# The National Criminal Pole to combat Offenses Linked to Information and Communication Technologies as a New Body in the Algerian Judicial System

# القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال كجهاز جديد في النظام القضائي الجزائري

**Assaad LAMAMRI**
**Mouloud MAMMERI University**
**a.lamamri@yahoo.fr**

**Khaled KHELOUI**
**Mouloud MAMMERI University**
**khelouikhaled@yahoo.fr**

**Date of submission:03/01/2023 Date of final acceptance:18/05/2023 Date of publication :June 2023**

**Abstract :**

The Algerian legislator has established the long-awaited national criminal pole to fight offenses linked to information and communication technologies. The new judicial body has jurisdiction, both over offenses against automated data processing systems and ordinary offenses committed or the commission of which is facilitated by the use of Information and Communication Technologies. Owing to a possible jurisdictional overlap between the new judicial body and other criminal judicial bodies, the Algerian legislator has conferred on the former, on the one hand, an exclusive jurisdiction over some cybercrime offenses and on the other hand, a concurrent jurisdiction with that resulting from the application of the articles 37, 40 and 329 of the code of criminal procedure.

**Keywords :** Cybercrime, national criminal pole, exclusive jurisdiction, concurrent jurisdiction.

**ملخص:**

أنشأ المشرع الجزائري، بعد طول انتظار، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال. يختص الجهاز القضائي الجديد بالنظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والجرائم العادية التي ترتكب أو يسهل ارتكابها باستعمال تكنولوجيات الإعلام والاتصال. بالنظر إلى التداخل المحتمل للاختصاص بين الجهاز القضائي الجديد والأجهزة القضائية الجزائية الأخرى منح المشرع الجزائري اختصاصا حصريا لهذا الأخير بشأن بعض الجرائم الإلكترونية هذا من جهة، ومن جهة أخرى منح له اختصاصا مشتركا مع الاختصاص الناتج عن تطبيق المواد 37، 40 و 329 من قانون الإجراءات الجزائية.

**الكلمات المفتاحية:** الجريمة الإلكترونية، القطب الجزائي الوطني، الإختصاص الحصري، الإختصاص المشترك.

**Auteur correspondent: Assaad LAMAMRI**

## Introduction:

The criminal law is now dealing with a new space, namely cyberspace, in which the growing international scourge of cybercrime develops. The latter constitute a greatest threat, not only to the individuals or institutions but also to the security and stability of the state; it is considered "the third greatest threat to the great powers, after chemical, bacteriologic and nuclear arms"[1].

Being conscious of this reality and the increasing openness of Algeria's society to the information and communication technologies the Algerian legislator, although late compared with the other Arab countries, have legislated, for the first time, on the cybercrime in 2004. Indeed, under the Act No. 04-15 of 10 November 2004[2], the legislator supplemented the penal code through a new section entitled "attacks on data automated processing systems" which include the article 394 bis to article 394 bis 7.

However, since these amendments cover only the offenses against the computer systems either interconnected or not with a telecommunications network and not cover all the cybercrime forms, the Algerian legislator has issued the Act No. 09-04 of 5 august 2009[3] in which the cybercrime scope, under the umbrella of "Offenses Linked to Information and Communication Technologies", has been expanded to include any offense committed or facilitated through either computer system or electronic communication system[4].

Furthermore, in consideration of the fact that the Algerian legislator has adopted a policy of specialized criminal jurisdictions to deal with the dangerousness and complexity of certain offenses[5], such as terrorism offenses, transnational organized offense and corruption offenses, they established The National Criminal pole to combat Offenses Linked to Information and Communication Technologies (Hereafter referred to as the national criminal pole) which are of equal importance to the aforementioned offenses. As long as this judicial body is the latest one created by the Algerian legislator, the question arises about its legal framework.

Accordingly, this research paper aims to study the context in which the National Criminal pole is created (SECTION I), the offenses over which it has jurisdiction (section II) and its relations with other criminal jurisdictions (section III).

## 1 - The National Criminal Pole as the Culmination of Panoply of Measures Adopted to Combat Cybercrime

Since the inception of its counter-cybercrime effort, the Algerian legislator has established various measures for efficacious fight against the cybercrime phenomena through the institutional measures (A), the preventive and investigative measures (B) and finally the creation of the national criminal pole (C).

### 1 – 1 The Institutional Measures for Combating Cybercrime

The institutional measures consisting of the courts with extended territorial jurisdiction (1) and the national organ for the prevention and fight against Offenses Linked to Information and Communication Technologies (Hereafter Organ) (2).

#### 1 – 1 - 1 The Courts with Extended Territorial Jurisdiction as Judicial tool to Combat Cybercrime

Having regard to the specificity of certain offenses, including cybercrime offenses, money laundering, terrorist offenses and transnational organized offense, the Algerian legislator has inserted, under the Act No. 04-14[6], new provisions to article 37, 40 and 329 of the code of criminal procedure according to which it allowed to extend, on regulatory basis, the territorial jurisdiction of the public prosecutors, the investigating judges and the trial judges of some courts of first instance to include the judicial district of other courts. On this basis, the territorial jurisdiction of the court of Sidi M'Hamed, the court of Constantine, the court of Ouargla and the court of Oran has been expended[7].

It is worth noting that the offenses committed against computer systems, interconnected or not, within the meaning of articles 394 bis *et seq*. of the penal code, are the only offenses that fall within the jurisdiction of the courts with extended territorial jurisdiction, that is to say that ordinary criminal offenses committed by means of information and communication technologies fall under the jurisdictional scope of the ordinary courts like other ordinary offenses.

Notwithstanding the application of the ordinary procedural rules regarding the criminal proceedings, judicial investigation and the trial before the courts with extended territorial jurisdiction, there is a special procedural process to which the offenses against the automated processing data systems are subjected. Indeed, when the judicial police officers proceed with a preliminary investigation in respect with the aforementioned offenses, they shall notify the public prosecutor territorially competent immediately and transmit to him, or her, the original and two copies of the investigation procedure. The second copy is transmitted, without delay, by the above-named public prosecutor to the public prosecutor within the court with extended territorial jurisdiction concerned[8]. If the latter considers that the relevant offense falls under the meaning of the offenses against the automated processing data systems he or she claims, on the advice of the general attorney within the court of appeal concerned, the proceedings immediately[9].

