

The Legal Framework For The Inspection of Information Systems in Algerian Legislation

النظام القانوني لتفتيش المنظومات المعلوماتية في التشريع الجزائري

BABAH Brahim¹, GHEHIOUECHE Alwalid²

¹ University of Algiers 1, Benyoucef Benkhedda (Algeria), ibr.babah@univ-alger.dz

² University of M SILA (Algeria), Alwalid.ghehioueche@univ-msila.dz

Received: 09/07 /2025

Accepted: 07/12 /2025

Published: December /2025

الملخص:

يعد تفتيش المنظومات المعلوماتية أحد الإجراءات القضائية المستحدثة التي تستهدف البحث و ضبط الأدلة الالكترونية أو نسخها أو حظر التصرف فيها من أجل كشف مرتكبي الجرائم الالكترونية التي أفرزها الإستخدام غير المشروع لتكنولوجيات الاعلام و الإتصال وإثبات مسؤوليتهم عنها، و الذي ينصب على المعالجات الآلية أو ملحقاتها و على مختلف الوسائط الالكترونية و الشبكات مما قد يعرض الحياة الخاصة الالكترونية للأفراد للمساس ما تطلب ضرورة مراعاة و إحترام القائم بالتفتيش للقيود و الضمانات التي كفلها الدستور ونصت عليها الاتفاقيات الدولية و الإقليمية وأقرها القانون الجزائري تحقيق لمبدأ الشرعية الإجرائية.

الكلمات المفتاحية: التفتيش ؛ المنظومات المعلوماتية ؛ الأدلة الالكترونية ؛ الجريمة الالكترونية ؛ الخصوصية الالكترونية

Abstract:

The inspection of information systems is one of the recently introduced judicial procedures aimed at searching for, seizing, copying, or restricting the use of electronic evidence in order to identify the perpetrators of cybercrimes resulting from the unlawful use of information and communication technologies and to establish their responsibility. This inspection targets automated data processing systems, their accessories, various electronic media, and networks, which may expose individuals' electronic privacy to violation. Therefore, it is essential for the inspector to respect and adhere to the safeguards guaranteed by the Constitution, stipulated in international and regional conventions, and affirmed by Algerian law, in order to uphold the principle of procedural legitimacy.

Key words: Inspection; Information Systems; Electronic evidence; Cybercrime; Electronic privacy.

Introduction:

Cybercrimes are among the new crimes that have emerged due to the illegal use of information and communication technologies, and the Algerian legislator has defined Cybercrimes which are expressed in crimes related to information and communication technologies under Article 2 of Law 09/04 dated 5/8/2009, which contains rules for the prevention and control of crimes related to¹ information and communication technologies as Offences targeting automated data processing systems as defined in the Penal Code, as well as any other offence perpetrated or made possible through the use of an information system or an electronic communications network

Cybercrimes is illegal behavior punishable by law in which one or more electronic means are used as a tool, environment or target to commit the crime. Basically, cybercrime is a digital activity designed to deal with computer systems through its own language, which is binary code (0, 1), and therefore any cybercrime is the translation of criminal ideas into a digital language and in an electronic environment².

The requirements for detecting cybercrime, detecting its perpetrator, proving it, and presenting evidence before the court, have imposed that the evidence and the specificity of the cybercrime, which is carried out in the digital environment, are in line with what led to the emergence of what is known as electronic evidence, which is one of the means of proof developed in the penal articles, as the electronic criminal evidence includes all electronic means, in addition to all electronic data that can prove that there is a crime committed or that there is a relationship between the crime and the perpetrator, or prove a relationship between the crime and the victim.

Given the specificity of committing Cybercrimes and the specificity of the digital environment in which or through which these crimes are committed, the Algerian legislator, similar to comparative national legislation, had to adopt special methods procedures in line with the specificity of Cybercrimes in order to seize electronic evidence and bring it to justice. Electronic inspection is one of the most important methods of collecting electronic evidence, where electronic systems of persons are accessed in order to seize electronic evidence related to a crime, or seize it and prevent its disposal, and there is no doubt that this measure would prejudice their electronic private life.

