hand, the state and society have become under the threat of what is known as cybercrimes or high-risk cyberspace crimes, as a result of the negative use of computers by cybercrime professionals with the aim of harming the information security of the state through the destruction of information data as well as data, hacking and vandalizing websites, in addition to infringing on the privacy of individuals by defamation and defamation through social media sites, in the face of the successive cyber threats that resulted in the frightening spread of this type of crime, but the state has confronted the crimes. In order to strengthen these bodies, the Algerian legislature has created the National Penal Pole to combat crimes related to information and communication technologies, pursuant to Law No. 25-14 of August 3, 2025, which includes the Code of Criminal Procedure (GRn) No. 54 of August 13, 2025, which aims to strengthen the role of judicial authorities in combating cybercrime.

To study and analyze the subject, we start from the following problem:

How effective is the National Penal Pole in reducing ICT-related crimes?

1. The Concept of Cybercrime:

Cybercrime is one of the most dangerous and complex crimes introduced, due to its negative effects on the victim, whether it is an institution or individuals, as cybercrime differs from classic crime because its perpetrator is characterized by high intelligence, in a way that makes him control this criminal means easily and without discovering his matter, it does not leave any trace in the criminal act, unlike the classic crime, where the perpetrator can be easily discovered, and the size of the spread of cybercrime is due to the development Today, the enormous technology in the field of informatics, where state institutions and individuals have become competing for the use of modern technologies in what is known as the information society, this society that has become a threat to institutional security and the security of individuals through cybercrimes committed against them, so we find most of the legislations that kept pace with and confronted this type of crimes according to the capabilities of each country, and even reached the conclusion of cooperation agreements between countries to combat cybercrime, and the Algerian legislator, like other legislations, was keen to criminalize Prohibited use of computers, resulting in penalties for perpetrators of cybercrimes or cybercrimes, to protect the right of society to information security and the privacy of individuals.

1.1. Definition of Cybercrime:

The jurisprudential definitions regarding cyber or electronic crime or crimes related to automated data processing systems differed, according to the angle that each jurist looks at, and the same is true for legislation that usually leaves the issue of definitions to jurisprudence and the judiciary and its role is limited to referring to cybercrimes without defining them, since the definition is not the competence of the legislator, this is on the one hand, on the other hand, cybercrime is characterized by characteristics and characteristics that make it different from the rest of other crimes, but the crime Electronic devices are consistent with other crimes in terms of the elements on which the crime is based, which are the physical, moral and legal pillars, which are the pillars on which all crimes, whether traditional or

modern, are based.

1.2. Definition of Cybercrime:

There is no agreement on a single term to denote and express cyber or cybercrime, as there are those who call it cybercrimes, cybercrimes, crimes against automated data processing systems, computer crimes, and cybercrimes. The instability of one term is an indication of the breadth of the subject of cybercrime as a field of legal and social study, which is why jurisprudence did not settle on a unified definition, but the definitions differed according to each angle.

1.2.1. Jurisprudential Definition:

Jurisprudence defines it as any criminal activity in which computer technology is used directly or indirectly as a means or goal to carry out the intended criminal act (Hijazi Abdel Fattah, 2007: p. 20).

This definition is based on the means used to commit the crime, which is the computer, or the computer may be the target of the crime.

The researcher Muhammad Al-Shawa defined it as those criminal acts resulting through or through the use of modern information and technology represented by the computer or any of the electronic means (Al-Shawa, Muhammad Sami, 1994: p. 5).

It is the definition that is based on the means as a tool to commit a crime, and it may be the target, i.e. the target.

Abdel Fattah Murad defines cybercrime as "the set of illegal acts and acts that are carried out through electronic equipment, devices, or the Internet, or transmit their contents through it, which are those types of crimes that require special familiarity with computer technologies and information systems to commit, investigate and prosecute the perpetrators (Abdel Fattah Murad, Un Year: p. 40).

As for Algerian jurisprudence, it adopted the definition given by the Tenth United Nations Congress on the Prevention of Crime on computer crimes and networks, where it defined it as "any crime that can be committed by a computer system or a computer network, or within a computer system, and in principle it represents all crimes that can be committed in an electronic environment" (Bolahia Scheherazade, Khaloufi Rashid, 2019: p. 1974).