Except for the phase of the trial and upon the opinion of the general attorney within the appellate court concerned, the aforementioned public prosecutor may claim the file

of the proceedings at any other phase of the criminal proceedings, *i.e.*, the preliminary investigation, the prosecution and the judicial investigation[10].

At any rate, until the decision on the arrest and pretrial detention orders, already issued by the investigating judge within the ordinary court concerned, has been taken by the court with extended territorial jurisdiction concerned and subject to the provision of the articles 123 *et seq* of the Algeria's code of criminal procedure, the decision for the relinquishment of the file of the proceedings taken by the former in favor of the later does not affect the enforceability of these orders[11].

**1 – 1 – 2 The National Organ for the Prevention and Fight Against Offenses Linked to Information and Communication Technologies**

For the purposes of leading and coordinating operations for the prevention and fight of information and communication technologies-related offenses; assisting judicial authorities and judicial police services with regard to the investigations carried out by them; and strengthening international cooperation to identify and localize the authors of the aforementioned offenses, a new national body specialized in preventing and combating information and communication technologies-related offenses, under the name of National Organ for the Prevention and Fight Against Offenses Linked to Information and Communication Technologies, is created in accordance with article 13 of the Act No. 09-04[12] as an independent administrative authority under the president of the republic with legal personality and financial independence[13].

In order to ensure its functioning, the new organ receives services of seconded public officers, namely magistrates, authorized judicial police officers and agents of military security services, gendarmerie, and the national police the number of which is determined jointly by the minister of national defense, minister of the interior, and the secretary-general of the presidency of the republic, and technical and administrative support staff of military security services, gendarmerie, and the national police[14]. The organ may also recruit other staff categories, according to need. Before their installation the organ's staff members that called to access to confidential information take an oath within the terms referred to in article 22 of the Presidential Decree No. 21-439[15], on the one hand, on the other hand, They are subject to the obligation to maintain professional secrecy[16].

Within the framework of cooperation, the organ may request any necessary document or information for the performance of the tasks entrusted to it from anybody, institution and department[17].

**1 – 2 The Preventive and Investigative Measures to Combat Cybercrime**

Owing to the peculiarity of the electronic offenses, it was necessary to adopt measures more

suitable for the prevention, investigation and prosecution of these offenses. Accordingly, the Algerian legislator has allowed using electronic surveillance (1), search computer systems and seizure data stored within them (2), and imposed obligations on service providers (3).

**1 – 2 – 1 The Electronic Surveillance as a Necessary and Exceptional Measure**

Although the Algerian legislator has not defined the electronic surveillance, they have determined the meaning of the electronic communications as the subject of such surveillance by defining it as "any transmission, emission or reception of signs, signals, writing, images, and sounds or intelligence of any nature by any electronic means"[18], on the one hand, on the other hand, they provided other elements of the this kind of surveillance consisting of the outcome of the latter, namely gathering and recording in real time the contents of the electronic communications, and the use of the technical devices for implementing it[19].

Consequently, we can define the electronic surveillance as the acquisition by surreptitious use of electronic devices of the contents of any electronic communications carried over both wired and wireless systems[20], "thus suggesting that the surveillance… includes more than simply intercepting the verbal contents of some communication"[21]. It includes, *i.e.,* bugging[22], which means "the interception of oral communication by concealed microphones"[23], "videotaping, geolocation tracking such as via RFID, GPS, or cell-site data; data mining, social media mapping, and the monitoring of data and traffic on the Internet"[24].

In order to strike a balance between the confidentiality requirements of the correspondences and communications; the protection of public order and the needs of ongoing preliminary investigations and judicial investigations, the electronic surveillance has been subjected to a legal framework the rules of which are stemmed from the code of criminal procedure and more especially the Act No. 09-04. According to the latter the surveillance falls into two categories: preventive and investigative electronic surveillance.

The electronic surveillance may be carried out either preventively when there is information on a probable attack against computer systems, which present threat to the public order, national defense, state institutions or national economic or for the purposes of the detection of possible terrorist and subversive offenses, or offenses against the state security[25]. For the needs of the preliminary and judicial investigation relevant to any other offenses related to information and communication technologies the surveillance can also be performed, provided that there is difficult to reach a result in respect with ongoing investigations without using the electronic surveillance[26].

Moreover, it is allowed to use the latter in the framework of the execution of international mutual legal assistance requests[27].

For the purposes of the judicial review of the electronic surveillance operations, the judicial police officers only use such operations upon written authorization, which include all the items allowing to identify the communications and the places in question, the offenses concerned and the duration of the operation, issued either by the public prosecutor territorially competent during the preliminary investigation or the investigating judge when a judicial investigation is opened[28], for up to 4 months renewable according to the needs of the preliminary or judicial investigation and under the same conditions[29].

However, when the electronic surveillance takes aim at terrorist and subversive offenses or offenses against the state security, the authorization relating thereto is issued by the general attorney within the Algiers court of appeal to the judicial police officers belonging to the organ for 6 months renewable on the basis of a report specifying the nature of the used technical process and its objectives. Subject to the penalties provided by the Algeria's penal code with regard to the offenses against the privacy of others, this technical process must be aimed only at gathering and recording data in relation to the prevention of terrorist acts and attack against the state security[30].

**1 – 2 – 2 Electronic Search and Seizure**

The systematization of the use of the digital tools has leaded to the inclusion by all subjects of law of considerable personal data in digital files, which are materially stored in various electronic devices[31] such as flash drives, hard disk drives and optical disks or remote storage servers, which may be located in the same place as one's premises, another place in national territory or another country[32]. Consequently, it is very important for the investigator in accessing to the computer from which he or she can read the relevant document because the access to the storage server premises do not allow him or her to read the data content. Hence, the access to the data storage systems constitutes an essential phase in the criminal investigation[33] regarding computer-related offenses.