Here we pose the following problem: How did the Algerian legislator regulate the provisions of the inspection of information systems and did it approve its own provisions or subject it to the general provisions of the inspection? What are the legal guarantees approved by the Algerian legislator to conduct an inspection of information systems, and how do we balance the relationship between achieving the public interest by detecting crime and arresting perpetrators and between protecting people's electronic privacy?

The subject of searching information systems occupies a position of paramount importance in criminal law, rendering it a fertile domain for contemporary legal scholarship. This significance stems from its role as a manifestation of the adaptation of the penal legal framework to crimes pertaining to information and communication technologies, as well as its alignment with the challenges posed by searches conducted within the electronic environment. Such adaptation is essential for the lawful seizure and preservation of electronic

evidence, thereby facilitating the detection and investigation of cybercrimes. This process necessitates the implementation of specialized procedures, mechanisms, and safeguards commensurate with the distinctive nature of these offenses. Furthermore, it raises critical legal issues, particularly concerning the extent to which the informational privacy of individuals—guaranteed by constitutional principles, international covenants, and statutory provisions—is duly observed and respected. Additionally, it encompasses the complex matter of remote tracing and seizure of electronic evidence, whether located in information systems beyond national jurisdictions or disseminated across the Internet, which in turn underscores the imperative of international cooperation and coordination in this field.

This study aims to determine the nature of the inspection of the information system, the extent to which non-intangible elements of automated processes, electronic media and the Internet can be subject to inspection, and to identify the legal procedures and guarantees established by the Algerian legislator with regard to the inspection of information systems, and to search for problems that arise in practical application, especially with regard to inspection, within the scope of the various legal texts of Algerian legislation.

To answer the problem, we adopted the descriptive and analytical approach to stand and analyze the various legal texts related to the subject of the study. The study was divided into two chapters. In the first chapter, we discussed the legal framework for inspecting information systems, while in the second chapter, we discussed the controls for inspecting information systems.

The first chapter : The concept of inspecting information systems

In this section, we will discuss the definition of the information system inspection procedure in the first requirement, and determine the extent to which the components of information systems and the networks associated with them are susceptible to inspection

1- Definition of Information System Inspection

The search is a procedure of investigation of a protected place, carried out by a competent authority in accordance with the procedures, restrictions and guarantees prescribed by law with the aim of accessing material evidence of a felony or misdemeanor that has occurred, to prove its commission and attribution to the accused³. If the subject of the search in traditional crimes is focused on a place that has special protection, the matter in electronic crimes and the search for electronic evidence is different from that due to the non-physical nature of the programs and data of information systems, as well as the Internet, it is just electronic data and programs that do not have any tangible physical appearance in the outside world⁴.

The Algerian legislator defined the information system as any separate system or group of systems connected to each other or linked, one or more of which automatically processes the data in implementation of a specific program⁵, while he defined the information data as any presentation of facts, information or concepts in a form ready for processing within an information system, including appropriate programs that would make an information system perform its function⁶. Automated processing means operations performed in whole or in part by automated methods such as recording data and applying logical and/or mathematical operations to these data, changing them, scanning them, extracting them or publishing them⁷.

The inspection of information systems, or what is known as electronic or information inspection, is defined as the inspection of computer crimes, which aims to access the material

or intangible data contained in computer systems that are useful in detecting crime and attributing it to the ⁸accused. It is access to a place granted special protection by law as a repository⁹ of the secret of its owner¹⁰. This place is equal to being a computer, its systems or the Internet. Electronic evidence is defined as evidence taken from computers and is in the form of magnetic or electrical fields or pulses that can be collected and analyzed using special technological programs and applications and is presented in the form of evidence that can be adopted before the judiciary.¹¹

The inspection and seizure of electronic evidence needs special techniques, methods and programs to copy, retrieve, repair and reassemble data and other procedures, due to the possibility of removing¹³ or hiding them or encrypting them and the development of multiple protection systems that prevent access to them or access to them in addition to the possibility of keeping evidence outside the crime scene completely and even outside the borders of the state¹⁴.