Crimes related to information and communication technologies, any role of the criminal justice in combating them, in the light of Law No. 25-14 of the Code of Criminal Procedure

The Law and Internet Conference held in Lisbon, Portugal, on 26/01/2001, stressed that it is necessary not to pay attention to inaccurate terminology to denote cybercrimes, and to use only the term "cyber crime" and not other terms (Abu Bakr bin Younis Muhammad, 2004, p. 158).

2.2.1. Legal Definition:

It is customary in the two laws that the definitions are within the jurisdiction of jurisprudence and the judiciary, and therefore the legislator usually avoids going into the definitions, but in the case of cybercrime, the legislator used the term crimes affecting the automated processing systems of data to express cybercrime, and this is evident through Law 09-04 of August 5, 2009, which contains the rules for the prevention and combating of crimes related to information and communication technologies, where it is stated in Article 2 of this law that "in the concept of this law, it is meant crimes related to technologies." Media and Communication: Crimes against automated data processing systems..."

Under Law No. 25-14 of 13 August 2025, which includes the Code of Criminal Procedure, the term "offences against automated data processing systems relating to public administrations and institutions" was used in Article 335 of the Code of Criminal Procedure, any offence committed or facilitated by the use of an information system, electronic communication system or any other means or mechanism related to information and communication technologies.

3.1. Characteristics of Cybercrime:

Cybercrime is distinguished from other traditional crimes by many features and characteristics that make it different in terms of its perpetrators, the consequences of committing it, and the means used for this purpose, as cybercrimes are national and cross-border crimes due to the multiplicity of perpetrators.

1.3.1 . Cybercrime is a transnational organized crime:

Due to the comprehensive coverage of the Internet and the Internet in all countries of the world, which has become just a small city or village due to the technological development in information technologies, communication between different countries and individuals in the world has

become rapid, which made communications and informatics beyond the borders of the country, and therefore it is easy to commit a crime in one country and its impact and perpetrators in another country, as borders are no longer an obstacle to cybercrimes, which made countries live A threat state that must be secured by putting

National and international legislation to combat cybercrimes, which has already happened through international cooperation between countries, such as the Budapest Convention of 2001 on cybercrime, although transnational cybercrimes raise the problem of the applicable law and the competent judicial authority.

2.3.1. Cybercrime is difficult to prove:

Cybercrime, being one of the fast-acting crimes due to the privacy of its perpetrators among the highly intelligent, in the case of committing cybercrime, the perpetrator quickly hides and erases its effects, unlike traditional crimes, where the perpetrator leaves physical traces through which the criminal is discovered, because most cybercrimes are not detected, and what is circulated represents only a few cybercrimes.

discovered by specialists, are usually followed by deception, destruction of programs, and the placement of passwords and codes that prevent access to the directory, and may also be encrypted (Tala Lamia, Salam Kahina, 2020: p. 75).

3.3.1 . The offender must be an information criminal:

Cybercrime is characterized by being an unusual crime, as its perpetrator is a person with sharp intelligence and is characterized by his ability to control computer technologies in a way that allows him to commit the crime easily, and thus he is able to block, penetrate and destroy any website, program or information system, and the cybercriminal is divided into:

1.3.3.1 Hackers:

They are the category of less dangerous criminals, as they have considerable experience in the field of computers, its functions, components, and information systems, and knowledge of programs that are taught such as accounting programs (Yaish Tammam Shawky, 2019, p. 22).

Crimes related to information and communication technologies, any role of the criminal justice in combating them, in the light of Law No. 25-14 of the Code of Criminal Procedure

Also called hackers are intrusive people, they often commit crimes out of defiance and entry into sites to prove themselves and are mostly teenagers.

2.3.3.1 Crackers – Professionals:

They are characterized by a great criminal danger compared to the first type, their goal may be to attack to earn money by entering banks and financial institutions, and the perpetrator may commit it with the aim of achieving political dimensions or putting forward a certain idea or direction, or it may affect other establishments and institutions, as this type of crime is committed by cybercrime professionals, and it is usually extremist, spy, or a system professional (Tala Lami, Salam Kahina, 2020: p. 73).

4.3.1 . For less violent and effortless cybercrime:

Cybercrime is different from traditional crime, as the first one does not require great efforts, but only needs a skilled and intelligent criminal who specializes in information technology who can commit any cybercrime in a very short period of time and without any effort, trouble, mobility or great capabilities, only relies on the strength of his intelligence and experience in the field of informatics to exploit it in committing cybercrime, for this is called a secured light crime.

4.1. Elements of Cybercrime:

Cybercrime, like other crimes, only provides for the availability of the elements of the crime agreed upon in criminal jurisprudence, which are the Shari'a element, the physical element, and the moral element.