Being conscious of this reality, the Algerian legislator allows, in accordance with the code of criminal procedure and in the cases provided for in the article 4 of the Act No. 09-04, both the competent judicial authorities, such as the investigating judge and the judicial police officers to access, for the purposes of search, to a computer systems or part of them, as well as the computer data stored on them and a computer storage systems[34]. It appears that the electronic search takes aim not only at data stored in the computer systems based in the places where the search is carried out but also at data stored in a remote computer system[35] situated outside the premises to be searched, but

on the national territory[36], provided that these data are accessible from the initial system that may be the former or the system based in judicial police premises.

However, such legal extension of the search warrant scope is confined to the prevention from the terrorist and subversive acts and offenses against the state security as a case referred to in article 4 of the Act No. 09-04. The paragraph 2 of the article 5 of the latter specified that when there are reasons to believe that the data sought are stored in the remote system and is accessible to it through the initial system, the search may be extended quickly to the remote system or a part of it once the competent judicial authority has been informed.

Moreover, when it previously found[37] that the data sought, accessible through the initial computer system, are stored in another system situated overseas, they are collected by the competent judicial authorities or the judicial police officers with the support of the competent foreign authorities in conformity with the relevant international agreements and the reciprocity principle[38].

Subject to the integrity of the data, when the authority carrying out the electronic search discovers a stored data, which are useful for investigative purposes, it copies these data as well as those that are necessary for understanding their to a computer-data storage medium which can be seized and sealed under the conditions laid down in the Algeria's code of criminal procedure[39]. Nonetheless, if the aforementioned authority is, for technical reasons, unable to proceed with the seizure under the above mentioned proceedings, it must use adequate techniques for the ban on access either to the data stored in the computer system or the copies of them that are available to the users of this system[40].

### 1 – 2 – 3 Obligations of the Service Providers

The service providers, which is defined as any public or private entity that provides to users of its service the ability to communicate by means of a computer system and/or telecommunication system; and any other entity that processes or stores computer data on behalf of such communication service or users of such service[41], commits to provide assistance to the authorities charged with judicial inquiry for collection and recording of the data in real-time associated with the communication contents[42].

Furthermore, the service providers make available to such authorities the traffic data[43] about which they are required to preserve for one year from the recording date. These data consist of the users' information, communication's origin, destination, route, time, date, size, duration or type of underlying service, the data related to terminal equipments of the used communications and the data concerning the required or used additional services and their providers[44].

In addition to the above-mentioned obligations, the internet service providers are required to intervene, without delay, for removing the data to which they permit the access and storing or making them inaccessible, as soon as they were, directly or indirectly, aware of a violation of law; and to set up technical measures limiting accessibility to distributors containing information contrary to the public order or morality and inform subscribers[45].

### 1 – 2 – 4 The Creation of the National Criminal Pole

In accordance with paragraph 1 of the article 211 bis 22 of the Algeria's code of criminal procedure, thus amended pursuant to ordinance No. 21-11 issued on august 25, 2001[46], a national criminal pole has been established within the tribunal sitting at the chief tower of Algiers court of appeal, charged with the prosecution and judicial investigation of the offenses linked to information and communication technologies and the related-offenses. It has also jurisdiction to try of such offenses when they constitute misdemeanors[47].

Put another way, when the investigating judge at national criminal pole considers that the offense concerned constitutes a felony, he or she issued an order to forward forthwith the proceedings file and exhibits, through the public prosecutor, to the general attorney within the Algiers court of appeal[48], who subject the case attached with his or her requests to the indictment pole[49]. When this pole considers that the conduct constitutes an offense qualified by the law as a misdemeanor it refers the accused to the national criminal pole[50], but if the conduct constitutes a felony the accused is referred to the criminal tribunal of first instance at the level of the Algiers court of appeal[51].

Owing to the national character of the new judicial body, the scope of the territorial jurisdiction of the public prosecutor, the investigating judge and the president within this body includes the entire national territory[52]; otherwise, these judges have a statewide jurisdiction. The general attorney within the Algiers court of appeal exercises hierarchical authority over the public prosecutor when he or she performs his or her prosecution powers provided by the code of criminal procedure in matters falling within his or her jurisdiction. As regards the investigating judge and the president of the national criminal pole, they are administratively subject to the Algiers court of appeal authority[53].

## 2 - The National Criminal Pole Subject-Matter Jurisdiction

Although the offenses linked to information and communications technologies include the attacks on automated data processing systems and ordinary offenses committed by means of information and communication technologies[54], the paragraph 3 of the article 211 bis 22 of the Algeria's code of criminal procedure limits the

jurisdiction ratione materiae of the national criminal pole to this latter category of offenses. Indeed, this paragraph defines the offenses linked to information and communications technologies as "any offenses committed or the commission of which is facilitated by the use of a computer system or an electronic communication system or by any other means or process related to information and communication technologies".

In consideration of the fact that article 211 bis 24 of the code of criminal procedure refers to the offenses against automated data processing systems related to administrations and public institutions as offenses falling within the national criminal pole exclusive jurisdiction, we consider nevertheless that the Algerian legislator has unintentionally omitted to refer to the attacks on automated data processing systems in above-mentioned paragraph 3.

Hence, the jurisdiction ratione materiae of the national criminal pole includes both the offenses against automated data processing systems (A) and ordinary offenses committed by means of information and communications technologies (B).

**2 – 1 Offenses Against Automated Data Processing Systems**

In accordance with the amendment of the Algeria's penal code in 2004[55], the attacks on automated data processing systems are criminalized as follows:

**2 – 1 – 1 Offense of Illegal Access**

Unauthorized access to the computer system constitutes the basic offense of dangerous attacks against the confidentiality, integrity and availability of computer systems and data. The mere illegal intrusion in the form of hacking, cracking or computer trespass may give access to secrets and confidential data, inter alia, passwords and information regarding the targeted system, to the use of the system concerned without payment or even encourage hackers to commit more dangerous forms of cybercrime offenses, such as computer-related fraud and forgery[56].