The Algerian legislator approved the inspection of information systems and regulated some of its provisions under Law 09/04, which contains the special rules for the prevention and combating of crimes related to information and communication technology, in Chapter Three of it under the title "Procedural Rules for the Inspection of Information Systems", Article 3 of which stipulates that the requirements for the protection of public order or the absence of requests for judicial investigations or inquiries, taking into account the legal provisions that guarantee the confidentiality of correspondence and communications, in accordance with the rules and guarantees stipulated in the various legal texts , may carry out search and seizure procedures within an information system.

- a) An information system or any part thereof, as well as the information data stored therein,
- b) An information storage system.

The information system consists of hardware , moral or software components, as well as local and international wired and wireless network telecommunications networks. The inspection aims to search for non-physical data stored in the computer ,

or stored in tablets. It also aims to search the information systems under investigation¹⁵.

Jurisprudential debate has arisen about the susceptibility of physical and moral computer components and associated networks to inspection¹⁶.

2.1- Physical Components of Information Systems

Criminal law doctrine unanimously concurs that the objective of search procedures is the seizure of tangible evidence conducive to uncovering the truth. Accordingly, the search of the physical components of various information systems in pursuit of any item connected to a cybercrime that has occurred-and which serves to elucidate the truth thereof and identify its perpetrators-falls within the scope of search, provided it is conducted in strict conformity with the prescribed statutory procedures¹⁷. These physical components raise no particular difficulty with respect to their searchability, subject, however, to compliance with specialized protocols for the seizure of such devices in light of their sensitivity and susceptibility to damage.

Nevertheless, the legal regime governing the search of the physical components of an information system is contingent upon the nature of the locus in which they are situated-specifically, whether they are located in public premises open to the general public or in private premises enjoying statutory protection. The locus assumes particular significance in the context of search operations. Where such components are situated in private premises-such as the suspect's domicile or any appurtenant thereto, or within an enterprise or office accorded legal protection-compliance with the procedures governing domiciliary searches as stipulated in Article 75 of the Code of Criminal Procedure becomes mandatory, particularly the requirement of obtaining a search warrant.

By contrast, the remaining safeguards ordinarily applicable to search operations-such as adherence to the statutory time frame for searches and the mandatory presence of the suspect or his legal representative are not applicable in the realm of cybercrimes. Thus, the search of information systems (or any part thereof) or information storage systems may be conducted at any hour of the day or night and in the absence of the data subject, pursuant to Articles 76 and 78 of the Code of Criminal Procedure, which dispense with both the prescribed temporal restrictions (from 05:00 to 20:00) and the requirement of the suspect's presence or that of his representative during the search¹⁸.

2.2- The intangible Components of Information Systems

It raised the issue of the possibility of subjecting the intangible components of information systems to inspection, contrary to the midst of legal jurisprudence, where jurisprudence was divided into two directions :

The first trend: Part of the jurisprudence considers that electronic data and data cannot be subject to inspection, as the inspection is an investigative procedure aimed at seizing material things that contribute to revealing the circumstances of the crime and

identifying the perpetrator, which is inconceivable in the moral components of information systems, and the owners of this trend concluded its interpretation to be based on the link between procedural texts and natural sciences and their application to data, data or programs, as the word thing means matter, and it is all that occupies a certain vacuum that can be measured and controlled, which does not apply to the moral elements of asp, which do not occupy a physical space, and its capacity and size cannot be measured and can be stored in it¹⁷

This jurisprudential aspect, in view of the legislative deficiency, suggests the need to add to this traditional purpose of inspection the possibility of searching and controlling materials processed by computer or computer data, so that the new purpose of inspection after this technical development is to search for physical evidence and any evidence or trace resulting from automated processing of data or data by computer¹⁸.