1.4.1. Shari'ah Pillar:

The Shari'a pillar means that the legislator criminalizes a certain behavior and determines the punishment that suits it by stipulating the crime in the Penal Code, all within the framework of the principle of criminal legality, since the principle of permissible acts is permissible, but if an act becomes a danger to social security, then in this case, the legislator intervenes, criminalizes it and prescribes a punishment for it under the Penal Code, as the Penal Code stipulates in its first article "There is no crime and no security measure except by a legal text."

Therefore, the legal element of cybercrime is any criminal act

punishable by law that affects automated data processing systems.

2.4.1. Physical Corner:

The material element means the behavior that the offender comes to or refrains from doing that would cause harm to the victim, as criminal behavior in cybercrime is based on the physical act, the result, and the causal relationship.

Where physical behavior in cybercrime requires the availability of a digital or information environment and computer means where the offender is aware of the criminal behavior from its beginning until the result is achieved, for the preparatory work in cybercrime that precedes the criminal behavior, such as the purchase of equipment, tools and systems with the intention of using them in the commission of the crime, the law does not punish the purchase, but their use in the execution of the crime is on the lookout for the penal code in the event that it is used to penetrate or destroy information systems, although the Physical Behavior

In cybercrime, it raises questions as it is difficult to know the beginning and outcome of the behavior, due to the speed of the commission of cybercrime and the difficulty of proving it with physical evidence.

3.4.1. Moral Element:

The moral element or criminal intention refers to the direction of the offender's will to commit the crime, with the obligation to be aware of all its legal elements, because when the knowledge and will of the offender is achieved, the criminal intent is available (Abdullah Suleiman, 2005: p. 249).

Therefore, the achievement of the moral element in cybercrime is necessary to determine the criminal behavior and the applicable law, as the lack of the moral element leads to the crime of illegal entry and exit only, and therefore the moral element in cybercrime requires that the will of the offender be directed towards accessing the data or data stored in any computer.

2. Forms of Cyber Crimes Specified in the Penal Code and Related Laws:

In the face of the legal vacuum that Algerian legislation has identified in the fight against cybercrimes, the Algerian legislature has worked to

Crimes related to information and communication technologies, any role of the criminal justice in combating them, in the light of Law No. 25-14 of the Code of Criminal Procedure

develop more stringent legal texts related to the definition of cybercrimes and the penalties prescribed for them, whether in the Penal Code or in other laws, in accordance with Law No. 04-15 of November 10, 2004, amending and supplementing the Penal Code, which includes provisions for compromising automated data processing systems, pursuant to Law No. 04-15 of November 10, 2004, amending and supplementing Decree No. 66-165 of June 8, 1966, which includes Penal Code, Decree No. 71 of 10 November 2004. Law No. 09-04 of 09-04 of 5 August 2009 and Decree No. 47 of 16 August 2009 containing the rules for the prevention of crimes related to information and communication technologies.

1.2. Law No. 24-06 containing the Penal Code:

These offences are stipulated in Section VII bis of the Penal Code, under the title of Infringement of Automatic Data Processing Systems, in Articles 394 bis to 394 bis7.1.1.2. Entry and retention offence:

Determining the criminal behavior of anyone who enters or stays through fraud in all or part of the automated data processing system or attempts to do so, as the article approves a prison sentence from three months to one year, and a fine from 50,000 to 200,000 DZD, and the penalty is doubled if this results in the deletion or alteration of the system's data.

If the aforementioned acts result in sabotage of the system's operating system, the penalty shall be imprisonment from six (6) months to two (2) years and a fine from 50,000 to 150,000 DZD.

In the text of the article, the legislator talked about entering or staying in the information system without achieving the result, i.e., attempting to commit the crime, for which he approved the full penalty of the crime.

2.1.2.2 Crime against the Information System:

Anyone who fraudulently enters data into the automated processing system or fraudulently removes or modifies the data contained therein, which is intended to destroy and vandalize the data, as the authorized access to information systems is a deliberate crime punishable by law, while the law does not punish the entry by mistake (Bakhsh Hisham, 2017: p. 98). False data or modification of pre-existing data and information, punishable by imprisonment from six (6) months to three (3) years and a fine of 500,000

Crimes related to information and communication technologies, any role of the criminal justice in combating them, in the light of Law No. 25-14 of the Code of Criminal Procedure

DZD to 2,000,000 DZD according to Article 394 bis 1.