Accordingly, the Algeria's code penal criminalizes the act of fraudulently accessing or staying in the whole or any part of an automated processing data system, *i.e.*, hardware, components, stored data of the system installed, directories, traffic and content-related data[57] or attempting to commit these acts and establishes penalties of 3 months to 1 year imprisonment and a fine of DA 50,000 to DA 100,000[58]. It also criminalizes interference with computer data and system by providing that the penalty shall doubled when the aforementioned acts has resulted in the deletion or alteration of the computer data and by establishing penalties of 6 months to 2 years' imprisonment and a fine of DA 50,000 to DA 150,000 when such acts has led to the sabotage of the computer system functioning[59].

### 2 – 1 – 2 Offense Against the Integrity of Data Processed Automatically

In order to protect the integrity of data contained in the computer systems, Algeria's penal code criminalizes any fraudulent input, alteration or deletion of computer data, regardless of whether or not such acts resulting in computer-related forgery or fraud, and establishes a penalty of 6 months to 3 years' imprisonment and a fine of DA 500,000 to DA 2,000,000[60].

### 2 – 1 – 3 Dealing with Illegal Data

As the commission of the offenses referred to in articles 394 bis and 394 bis 1 of the Algeria's penal code generally requires the perpetrators to have the means of access and other tools, there is a strong need to obtain them by the perpetrators, which may then result in the appearance of "a kind of black market in their production and distribution"[61]. Hence, the criminal legal texts should criminalize unlawfully making available devices and data for the commission of these offenses[62]. In this regard the article 394 bis 2 of Algeria's penal code provides that any person who intentionally and fraudulently designs, searches, gathers, makes available, distributes or markets data stored, processed or transmitted by a computer system, and through which the above-mentioned offenses may be committed, is liable to imprisonment for a term of between 2 months and 3 years and to a fine of DA 1,000,000 to DA 5,000,000.

Moreover, the article 394 bis extends the criminalization to include the possession, disclosure or the use for any purpose of data obtained from the above-mentioned offenses and establishes the above-described penalties.

### 2 – 2 Offenses Against Automated Data Processing Systems

The second list of offenses that fall within the subject-matter jurisdiction of the national criminal pole consists of ordinary offenses that already existing before the arrival of the internet, but the latter has provided an environment conductive to their perpetuation and development. In this regard, the existing child pornography is the most notable example of the ordinary offenses that have gathered momentum through the evolution of the internet[63].

The definition of the ordinary offenses must sufficiently be broad to cover the situations involving computer systems or network and therefore when the definition does not already include such situations, there is necessary to amend it or enact new offenses[64]. Accordingly, some ordinary offenses in the Algerian law may be committed by the use of computer systems or network. In this respect, the Algeria's code of criminal procedure qualifies certain ordinary offenses as offenses linked to information and communications technologies, i.e., the offenses against state security and national defense such as terrorism offenses, the offenses related to the dissemination and propagation within the public of false information likely to disturb the public security

and peace or stability of society, the organized or transnational offenses related to the dissemination and propagation of slanderous information affecting the public order and security, the offenses related to trafficking in persons or human organs or smuggling of migrants and the offenses related to discrimination and hate speech[65].

It is important to note that the jurisdiction ratione materiae of the national criminal pole may include not only the computer-related offenses and offenses against automated data processing systems of less complexity but also the highly complex ones. In order to determine what the criterion "highly complex" implies, the Algeria's code of criminal procedure has established several elements that require the use of special investigative techniques, specialized expertise or the recourse to international judicial cooperation. Having regard to article 211 bis 25 of the code of criminal procedure, these elements are as follows[66]:

**2 – 2 – 1 Element of Multiplicity**: it means that the Offenses Linked to Information and Communications Technologies have been the product of a criminal participation either because of the multiplicity of offenders or accomplices. It means also that such offenses have caused harm to more than one person.

**2 – 2 – 2 Geographic Element:** it means that the Offenses Linked to Information and Communications Technologies have been committed on a large scale of the national territory or involve more than one country in their planning, execution or impact; In that case, such offenses may be qualified as "transnational offenses".

**2 – 2 - 3 Element of Dangerousness:** assessment must be focused here on the gravity of the consequences that result from the commission of Offenses Linked to Information and Communications Technologies.

**2 – 2 - 4 Element related to the Organized Character of the Offenses:** it means that the Offenses Linked to Information and Communications Technologies, which are punishable by at least four years or a more serious penalty, have been committed by "structured group of three or more persons, existing for a period time and acting in concert with the aim of committing" these offenses, "in order to obtain, directly or indirectly, a financial or other material benefit"[67]. When the offenses have a transnational character and involve organized criminal group, they may be qualified as "transnational organized offenses".

**2 – 2 - 5 Element related to Public Order and Peace:** it means that the Offenses Linked to Information and Communications Technologies have prejudiced to public order and peace.

### 3 - The Jurisdictional Relationship Between the National Criminal Pole and Other Criminal Judicial Bodies

Owing to the possible overlap between the jurisdiction of the national criminal pole jurisdiction and that of other criminal judicial bodies, the Algerian legislator has divided the jurisdiction between them by adopting two jurisdictional concepts that consist of exclusive jurisdiction (A) and concurrent jurisdiction (B).

### 3 – 1 The National Criminal Pole's Exclusive Jurisdiction

Subject to paragraph 2 of the article 211 bis 22 of the Algeria's code of criminal procedure, which allows the national criminal pole not only to prosecute and judicially investigate the cybercrime offenses that constitute misdemeanors but also to try them, the public prosecutor, investigating judge and the president of the national criminal pole have exclusive jurisdiction to prosecute, judicially investigate and try a list of cybercrime offenses, such as offenses against the automated processing data systems related to public administration and institution, and related offenses [68]. Furthermore, such bodies are granted exclusive jurisdiction to prosecute and judicially investigate the cybercrime offenses of high complexity within the meaning of article 211 bis 25 of the Algerian code of criminal procedure[69], and even try them when they constitute misdemeanors.