The second trend: This trend sees the permissibility and possibility of conducting an inspection in all components of a system of automated data processing, including the moral components of data and data stored, whether in computers, smart phones or even in internal or international Internet communication networks.

From the legislative point of view, we find that all legislations have taken the second opinion, including the Algerian legislator, who authorized the inspection of information systems in accordance with the provisions of Article 05 of Law No. 09/04.

2.3- The extent to which communication networks are subject to electronic inspection "remote inspection"

With the advent of the Internet, cybercrime has taken place internationally. Its impact is no longer limited to the territorial borders of one country, but has extended to all countries of the world, which made it difficult to search and seize criminal evidence on the investigation authorities because of its extension through the networks of the computer to places far from the physical location of the child.¹⁹

Here, the question arises: Is it possible to extend the inspection to an information system from an information system related to which permission has been obtained to inspect it within the territory of one country? Is it possible to extend this inspection to an information system located outside the territory of the state?

the legislator distinguished between two cases:

The first case: When the information system of the suspect or accused is connected to another information system located within the national territory:

Where an inspection is carried out on an information system or a part thereof, or on the data stored therein, and where there are reasonable grounds to believe that the

data being sought is stored in another connected information system that can be accessed from the first, the Algerian legislator permits the prompt extension of the inspection to include that other system or part thereof, subject to the prior notification of the competent judicial authority²⁰.

The second case: The connection of the inspected information system to an information system located outside the national territory.

The Algerian legislator has authorized the inspection of information systems located outside the territory of the State when it is confirmed that the data in question are stored in that system and can be accessed from the system located in the national territory, provided that this is with the assistance of the competent foreign authorities to reflect international cooperation to combat cybercrime and in accordance with the²¹ relevant international conventions and in accordance with the principle of reciprocity²².

The third case: When the data or data to be searched is on the Internet

Cloud Storage is defined as a digital storage model based on a virtual infrastructure distributed across the Internet, where information and data are stored on platforms of virtual servers rather than confined to a specific server, and this is managed through specialized hosting companies that have advanced technical infrastructures that include huge data centers, allowing users to allocate flexible storage spaces commensurate with their requirements

With reference to the text of Article 5 of Law No. 09/04 on the prevention of crimes related to information and communication technologies, we find that the legislator has authorized the inspection of any information storage system, whether it is within the information system or on the Internet. The legislator also obligated all service providers active on the national territory and subject to Algerian law to provide assistance to the authorities in charge of judicial investigations to collect and record data related to the content of communications in a timely manner and to put the data that they must keep in accordance with the law.²³ They are also under a legal obligation to preserve the confidentiality of all operations carried out at the request of the investigative authorities, as well as any information related thereto, subject to the penalties prescribed by law for the unauthorized disclosure of investigation or inquiry related secrets²⁴.

The second chapter : Inspection controls in information systems

The right to privacy is recognized as one of the fundamental rights inherent in the human person. The scientific advancements and the proliferation of information and communication technologies (ICT) among individuals have given rise to a novel conceptual framework known as informational privacy or electronic privacy²⁵, This is defined as the right of

individuals to safeguard the confidentiality of their data and personal information within the digital environment, and to prohibit unauthorized access or dissemination thereof absent their express consent. Accordingly, informational privacy denotes the protection of individuals' personal data and information security during their utilization of information systems, electronic devices, and the Internet, encompassing the capacity to exercise control over access to such data and information²⁶. This dimension has become an integral and indivisible component of human privacy, which has, in turn, been accorded robust legal protection.

Given that the search of information systems constitutes one of the most intrusive investigative measures that infringes upon the rights and freedoms of individuals²⁷ and violates their informational privacy, thereby enabling the searching authority to access private electronic data and information, it became imperative for the legislator to regulate this procedure through statutory provisions designed to strike a delicate balance between, on the one hand, safeguarding individuals' informational privacy, and on the other, upholding the State's legitimate interest in imposing criminal sanctions against cybercriminals by authorizing judicial authorities to conduct searches of information systems for the detection of offenses and the seizure of electronic evidence²⁸.