3.1.2. Crimes of designing, researching, collecting, possessing, or publishing data:

Any person who designs, researches, collects, provides, publishes, or trades in data stored, processed, or transmitted through an information system, in which the offences mentioned in this section may be committed.

Possess, disclose, publish, or use for any purpose the data obtained from one of the offences mentioned in this section. This means cyber viruses, hacking programs that are used against information systems or information data, according to Article 394 bis 2, which is punishable by imprisonment from two (2) months to three (3) years and a fine of 1,000,000 to 5,000,000 DZD.

2.2. Cybercrime under Law 09-04 containing the Special Rules for the Prevention and Combating of Crimes Related to Information and Communication Technologies:

In order to further protect the information and communication systems, Law No. 09-04 of 5 August 2009 was promulgated, which contains the rules for the prevention and combating of crimes related to information and communication technologies, as the law includes nineteen (19) articles, Article 2 of which defines crimes related to information and communication technologies, which are crimes of compromising the automated data processing systems specified in the Penal Code, and any other crime committed or facilitated by an information system or electronic communication system.

Article 2 also talks about the information system, which means any separate system or a group of interconnected or interconnected systems that process data mechanisms in order to implement a particular program.

Informatics also defines paragraph (c) of Article 2 as "any process of presenting facts, information or concepts in a form ready to be processed within an information system, including appropriate programs that would make an information system perform its function.

The second chapter of the Constitution also specifies the cases in which electronic surveillance is allowed, and in Article 4 of the Constitution,

surveillance operations can be carried out. In the event that there is information about the possibility of an attack on an information system in a manner that threatens public order, national defense, state institutions or the national economy.

2.3. Law No. 18-04 establishes the general rules relating to postal and electronic communications:

In accordance with Law No. 18-04 of May 10, 2018, the General Rules on Mail and Electronic Communications, Decree No. 27 of May 13, 2018, which is stated in Chapter 2 of Section 2 under the title of Electronic Communications, in Article 10, paragraph 3, Cybersecurity: a set of tools, policies, security concepts, security mechanisms, guidelines, methods of conducting risks, business training, good practices, safeguards and technologies that can be used to protect electronic communications against any event that may compromise to provide, secure and confidentially store data, process or transmit.

3. Competence of the National Penal Pole to Consider Cybercrimes:

Article 335 of the Code of Criminal Procedure 25-14 stipulates that the penal pole has national competence to combat cybercrimes, as this is part of the State's policy to confront organized crimes, especially cybercrimes, which have become a great danger as they affect the public security of the State in all its dimensions.

This institutional structure is a new addition to other bodies in charge of combating cybercrime, such as the National Authority for the Prevention of Crimes Related to Information and Communication Technologies (ICTs) introduced by Law 09-04.

This shows that the Algerian legislator is always keen on preventing and combating cybercrimes, and this is shown through the institutional development of the bodies competent to combat cybercrimes, as for the first time a penal pole specialized in cybercrimes has been created, thus it is considered a qualitative leap in the criminal judiciary.

3.1. Legal basis for the creation of the penal pole:

Crimes related to information and communication technologies, any role of the criminal justice in combating them, in the light of Law No. 25-14 of the Code of Criminal Procedure

In view of the multiplicity and diversity of organized crime that threatens the social security of the State and its institutions, due to its seriousness, of which cybercrime is one of its forms and the most prevalent today, it has become necessary for the Algerian state to confront cybercrimes and to fill the shortage of judicial bodies that have become incapable of dealing with this type of new crimes, which have become beyond national borders, whether in terms of their perpetrators or in terms of the effects of committing them and the losses that cost the state in this regard. Due to its peculiarities and its distinction from traditional crime, the Algerian legislature has prompted the creation of a national penal pole to combat crimes related to information and communication technologies, for the first time in Algeria. Pursuant to Decree No. 21-11 of 25 August 2021 on the Code of Criminal Procedure.

3.1.1.1. Legislative basis for the creation of the penal pole:

Referring to the provisions of Decree No. 21-11 of the Code of Criminal Procedure, which stipulates in article 211 bis 22 of the Code of Criminal Procedure, "A national penal pole shall be established at the level of the court of the headquarters of the Judicial Council of Algeria, specialized in the follow-up and investigation of crimes related to information and communication technologies and related crimes.

It shall also have jurisdiction to sentence the offences stipulated in this chapter if they constitute misdemeanours."