Acting in the framework of the offenses falling within the national criminal pole exclusive jurisdiction, the judicial police officers transmit information reports and investigation proceedings directly to the public prosecutor within the national criminal pole and hence directly receive instructions from the latter, but when a judicial investigation is opened the judicial police officers directly receive letters rogatory from the investigating judge within the national criminal pole[70].

When the public prosecutor within the national criminal pole considers that the acts referred to him or her in accordance with the proceedings described above do not fall within his or her jurisdictional scope, he or she issues a relinquishment decision in favor of the public prosecutor who is territorially competent[71]. When the investigating judge hearing the case considers that he or she has not jurisdiction, he or she declares, either of his or her own motion upon the opinion of the public prosecutor or at the request of the latter, that he or she lacks jurisdiction. As soon as the investigating judge's order becomes final, the file of the proceedings is transmitted by the public prosecutor within the national criminal pole to that who is territorially competent. However, the arrest warrants and the remand in custody orders continue to be enforceable.

In addition, the prosecution and judicial investigation proceedings as well as the formalities taken prior to the issuance of an order declaring the investigating judge

incompetent continue to produce their legal effects and may not be renewed[72]. Such proceedings include, for example, the request of the public prosecutor to open a judicial investigation in accordance with article 67 of the Algeria's code of criminal procedure, a complaint accompanied by the lodging of an application for criminal indemnification pursuant to article 72 and all the acts and orders taken by the investigating judge such as the research and seizure set forth in articles 81 *et seq.* of the Algeria's code of criminal procedure; hearing of witnesses in conformity with articles 88 *et seq.*, the interrogation of the accused and the confrontation in accordance with articles 100 *et seq.* of the Algeria's code of criminal procedure[73].

**3 – 2 The National Criminal Pole's Concurrent Jurisdiction**

Except for the offenses that fall within the national criminal pole exclusive jurisdiction in conformity with article 211 bis 24 and 211 bis 25 of the Algerian code of criminal procedure, the other cybercrime offenses and related offenses are subjected to concurrent jurisdiction between the national criminal pole and the criminal judicial bodies that have territorial jurisdiction in accordance with articles 37, 40 and 329 of the Algeria's code of criminal procedure. In such case, the procedures provided for in articles 211 bis 6 to articles 211 bis 15 of the Algeria's code of criminal procedure are applied before the national criminal pole[74].

Accordingly, after being informed about one of the cybercrime offenses pursuant to article 40 ter of the Algeria's code of criminal procedure, the public prosecutor within the court territorially competent in conformity with article 37[75] transmits, without delay and by any means, the copies of information reports and investigation proceedings carried out by the judicial police to the public prosecutor within the national criminal pole[76]. When the latter considers, during the preliminary investigation and prosecution phases, that the offense concerned falls within its jurisdiction, he or she, upon the opinion of the general attorney at the Algiers court of appeal, claims the file of the proceedings from the public prosecutor territorially competent who issues a decision of relinquishment in favor of the former.

When a judicial investigation is opened, the requests containing the claim of the file of the proceedings are referred, however, to the investigating judge hearing the case who issues an order of relinquishment in favor of the investigating judge within the national criminal pole[77].

In the case of the simultaneous claims referred by the public prosecutor within the national criminal pole and the one within the courts with extended territorial jurisdiction, the jurisdiction is rested ex officio with the former. However, if the file of the proceedings is pending before the courts with extended territorial jurisdiction during the phase of preliminary investigations and prosecution or judicial investigation,

the relinquishment in favor of the public prosecutor within the national criminal pole is made in accordance with the forms described below. At any rate, the public prosecutors within the courts with extended territorial jurisdiction may inform the public prosecutor within the national criminal pole about new elements that may lead to claim the file of the proceedings by the national criminal pole[78].

Once a decision or an order of the relinquishment is respectively issued by the public prosecutor and the investigating judge, at either the territorially competent court of ordinary jurisdiction or the court with extended territorial jurisdiction concerned, the competent public prosecutor forwards the file of the proceedings, the related documents and the exhibits to the public prosecutor within the national criminal pole[79]. The relinquishment procedure results in the devolution of the powers of direction and control of the judicial police activities, regarding the performed acts, ongoing acts or the acts to be performed, to the public prosecutor within the national criminal pole. Hence, regardless of the courts upon which they depend, the judicial police officers and agents directly receive the instructions and letters rogatory from both the public prosecutor and investigating judge within the national criminal pole[80].

Unless the investigating judge within the national criminal pole decides otherwise, the arrest warrants and the pre-trial *detention* orders continue, however, to produce their legal effects. Consequently, the aforementioned judge becomes the guarantor for the legality and regularity of the proceedings related to the pre-trial detention. Moreover, the proceedings of the prosecution and judicial investigation taken prior to the relinquishment decision continue to be enforceable and may not be renewed[81]. Such proceedings may include the public prosecutor's request to open a judicial investigation in accordance with article 67 of the Algeria's code of criminal procedure, a complaint accompanied by the lodging of an application for criminal indemnification pursuant to article 72 and all the acts and orders taken by investigating judge such as the search and seizure referred to in articles 81 *et seq.* of the Algeria's code of criminal procedure; hearing the witnesses pursuant to articles 88 *et seq.* of the Algeria's code of criminal procedure, the interrogation of the accused and the confrontation pursuant to articles 100 *et seq.*[82].

At any rate, the relinquishment procedure results in the application of the code of criminal procedure provisions throughout the phases of the criminal proceedings related to cybercrime offenses, *i.e.*, the criminal action initiation, judicial investigation and the trial[83]

In another context, when the national criminal pole jurisdiction coincides with that of the economic and financial criminal pole or the court setting at the chief tower of the Algiers court of appeal, the territorial jurisdiction of which is extended to include

all national territory in respect with terrorist offenses and organized transnational crime[84], the jurisdiction rests *ex officio* with these latter two judicial bodies[85].