The constitutional legislator has enshrined legal protection for private life by subjecting domiciliary searches to stringent statutory safeguards. It has expressly provided that the State shall guarantee the inviolability of the home, such that no search may be conducted except in accordance with law and in strict compliance therewith, and only pursuant to a written order issued by the competent judicial authority²⁹. Furthermore, Article 47 of the 2020 Constitutional Amendment affirms that every person enjoys the right to the protection of their private life and honor, and that every individual has the right to the confidentiality of their private correspondence and communications in any form whatsoever. The phrase "in any form whatsoever" unequivocally encompasses individuals' electronic private life, otherwise known as informational privacy, which constitutes an inseparable component of the broader right to private life.

Numerous international human rights instruments have likewise guaranteed legal protection for informational privacy as an integral facet of individual privacy³⁰. Notable among these are the Universal Declaration of Human Rights³¹ and the International Covenant on Civil and Political Rights³². These instruments have encircled the search of information systems with multiple procedural safeguards and limitations to ensure its protection.

From a statutory perspective, the legislator has criminalized the violation of domiciliary inviolability as a punishable offense³³. Moreover, it has proscribed a wide array of conduct capable of compromising information systems under Section Seven Bis of Chapter Three, Title Two, Book Three of Ordinance No. 66-156, entitled "Attacks on Automated Data Processing Systems", as articulated in Articles 394 bis to 394 bis 7³⁴. Additionally, the legislator has criminalized infringements upon informational privacy by prohibiting the unauthorized automated processing, access, or interception of individuals' personal digital data and information without prior consent of the data subject³⁵.

For electronic evidence to possess probative value, it must satisfy reliability guarantees consonant with two distinct categories of conditions—general and specific—such that the evidence, like any other form of proof, must be legally and rationally admissible before the criminal court, directly linked to the facts of the offense under investigation, and collected under circumscribed conditions that respect constitutionally and statutorily prescribed limitations and safeguards, thereby upholding the principle of procedural legitimacy³⁶.

Accordingly, the search of information systems is subject to a comprehensive set of conditions and controls to ensure its validity, thereby permitting reliance upon the minutes thereof for proving the offense. These include grounds for the search, which require the actual

commission of an offense subject to investigation; and judicial authority competent to issue authorization, supervise, and oversee the execution of the search. Thus, conducting the search necessitates obtaining prior permission from the Public Prosecutor or the competent investigating judge. Consequently, the regulatory framework governing searches is bifurcated into two categories: substantive controls and formal (procedural) controls.

1. Objective controls for inspection in information systems and networks

In order for the inspection of the information system to be legal and productive of its impact, the inspector must comply with the conditions and guarantees specified by law .

1.1- There is a reason for inspection in information systems

The inspection of information systems aims to obtain electronic evidence within an existing investigation following the occurrence of a crime, whether a felony or a misdemeanor, and to accuse one or several persons of committing or participating in it, with strong evidence and indications of the existence of evidence or things useful in revealing the truth stored in the information system. Judicial inspection is not a means of preventing crimes, but rather an investigation procedure to uncover the circumstances of the occurrence of the crime and seize evidence to detect and arrest the perpetrator³⁷

With reference to the provisions of Law No. 09/04, especially Article 3 and 5 thereof, we find that the Algerian legislator has authorized the competent judicial authorities as well as judicial police officers to carry out search and seizure procedures within an information system whenever the requirements of protecting public order or the requirements of ongoing judicial investigations or inquiries require, or in order to prevent acts that are described as terrorist or subversive crimes, or those that are described as crimes against state security, or when there is information indicating the possibility of an attack on a system My information may negatively affect public order, national defense, state institutions, or the national economy, or when resorting to electronic surveillance is necessary required by the requirements of judicial investigations, and without which it is difficult to reach results of ongoing research, and inspection can be carried out in the context of the implementation of requests for mutual international judicial assistance³⁸, and in all cases stipulated by law³⁹ through access to any automated data processing system or part of it, as well as the electronic data and data stored in it, or to any information storage system In order to conduct an inspection, whether directly or remotely, provided that this is within the framework of procedural legitimacy.