Thus, for the first time, the legislator has established a penal pole concerned with dealing with crimes related to information and communication technologies, given that they are one of the most widespread, serious and complex crimes, which necessitated the allocation of a penal pole to combat crimes related to information and communication technologies.

Article 32 of the Code of Criminal Procedure also emphasizes this, stating: "The court is the judicial body with general jurisdiction and is composed of sections that may also be composed of specialized poles."

Article 329, paragraph 5, emphasizes the local jurisdiction, which extends according to the case, stating that "the local jurisdiction of the court may be extended to the jurisdiction of other courts by way of regulation, in

Crimes related to information and communication technologies, any role of the criminal justice in combating them, in the light of Law No. 25-14 of the Code of Criminal Procedure

drug crimes, transnational organized crime, crimes against automated data processing systems, crimes against money laundering, terrorism, and crimes related to exchange legislation", which is further strengthened by article 211 bis 23.

2.1.3. Motives for the creation of the penal pole:

The Penal Pole is a judicial body that is competent to consider the crimes mentioned in Article 211 bis 24, and therefore this pole was created specifically to confront organized crime, especially cybercrimes, as it has become necessary to create this type of judicial body, to confront the threats facing the state and society with regard to crimes related to information and communication technologies, which have become the first rank in terms of crimes committed due to the ease of committing them and the difficulty of proving them. The National Penal Code is specialized in combating crimes related to information and communication technologies in terms of:

- The increasing volume of crimes related to information and communication technologies, which have become transnational crimes due to the tremendous technological development in information technologies.
- The complexity and difficulty of combating crimes related to information and communication technologies necessitated the creation of a penal pole to combat these crimes.
- The inability of the non-specialized criminal judiciary to confront crimes related to information and communication technologies, and thus to fight cybercrime, which requires a specialized judiciary with experience and efficiency, so that they can detect the perpetrators of the crime through the interrogation of the perpetrators, and therefore it has become necessary to rely on a criminal justice specialized in combating crimes related to information and communication technologies.
- The need to go beyond the regional jurisdiction of the courts that rely on it in traditional crimes, and work to accredit judicial bodies with national competence.
- The specificity, difficulty, and complexity of crimes related to information and communication technologies has made it possible for the legislature to consider them by allocating a more sophisticated judicial body in terms of

material and human resources to reduce these crimes, as the reality of these crimes has made it imperative for the state to intervene in a distinct manner and impose its punitive authority through the creation of the penal pole.

- The necessity of international cooperation between countries to combat cybercrimes prompted the legislator to create the National Penal Pole.

3.1.3. Advantages of the National Penal Pole:

The National Penal Pole for Combating Crimes Related to Information and Communication Technologies is characterized by several features that make it

It differs from the rest of the judicial bodies in terms of:

- In terms of nomenclature: the adoption of the term penal pole instead of a criminal court, and thus the legislator has succeeded in using the term penal pole, since the pole depends on specialization in its establishment.
- In terms of composition: The penal pole consists of a collective composition, a prosecutor, an investigative judge, and the head of the same pole.
- In terms of structure: The penal pole is a court established at the level of the headquarters of the Algerian Judicial Council to try crimes related to information and communication technologies.
- In terms of specialization: The National Penal Pole is solely responsible for combating crimes related to information and communication technologies.

2.3. Regional and Qualitative Jurisdiction of the National Penal Pole in Cybercrimes:

The National Penal Pole exercises its regional and specific competencies in accordance with Law 25-14 of the Code of Criminal Procedure, where the law grants the Penal Pole an expanded regional jurisdiction that includes the national territory, and this is due to the specificity of cybercrime and the inability of the courts to follow up on these crimes due to their diversity and multiplicity. To the National Penal Pole for Combating Crimes Related to Information and Communication Technologies.

3.2.1. Territorial jurisdiction of the National Penal Pole:

Law No. 04-14 defined the local jurisdiction of criminal magistrates as a

Crimes related to information and communication technologies, any role of the criminal justice in combating them, in the light of Law No. 25-14 of the Code of Criminal Procedure

general principle in Articles 37, 40 and 329 thereof, through which the local jurisdiction of the Prosecutor of the Republic, the investigating judge and the court was expanded to the jurisdiction of other courts, and this was later embodied through Executive Decree No. 06-384 Executive Decree No. 06-348 dated 05/10/2006 which includes the extension of the local jurisdiction of some courts, prosecutors of the Republic and investigative judges, C. No. 63, as amended by Executive Decree No. 16-267 dated 17/10/2016. IR No. 62, which specifies these courts.