## Conclusion:

By studying the legal framework of the national criminal pole, we have reached the following conclusions:

- Owing to the national character of the national criminal pole, the judges belonging to it have a statewide jurisdiction.
- The jurisdiction ratione materiae of the national criminal pole includes the cybercrime offense in its broader sense, *i.e.*, offenses against automated data processing systems and ordinary offenses committed or the commission of which is facilitated by the use of information and communication technologies.
- The national criminal pole has jurisdiction not only to proceed with the prosecution and investigation in respect of offenses linked to information and communication technologies but also to try the accused of these offenses provided that such offenses constitute misdemeanors.
- In order to determine the relationship between the national criminal pole and other criminal judicial bodies, the Algerian legislator has, rightly so, conferred on the former an exclusive jurisdiction over some cybercrime offenses such as those that include high complexity element, on the one hand, and a concurrent jurisdiction to that of the courts with extended territorial jurisdiction and the ordinary criminal judicial bodies on the other hand.
- In consideration of the fact that the jurisdiction ratione materiae of the courts with extended territorial jurisdiction includes only offenses against automated data processing systems among other cybercrime offenses, the scope of the concurrent jurisdiction between these courts and the national criminal pole is limited to such offenses.
- Due to its national character and its specialization in investigating and prosecuting cybercrime offenses, the national criminal pole has jurisdictional priority over the jurisdiction of the courts with extended territorial jurisdiction and the ordinary criminal judicial bodies.
- The jurisdictional priority is subject to the claim by the public prosecutor within the national criminal pole of the file of the proceedings.
- The relinquishment of the proceedings does not affect the proceedings taken prior to the claim of the proceedings file.

- As regards the exclusive jurisdiction, the prosecution and judicial investigation proceedings as well as the formalities taken prior to the issuance of the order declaring the investigating judge within the national criminal pole incompetent continue to produce their legal effect and may not be renewed.

Finally, we suggest that the Algerian legislator amend the definition set forth in paragraph 3 of the article 211 bis 22 of the code of criminal procedure to include the offenses against automated data processing systems.

---

[1] " *La cybercriminalité est la troisième grande menace pour les grandes puissances, après les armes chimiques, bactériologiques et nucléaires"* . ROSE (C.), chercheur dans le domaine de la piraterie sur Internet. Discours prononcé lors de l'ouverture du G-8 sur la cybercriminalité, Paris, (2000), cited in : Romain BOSS, la lutte contre la cybercriminalité au regard de l'action des États, doctorat de droit privé et sciences criminelles, faculté de droit, sciences économiques et gestion, Université de lorraine, France, 2016, 22.

[2] See the official journal of PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA No. 71, published on November 10, 2004, online at: http:// www.joradp.dz, accessed 25 January 2022.

[3] See official journal of PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA No. 47, published on august 16, 2009, online at: *Ibid.*

[4] See Art. 2 of the Act No. 09-04, *Ibid.*

[5] The Algeria's legislation has provided for the courts with extended territorial jurisdiction and the economic and financial criminal division.

[6] See the official journal of PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA, supra note 2.

[7] To include respectively the judicial districts of the courts of appeal of Algiers, Laghouat, Blida, Bouira, Tizi Ouzou, Djelfa, Médèa, M'Sila, Boumerdés, Tipaza and Ain Defla; the courts of appeal of Constantine, Oum El Bouaghi, Batna, Béjaia, Tébessa, Jijel, Sétif, Skikda, Annaba, Guelma, Bordj Bou Arréridj, El Tarf, Khenchela, Souk Ahras and Mila; the courts of appeal of Ouargla, Adrar, Tamenghasset, Illizi, Biskra, El Oued and Ghardaia; and the courts of appeal of Oran, Béchar, Tlemcen, Tiaret, Tindouf, Saida, Sidi Bel Abbés, Mostaganem, Mascara, El Bayadh, Tissemsilt, Naama, Ain Témouchent and Relizane. See: Décret executive n° 06-348 DU 12 Ramadhan 1427 correspondant au 5 octobre 2006 portant extension de la compétence territoriale de certains tribunaux, procureurs de la république et juges d'instruction, the official journal of PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA N0. 63, published on October 8, 2006 amended by ; Décret exécutif N° 16-267 du 15 moharram 1438 correspondant au 17 octobre 2016, the official journal of PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA N0. 62, published on October 23, 2016.

[8] See Art. 40 bis 1 of the code of criminal procedure thus amended in 2020 in : Ordonnance N° 20-04 du 11 Moharram 1442 correspondant au 30 août 2020 modifiant et complétant l'ordonnance N° 66-155 du 8 juin 1966 portant code de procédure pénale, the official journal of PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA N0. 51, published on August 31, 2020, online at: *supra note 2.*

[9] See Art. 40 bis 2 in: *Ibid.*

[10] See Art. 40 bis 3 in: *Ibid.*

[11] See Art. 40 bis 5 in: *Ibid.* for more details on the procedural process set forth in articles 40 bis 1 *et seq.* of the Algeria's code of criminal procedure, see: Khaled KHELOUI, Assaad LAMAMRI, "corruption offenses: between the jurisdiction of the tribunals with extended territorial jurisdiction and the economic and financial criminal pole", Critical Journal of Law and Political Sciences, 16(04) (2021): 764-766.