1.2- The place of inspection in information systems.

The nature of the crime committed, the nature of the evidence to be searched, searched and seized, and the strong signs of determining where to keep, possess or store it play an important role in determining the places and devices to be searched. In general, the inspector may proceed to search in all places where things can be found

whose detection is useful to reveal the truth in accordance with the provisions of Article 157 of the Code of Criminal Procedure, The subject of the inspection in crimes related to information and communication technologies includes all components of automated processors, whether physical or moral, such as computer or smart devices, and its accessories, as well as its communication networks, or any device for carrying, transferring and storing

When the authority conducting the inspection in an information system discovers stored data that are useful in detecting crimes or their perpetrators and that it is not necessary to seize the entire system, the data in question is copied as well as the data necessary to understand it on an electronic storage pillar that is subject to seizure and placement in holdings in accordance with the rules established in the Code of Criminal Procedure⁴⁰.

In all cases, the electronic searcher and seizure must ensure the safety of the data in the information system in which the operation is conducted. It must also preserve the seized evidence and ensure that no modification, deletion, addition or any other change of any nature that would affect the content of the evidence is made⁴¹, and the inspector may have to prove the impossibility of conducting it, even if the legislator has granted the electronic inspecting authority the use of the necessary technical means to form or reconfigure these data in order to make them exploitable for the purposes of the investigation, as long as this does not prejudice the content of the data.

1.3- The competent authority for inspection of information systems

The principle is that inspection is one of the judicial investigation procedures that affect the personal freedoms of individuals⁴², so the penal legislation was keen to assign it to the judicial authorities themselves⁴³, and as an exception and because of the preoccupation with many other judicial tasks and the lack of judges and the large number of crimes committed, the legislation allowed the delegation to conduct the inspection of the judicial police bodies, provided that this is done by a judicial police officer, and that this is done with their permission and under their supervision and control in accordance with the text of Articles 141 and 75/4 of law 24/14⁴⁴ ..

In accordance with the provisions of Article 5 of Law 09/04, the legislator has authorized the competent judicial authorities, as well as judicial police officers, to access any system of automatic processing of data or part thereof, as well as the electronic data and data stored therein, or to an information storage system in order to conduct an inspection, whether directly or remotely, provided that this is within the framework of procedural legality.

Due to the specificity of the search and inspection of the electronic evidence and the specificity of seizing, processing and preserving it or even taking the necessary measures to prevent it from being compromised, destroyed or manipulated, the legislator authorized the authorities in charge of the inspection to harness every person

who has knowledge of the work of the information system in question or the measures taken to protect the information data it contains⁴⁵, in order to assist them and provide them with all the information necessary to accomplish their mission⁴⁶.

2. Formal controls for inspection in information systems or the network

The legislator subjected the inspection of information systems to a set of formal controls, which are :

2.1- Obtaining permission to inspect information systems

The search warrant is defined as that written license issued by the competent judicial authorities to the judicial police officer in order to enter a special place that has legal protection in order to search and search to seize evidence in order to detect the crime and arrest the perpetrators⁴⁷.

In order for the inspection of information systems or the inspection of data storage systems to be correct in line with the principle of procedural legitimacy, the inspector must adhere to the procedures as specified by law, which are represented in the need to obtain judicial permission, as national legislation regulates these procedures accurately to ensure a balance between the requirements of security and truth detection on the one hand and the protection of individual rights and freedoms on the other.