In this context, Article 329, paragraph 1 of the Code of Criminal Procedure, states: "The court of the place of the crime or the court of residence of one of the defendants or their accomplices or the place of arrest shall have jurisdiction locally to hear the misdemeanor, even if such arrest is for another reason."

However, paragraph 5 of article 329 makes the exception that "the local jurisdiction of the Court may be extended to the jurisdiction of other courts by means of the regulation of drug crimes, transnational organized crime, crimes against automated data processing systems, money laundering crimes, terrorism and crimes related to exchange legislation.

This was exemplified by Executive Decree No. 06-348 of 05/10/2006 whereby four courts were established at the national level and their territorial jurisdiction was expanded.

It should be noted that the regional jurisdiction of the penal pole includes all stages of the public lawsuit until the issuance of the judgment to include the jurisdiction of other courts distributed among four regions of the country:

- Sidi Mohamed Court
- Constantine Court
- Oran Court
- Ouargla Court

In accordance with Articles 3.4.5 of Executive Decree No. 06-348 mentioned above, the jurisdiction of these courts extends to judicial councils according to this entire regional division to confront organized crime through penetration through leakage, eavesdropping, interception of

Crimes related to information and communication technologies, any role of the criminal justice in combating them, in the light of Law No. 25-14 of the Code of Criminal Procedure

communications, and taking pictures, but the standard of traditional regional jurisdiction does not apply to cybercrimes, as confirmed in Article 336 of the Law 25.14 "The Prosecutor of the Republic of the National Penal Pole competent to combat crimes related to information and communication technologies, as well as the investigating judge and the head of the same pole, shall exercise their powers throughout the national territory;

Thus, the National Penal Pole, which is responsible for combating crimes related to information and communication technologies, has national competence in the exercise of its powers, and this is an exception to the general rule that the jurisdiction is local, on the one hand, in addition to the devotion of the penal pole alone to the new crimes that are characterized by complexity and seriousness.

3.1.1.2.1 The case of the exclusive jurisdiction of the penal pole:

Referring to Article 337 of Law 25-14, which granted the exclusive jurisdiction of the National Penal Pole to combat crimes related to information and communication technologies .

3.2.1.2 The Status of the Joint Jurisdiction of the Criminal Pole to Combat Cybercrime

Article 340 of Law No. 25-14 stipulates, without prejudice to the provisions of articles 337 and 338 above, that the prosecutor of the National Penal Pole for the Fight against Crimes Related to Information and Communication Technologies, as well as the investigating judge and the head of the same pole, shall exercise common jurisdiction with the jurisdiction resulting from the application of articles 37, 40 and 329 of this Code.

The specificity of the crimes related to automated data processing systems necessitated the need for joint action between the prosecution and investigation authorities and the head of the same penal pole.

3.2.1.3 Status of Compulsory Jurisdiction:

In the event that the competence of the National Penal Pole to combat crimes related to information and communication technologies coincides with the competence of the Economic and Financial Pole, in this case the competence shall vest in the latter.

The same is true of the competence of the National Penal Pole to combat

Crimes related to information and communication technologies, any role of the criminal justice in combating them, in the light of Law No. 25-14 of the Code of Criminal Procedure

crimes related to information and communication technologies with the jurisdiction of the Court of the Headquarters of the Judicial Council of Algiers.

In accordance with Article 341 of Law No. 25-14, in this case, jurisdiction must be vested in the National Economic and Financial Penal Pole.

3.3. Specific jurisdiction of the penal pole:

Specific jurisdiction is determined as a general rule on the basis of the type of crime and the amount of punishment prescribed for it according to articles 5-27 of the Penal Code, whether it is a felony, misdemeanor or violation, but the specific jurisdiction of the penal pole is determined by the crimes mentioned exclusively in article 337 . provided in this chapter if they constitute misdemeanors.