[12] See *supra* note 2.
[13] See Art. 2 of the Presidential Decree No. 21-439 of 7 November 2021 on reorganization of the national Organ for the Prevention and Fight against Offenses Linked to Information and Communication Technologies in: the official journal of PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA No. 86, published on November 11, 2021, online at: *supra* note 2.
[14] See Art. 20 of the Presidential Decree No. 21-439 in: *Ibid.*
[15] *Ibid.*
[16] See Art. 23 of the Presidential Decree No. 21-439 in: *Ibid.*
[17] See Art. 24 of the Presidential Decree No. 21-439 in: *Ibid.*
[18] See Art. 2(f) of the Act No. 09-04, *supra* note 3.
[19] See Art. 3, *ibid.*
[20] In accordance with the foreign intelligence surveillance Act (FISA) enacted by the United States congress in 1978 the electronic surveillance is defined as "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs within the United States …". Cited in: https://www.justice.gov/archives/jm/criminal-resource-manual-1077-electronic-surveillance, accessed 13 February 2021.
[21] Electronic surveillance, at: https://www.justice.gov/archives/jm/criminal- resource-manual-1077-electronic-surveillance, accessed 13 February 2021. See about the interception of correspondence carried over wired and wireless communication means, article 65 bis 5(1) of the Algeria's code of criminal procedure thus amended in 2006 in: Loi N° 06-22 du 29 Dhou El Kaada 1427 correspondant au 20 décembre 2006 modifiant et complétant l'ordonnance n° 66-155 du 8 juin 1966 portant code de procedure pénale, journal official de la république algérienne N° 84, publié le 24 décembre 2006, online at: *supra* note 2.
[22] See Arti. 65 bis 5(1), *ibid.*
[23]State V. Lester, 64 HAW. 659(1982), p. 668, online at: https://www.cite.case.law/pdf/1432343/State%20v.%20Lester,%2064%20Haw.%20659%20(1982).pdf, accessed 13 February 2021.
[24]Stephanie JURKOWSKI, Electronic Surveillance, online at: https://www.law.cornell.edu/wex/electronic_surveillance#footnote1_hu8myuf, accessed 13 February 2021.
[25] See Art. 4(a)(b) of the Act No. 09-04, *supra* note 2.
[26] See Art. 4(c), *Ibid.*
[27] See Art. 4(d), *Ibid.*
[28] See Art. 4(2), *Ibid.*; Art. 65 bis 5(1) (3) of the Algeria's code of criminal procedure, *supra* note 21.
[29] See Art. 65 bis 7 of the code of criminal procedure, *Ibid.*
[30] See Art. 4(4) of the Act No. 09-04 *supra* note 2.
[31] See Alexandre ROUSSSELET-MAGRI, "les perquisitions « informatiques » à l'épreuve du principe de souveraineté, dans un contexte de mondialisation du stockage de données", Revue de Sciences Criminelle et de Droit Pénal Comparé (4) (2017) : 4, DOI 10.3917/rsc.1704.0659.
[32] See Kennn WANG, "Using a local Search Warrant to Acquire Evidence Stored Overseas via Internet", in K.P. Chow, S. Shenoi (ed.), advances in digital forensics VI (Berlin: Springer, 2010) 37.
[33] See Alexandre ROUSSSELET-MAGRI, *supra* note 31 at 661.
[34] See Art. 5 of the Act No. 09-04, *supra* note 3.
[35] The article 5 of the Act No. 09-04 provides that "the competent judicial authorities and the judicial police officers as well… may access, including remotely, to… ".
[36] On this question See the French procedural law point of view in: Alexandre ROUSSSELET-MAGRI, *supra* note 31 at 661.
[37] On the prior information clause see: Alexandre ROUSSSELET-MAGRI, *Ibid.*, pp. 662-664.

[38] See Art. 5(3) of the Act No. 09-04, *supra* note 3.
[39] See Art. 6 of the Act No. 09-04, *ibid*.
[40] See Art. 7 of the Act No. 09-04, *ibid*.
[41] See Art. 2(d) of the Act No. 09-04, *ibid*.
[42] See Art. 10 of the Act No. 09-04, *ibid*.
[43] *Ibid*.
[44] See Art. 11 of the Act No. 09-04, *ibid*.
[45] See Art. 12 of the Act No. 09-04, *ibid*.
[46] See the official journal of PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA No. 65, published on August 26, 2021, online at: *supra* note 2.
[47] See paragraph 2 of the article 211 bis 22 of the Algeria's code of criminal procedure thus amended in 2021 in: *ibid.*
[48] See Art. 166 of the Algeria's code of criminal procedure, online at: *supra* note 2.
[49] See Art. 179 of Algeria's code of criminal procedure, *ibid*.
[50] See art. 196 of Algeria's code of criminal procedure, *ibid*.
[51] See 197 of Algeria's code of criminal procedure, *ibid*.
[52] See Art. 211 bis 23 in: *ibid.*
[53] See Art. 211 bis 4 and Art. 211 bis 5 of the Algeria's code of criminal procedure to which it refers article 211 bis 27 thereof as a special procedural legal text applicable for the national criminal division.
[54] See Art. 2 of the Act No. 09-04 *supra* note 3.
[55] See *supra* note 2.
[56] See Explanatory Report to the Convention on Cybercrime, Council of Europe, Budapest, 23.XI.2001, European Treaty Series - No. 185, at online: https://rm.coe.int/16800cce5b, accessed 26 March 2022.
[57] *Ibid.*
[58] See paragraph 1 of the article 394 bis of the Algeria's code of criminal procedure thus amended in 2004, at online: *supra* note 2.
[59] See paragraph 2 and 3 of the article 394 bis of the Algeria's code of criminal procedure thus amended in 2004, *ibid*.
[60] See Art. 394 bis 1 of the Algeria's code of criminal procedure thus amended in 2004, *ibid*.
[61] Explanatory Report to the Convention on Cybercrime, *supra* note 56 at 12.
[62] *Ibid.*
[63] See BOSS, *supra* note 1 at 28.
[64] See Explanatory Report to the Convention on Cybercrime, *supra* note 56 at 14.
[65] See Art. 211 bis 24 of the Algeria's code of criminal procedure thus amended in 2021, *supra* note 46.
[66] In the context of corruption offenses see a same study related to the first four of these elements: KHELOUI, LAMAMRI, *supra* note 11 at 776.
[67] See Art. 2(a)(b) of the United Nations Convention against transnational organized crime ratified by Algeria on February 5, 2002, with reservation. See: Décret présidentiel N° 02-55 du 22 Dhou El Kaada 1422 correspondant au 5 février 2002 portant ratification, avec réserve, de la convention des Nations Unies contre la criminalité transnationale organisée, adoptée par l'Assemblée générale de l'Organisation des Nations Unies le 15 Novembre 2000, J.O.R.A.D.P., N° 09, published on February 10, 2020.
[68] See Art. 211 bis 24 of the Algeria's code of criminal procedure, about the other offenses see *supra* at 15.
[69] See *supra* at 15, 16.