In accordance with the provisions of Article 5 of Law No. 09/04, the legislator authorized judicial police officers to inspect the automated processing systems for information and data or data storage systems. However, it did not explicitly stipulate the need for them to obtain a "**judicial permit**" to conduct the search. It only stipulated the phrase "within the framework of the Code of Criminal Procedure", which leads us to refer to the general provisions of the Code of Criminal Procedure, especially Article 75 of law 24/14, which requires that judicial police officers must obtain a judicial permit with the need to present it to the owner of the residence and invoke it before entering the residence and starting the search process⁴⁸. This is under penalty of nullity, as the base where the restriction was found refrained from entering and the lesson in determining the restrictions on entry is at the place to be entered and at the moment of entry⁴⁹.

With reference to the provisions of Law No. 09/04 on the prevention and control of crimes related to media and communication technologies, we do not find that the Algerian legislator has set rules for the permission to conduct electronic inspection, and therefore reference is made to the general rules for inspection stipulated in the Code of Criminal Procedure.

Among the necessary data in the search warrant is that the search warrant must specify the place or information systems to be inspected and all components or

objects to be inspected and seized accurately⁵⁰ (computers, electronic sexual images of children, counterfeit electronic works...), in order to avoid exploratory inspection, so that the person authorized to inspect is not left with any discretion in this regard. However, there is difficulty in respecting this condition during practice in inspecting different automated processors, due to the special nature of the latter. Computers or phones contain a large number of files. In addition, the names of these files do not necessarily indicate what they contain. Therefore, difficulties are raised. Is each file considered a "closed box that needs judicial permission independent of the other? In particular, the accused may resort to pseudonyms for files containing illegal materials⁵¹.

By virtue of the provisions of Law No. 09/04, the legislator has introduced specific procedural rules governing the extension of electronic inspection to other information systems. Article 5, in particular, provides that in the scenario referred to in paragraph (a) which concerns an information system or part thereof, as well as the data stored therein it is permitted to expand the scope of the inspection to include other systems, provided that the applicable legal conditions are met.

Where there are reasonable and compelling grounds to believe that the data subject to search is stored within another information system that is accessible from the initially inspected system, the competent authority may, following prior notification to the competent judicial authority, proceed to promptly extend the scope of inspection to encompass that additional system or any part thereof. However, if the data sought is located within an information system situated outside the national territory and can be accessed from within the national jurisdiction, such access shall be effected through cooperation with the competent foreign authorities, in accordance with the applicable international treaties or agreements concluded for this purpose, and subject to the principle of reciprocity.

The Algerian legislature has authorized the competent authorities, within the framework of ongoing investigations or judicial inquiries aimed at detecting crimes involving information and communication technologies and identifying their perpetrators, to engage in the exchange of international mutual legal assistance for the purpose of gathering evidence pertinent to the offense in electronic format. Accordingly, responses may be provided to assistance requests intended for the exchange of information or the implementation of any preservative measures to secure or seize any information system associated with the committed offense or the electronic evidence contained therein. Judicial assistance requests shall be accepted even if transmitted via expedited communication channels, including facsimile devices or electronic mail, provided that such channels incorporate adequate security measures to verify their authenticity. This shall be conducted in accordance with relevant

international conventions, bilateral international agreements, and the principle of reciprocity⁵².

Assistance requests that may infringe upon national sovereignty or public order are exempted from judicial and security cooperation as well as information exchange. Furthermore, when responding to international assistance requests, the competent authorities may stipulate the necessity of preserving the confidentiality of the disclosed information and restricting its use solely to the purposes delineated in the request⁵³.

2.2- Non-requirement of the presence of stakeholders to conduct inspection in information systems

The presence of the suspect, the accused, or the person whose residence is to be searched, or their representative, is one of the most important guarantees prescribed by law for them. It is also one of the most important formal conditions required by law for the validity of the search, in order to ensure the safety of the search, in addition to personally identifying the evidence seized, and the possibility of access to the secrets of others.