Article 338 of Law 25-14 states: "Subject to the provisions of article 335, paragraph 2, above, the Prosecutor of the Republic at the National Penal Pole for Combating Crimes Related to Information and Communication Technologies, the investigating judge and the head of the same pole shall have exclusive competence to follow-up, investigate and adjudicate the crimes related to the information and communication technologies mentioned below, as well as the crimes related thereto:

- Crimes that affect State security or national defense;
- Crimes of spreading and promoting false news among the public that may harm the security, public tranquility or stability of the community;
- Offences of dissemination and dissemination of malicious news affecting public order and security of an organized or transnational nature;
- Crimes of compromising automated data processing systems related to public administrations and institutions;
- Crimes of trafficking in persons or human organs or smuggling of migrants;
- Crimes of discrimination and hate speech;

In addition to the crimes specified in Article 337 , the Prosecutor of the Republic at the National Penal Pole for Combating Crimes Related to Information and Communication Technologies, as well as the investigating judge and the head of the same pole, shall be exclusively responsible for the

Crimes related to information and communication technologies, any role of the criminal justice in combating them, in the light of Law No. 25-14 of the Code of Criminal Procedure

follow-up, investigation and adjudication of crimes related to the most complex information and communication technologies and related crimes, which means a crime that is committed in view of the multiplicity of actors, accomplices or victims, or due to the geographical area of the place where the crime was committed, the gravity of its effects, the damage caused therefrom, or the nature of the crime. Transnational organization or its violation of public order and security, where it requires the use of special investigative methods, specialized technical expertise, or recourse to international judicial cooperation.

3.4. Special Rules on Follow-up and Investigation:

The Code of Criminal Procedure assigned the task of follow-up, investigation and adjudication of crimes related to information and communication technologies to the Penal Pole, which alone through the Public Prosecution, the investigating judge and the head of the same pole is to follow up on the file from the public case until the issuance of the verdict.

3.4.1 Jurisdiction of the Prosecutor of the Republic:

Article 337 of Law No. 25-14 entrusts the Prosecutor of the Republic at the Penal Pole with the jurisdiction to consider crimes related to information and communication technologies, where the Prosecutor of the Republic is responsible for sending expert reports and investigating the crimes stipulated in Article 337 before the competent judicial authorities in the region.

The Public Prosecutor at the Penal Pole shall receive the reports of the expertise and investigation carried out by the Judicial Enforcement Service in the crimes stipulated in Article 337 of the Code of Criminal Procedure.

The Prosecutor of the Republic can request the file of the proceedings through all stages of the public lawsuit .

In the event that the Public Prosecutor at the Criminal Pole requests a request for the file of the proceedings, the Prosecutor of the Republic in respect of the former may issue a decision to abandon in favor of the former, during the stages of preliminary investigation and follow-up in accordance with Article 324 of the Code of Criminal Procedure. However, if the Prosecutor of the Republic finds that the reported facts do not fall within his

Crimes related to information and communication technologies, any role of the criminal justice in combating them, in the light of Law No. 25-14 of the Code of Criminal Procedure

jurisdiction, he shall issue a decision to abandon in favor of the Prosecutor of the Republic competent regionally .

The National Penal Pole for Combating Crimes Related to Information and Communication Technologies (ICTs) was notified of 72 files during the year 2020-2021.

3.4.2.Competence of the investigating judge:

In accordance with Article 325 of the Code of Criminal Procedure, in the event of the opening of a judicial investigation, the petitions of the Public Prosecutor shall be referred to the National Penal Pole for the Prevention of Crimes Related to Information and Communication Technologies, including the request for the file of proceedings by the Prosecutor of the Republic, in which case the investigating judge shall issue an order to abandon the investigative judge at the National Penal Pole for the Prevention of Crimes Related to Information and Communication Technologies.

According to Article 327 of the Code of Criminal Procedure, and in order to achieve the necessary guarantees, the arrest warrants and orders for placing them in temporary custody shall remain productive until a contrary order is issued by the investigating judge of the penal pole, who shall ensure the validity of the procedures.

4. CONCLUSION

In conclusion, cybercrime appears to be one of the most serious, complex and widespread crimes, due to its specificity and the experience of the perpetrators of these crimes with information and communication technologies, in addition to its transgression of national borders, it has become necessary for the state to develop legislative and institutional frameworks to reduce or reduce these crimes, which requires the intensification of national efforts through coordination between the various judicial and security agencies of the state, in addition to international efforts for the purpose of cooperation between countries, whether in the field of training or the fight against crime, which has already been embodied through the establishment by the legislature of a national penal pole to combat crimes related to information and communication technologies as a body that supports ordinary courts and the National Authority for the Prevention of

Crimes related to information and communication technologies, any role of the criminal justice in combating them, in the light of Law No. 25-14 of the Code of Criminal Procedure

Crimes related to information and communication technologies in the fight against cybercrime.