[70] See Art. 211 bis 19 of Algeria's code of criminal procedure to which article 211 bis 26 thereof refers.
[71] See art. 211 bis 20 of Algeria's code of criminal procedure to which article 211 bis 26 thereof refers.
[72] See art. 211 bis 21 of Algeria's code of criminal procedure to which article 211 bis 26 thereof refers.
[73] See KHELOUI, LAMAMRI, *supra* note note 11 at 772.
[74] See Art. 211 bis 27 of the Algeria's code of criminal procedure thus amended in 2021, *supra* note 46.
[75] The first paragraph of this article provides that "the territorial jurisdiction of the public prosecutor is determined by the place where the offense has committed, the place of the residence of the persons alleged to involve in the offense or that of their arrest, even if this arrest is carried out for another reason…".
[76] See Art. 211 bis 6 of the Algeria's code of criminal procedure thus amended in 2020, *supra* note 8.
[77] See articles 211 bis 8 to 211 bis 10 of the Algeria's code of criminal procedure thus amended in 2020, *Ibid*.
[78] See Art. 211 bis 11, *ibid*.
[79] See Art. 211 bis 12, *ibid*.
[80] See Art. 211 bis 14, *ibid.*
[81] See Art. 211 bis 11, *ibid.*
[82] See KHELOUI, LAMAMRI, *supra* note 11 at 772.
[83] See Art. 211 bis 15 of the Algeria's code of criminal procedure thus amended in 2020, *supra* note 46.
[84] See article 211 bis 16 to 211 bis 21, *ibid*.
[85] See articles 211 bis 28 and 211 bis 29 of the Algeria's code of criminal procedure thus amended in 2021, *supra* note 46.

**Bibliography:**

**B - dissertation:**

1- Romain BOSS, la lutte contre la cybercriminalité au regard de l'action des États, doctorat de droit privé et sciences criminelles, faculté de droit, sciences économiques et gestion, Université de lorraine, France, 2016.

**C - Journal Articles:**

1- KHELOUI Khaled, LAMAMRI Assaad, "corruption offenses: between the jurisdiction of the tribunals with extended territorial jurisdiction and the economic and financial criminal pole", Critical Journal of Law and Political Sciences, 16(04), 2021, (764-766).
2-Alexandre ROUSSSELET-MAGRI, "les perquisitions « informatiques » à l'épreuve du principe de souveraineté, dans un contexte de mondialisation du stockage de données", Revue de Sciences Criminelle et de Droit Pénal Comparé, N°4, 2017.

3- Kennn WANG, "Using a local Search Warrant to Acquire Evidence Stored Overseas via Internet", in K.P. Chow, S. Shenoi (ed.), advances in digital forensics VI , Springer, Berlin, 2010.

**D- Legal texts:**

1- Loi N° 04-15 du 27 ramadhan 1425 correspondant au 10 novembre 2004 modifiant et complétant l'ordonnance N° 66-155 du 8 juin 1966 portant code de procédure pénale, J.O.R.A.D.P. N° 71, published on november 2004.

2- Loi N° 06-22 du 29 Dhou El Kaada 1427 correspondant au 20 décembre 2006 modifiant et complétant l'ordonnance n° 66-155 du 8 juin 1966 portant code de procedure pénale, journal official de la république algérienne N° 84, publshed on december 24, 2006.

3- Loi N° 09-04 du 14 Chaabane 1430 correspondant au 5 août 2009 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication, J.O.R.A.D.P. N° 47, published on August 16, 2009.

4- Ordonnance N° 20-04 du 11 Moharram 1442 correspondant au 30 août 2020 modifiant et complétant l'ordonnance N° 66-155 du 8 juin 1966 portant code de procédure pénale, J.O.R.A.D.P. N° 51, published on August 31, 2020.

5- Ordonnance N° 21-11 du 16 Moharram 1443 correspondant au 25 août 2021 complétant l'ordonnance N° 66-155 du 8 juin 1966 portant code de procédure pénale, J.O.R.A.D.P.A. N° 65, published on August 26, 2021.

6- Décret présidentiel N° 02-55 du 22 Dhou El Kaada 1422 correspondant au 5 février 2002 portant ratification, avec réserve, de la convention des Nations Unies contre la criminalité transnationale organisée, adoptée par l'Assemblée générale de l'Organisation des Nations Unies le 15 Novembre 2000, J.O.R.A.D.P., N° 09, published on February 10, 2020.

7- Décret présidentiel N° 21-439 du 2 Rabie Ethani 1443 correspondant au 7 novembre 2021 portant réorganisation de l'organe national de prévention et de lutte contre les infractions liées aux technologies de l'information et de la communication, J.O.R.A.D.P. N° 86, published on November 11, 2021.

8- Décret exécutif N° 06-348 du 12 ramadhan 1427 correspondant au 5 octobre 2006 portant extension de la compétence territoriale de certains tribunaux, procureurs de la république et juges d'instruction, J.O.R.A.D.P. N° 63, published on octobre 8, 2006.

9- Décret exécutif N° 16-267 du 15 moharram 1438 correspondant au 17 octobre 2016 modifiant le Décret exécutif N° 06-348 du 12 ramadhan 1427 correspondant au 5 octobre 2006 portant extension de la compétence territoriale de certains tribunaux, procureurs de la république et juges d'instruction , J.O.R.A.D.P. N° 62, published on October 23, 2016.

**E – Website references:**

1- Electronic surveillance, at: https://www.justice.gov/archives/jm/criminal-resource-manual-1077-electronic-surveillance, accessed 13 February 2021.

2- State V. Lester, 64 HAW. 659(1982), p. 668, online at: https://www.cite.case.law/pdf/1432343/State%20v.%20Lester,%2064%20Haw.%20659%20(1982).pdf, accessed 13 February 2021.

3- Stephanie JURKOWSKI, Electronic Surveillance, online at: https://www.law.cornell.edu/wex/electronic_surveillance#footnote1_hu8myuf, 2017, accessed 13 February 2021.

4- Explanatory Report to the Convention on Cybercrime, Council of Europe, Budapest, 23.XI.2001, European Treaty Series - No. 185, at online: https://rm.coe.int/16800cce5b, accessed 26 March 2022.