It is clear that cybercrime is a complex, dangerous, fast-paced, and difficult crime to prove, in addition to being one of the transnational crimes, as it is characterized by characteristics that differ from traditional crimes, as it has reached the point of not setting a unified definition of it, and in order to combat it, the state has harnessed material and human resources for this as it affects the public order of the state and the private life of individuals, for this reason the legislator has increased the punishment for the perpetrators of crimes related to information and communication technologies, this is shown through the amendments of the Penal Code. On the other hand, the legislator worked to establish the National Penal Pole to combat crimes related to information and communication technologies, as a pole specialized in cybercrime, as the legislator granted it national jurisdiction to confront these crimes, and its collective composition consists of a public prosecutor, an investigative judge, and the head of the same pole. Among the most important recommendations we make in this topic are:

- The need to establish regional penal poles to combat crimes related to information and communication technologies, given the rapid spread of these crimes.
- Expanding the composition of the members of the National Penal Pole, as the latter alone is unable to confront cybercrime through this formation, by including experts in informatics in the composition of the court as assistants to the judiciary.
- The need to establish independent structures for the specialized national penal pole, rather than just the seat court of the Council.
- Good training of judges in the field of informatics to qualify them to handle cases easily.
- The need to spread cyber awareness through forums and study days for the benefit of students in framing and organizing the penal pole.
- Determining the priority area of intervention of the National Penal Pole to combat crimes related to information technologies and communication with the Financial and Economic Penal Pole in financial and economic crimes

committed through computers.

5. Bibliography List :

Books and articles:

- Hijazi Bayoumi Abdel Fattah, Computer and Internet Crimes in the Arab Model Law: An In-Depth Legal Study in Information Law, Dar Al-Kutub Al-Qanuniyya, Dar Dittat for Publishing and Software, Egypt, 2007.
- Mohamed Sami Al-Shawa, The Information Revolution and its Implications on the Penal Code, Dar Al-Nahda Al-Arabiya, Cairo, 1994.
- Abdel Fattah Murad, Explanation of Computer and Internet Crimes, without the publishing house, without the year of publication.
- Boulahia Scheherazade, Khaloufi Rachid, The Challenges of Cybercrime in Algeria, Journal of the Research Professor for Legal and Political Studies, Vol. 4, No. 02, 2019.
- Omar Muhammad Abu Bakr Bin Younis, Crimes Arising from the Use of the Internet, Substantive Judgments and Procedural Aspects, First Edition, Dar Al-Nahda Al-Arabiya, Cairo, 2004.
- Lamia Tala, Kahina Salam, Cybercrime, A New Dimension of the Concept of Criminality through Social Media Platforms, Al-Riwaq Journal for Social and Humanitarian Studies, Volume 6, Issue 02, 2020.
- Yahy Tammam Shawky, Cybercrime, A Comparative Original Study, Laboratory of the Impact of Judicial Jurisprudence on the Legislative Movement, Mohamed Khidir University, Biskra, First Edition, 2019.
- Abdallah Suleiman, Explanation of the Algerian Penal Code, Crime, General Section, Diwan of University Publications, Algeria, 2005.
- Bekhoush Hicham, Crimes Related to Information and Communication Technologies under Algerian Legislation, Journal of Law and Political Science, University of Khenchela, No. 07, January 2017.

Legal Texts:

- Law No. 25-14 of 3 August 2025, supplementing Ordinance No. 66-155 of 8 June 1966 containing the Code of Criminal Procedure, Decree No. 54 of 13 August 2025.

Crimes related to information and communication technologies, any role of the criminal justice in combating them, in the light of Law No. 25-14 of the Code of Criminal Procedure

- Law No. 24-06 of 08 June 2024, amending and supplementing Ordinance No. 66-165 of 8 June 1966, incorporating the Penal Code, Decree No. 30 of 30 April 2024.
- Law No. 09-04 of 5 August 2009 on the Special Rules for the Prevention of Crimes Related to Information and Communication Technologies, Decree No. 47 of 16 August 2009.
- Law No. 18-04 of 10 May 2018 defining the general rules on postal and electronic communications, Decree No. 27 of 13 May 2018.
- Executive Decree No. 06-348 of 05/10/2006 extending the domestic jurisdiction of certain courts, prosecutors and investigative judges, c. No. 63, as amended by Executive Decree No. 16-267 of 17/10/2016, G.R. No. 62.

Websites

<https://elmaghrebelwassat.dz> Date of visit: 02 February 2021 10:30 pm