However, pursuant to Article 76 of Criminal Procedure Law No. 24/14, the legislator has not mandated the presence of the concerned individual during the conduct of searches in certain offenses, including those pertaining to information and communication technologies, as expressly provided therein: ("These provisions shall not apply in cases involving offenses related to information and communication technologies....")⁵⁴, and the wisdom of this is due to the need to confer some kind of secrecy during the collection of electronic evidence, especially since this evidence is of a special nature in terms of the speed of modification and manipulation even remotely, and this guarantee is beginning to diminish its importance in countries that adopt the system of remote inspection, or what the French jurisprudence calls "indirect inspection"⁵⁵.

In this regard, the Algerian legislator had to distinguish between two cases :

The first case: If the inspection targets an information system or its accessories, data storage devices, data or any other devices related to the crime and contributes to revealing the truth present in the house of the accused, here the owner of the house must be present, whether he is a suspect or accused, and in the event that he is unable or present in the penal institution or is a fugitive, the procedures specified in Article 76 shall be applied in the presence of a representative of the owner of the house or two witnesses who are not subject to the authority of the judicial police officer, because in this case he will be arrested. The seizure of evidence and recording this in the inspection record, and this is a protection and guarantee for the person and in order to achieve the legitimacy of the electronic evidence that was seized and sealed, as Article

73 of the Criminal Procedure Law stipulates that the judicial police officer must take all necessary measures to preserve the evidence that is feared to disappear, and seize all elements and evidence that would contribute to revealing the truth, and he must also present the seized objects to the persons suspected of contributing to the commission of the crime to confirm their identity or identify them. A second party in order to achieve its legitimacy and in application of the text of Article 1 of the Criminal Procedure Law, which stipulates this law is based on the principles of legality, fair trial and respect for human dignity and rights, and to ensure that the concerned person does not claim that electronic evidence was not seized at his home.

The second case: If the information system or network is inspected remotely according to specialized technologies and programs, whether inside or outside the national territory, then the presence of the concerned person is not required, but it is not necessary as long as the penetration, seizure, preservation, or taking measures to prevent access to or disposal of the evidence.

2.3- Timeline for conducting inspections in information systems

In order to narrow the scope of the attack on individual freedoms and to protect private life and the inviolability of housing, the Algerian legislator stipulates that it is not permissible to start searching and inspecting housing before five (5) am, or after eight (20) pm as a public asset, except in the legally prescribed cases where it is permissible to depart from these dates. The inspection may be carried out at any hour of the night and day, in accordance with the text of Article 78 of the Code of Criminal Procedure.

However, the Algerian legislator, pursuant to Article 78, paragraph 3 of the Criminal Procedure Law, has excepted the application of these safeguards to a category of offenses, including those related to information and communication technologies.

However, if the inspection is carried out in private places such as residences or offices, or if the person carries with him computer components or devices for storing and transferring the aforementioned information and data, or if he controls or possesses them, the inspection shall not be carried out except in cases where it is permissible to inspect places or persons with the same guarantees and restrictions stipulated in this field.

2.4- Minutes of inspection in information systems

Considering that the inspection is an investigation work aimed at collecting evidence to uncover the truth, and because the electronic inspection affects the electronic private life of persons, the legislator obligated the electronic inspection authority to write a report proving the procedures that took place and the results of the

inspection of the seizure of evidence and the circumstances in which this was done, and it must also include all the measures that have been taken, such as seizing or copying data or deleting it, or the procedures and measures taken to prevent the disposition or access to electronic evidence, and in general all the procedures followed by the person specialized in the systems, where the inspector must document all the procedures that are taken in an official record⁵⁶.

In all cases, the inspector must seize everything that can lead to revealing the truth⁵⁷, present the seized objects to the persons suspected of contributing to the felony or misdemeanor for identification, and take inventory in the record of all objects, documents, and evidence that have been seized, seized, and their nature determined, and put them in a bag and close it with paper tape and seal it.

It should also be noted that if during the inspection of the information system or network inspection, crimes are discovered and evidence other than those stipulated in the search warrant is seized, the inspection remains valid and produces its legal effects. The Public Prosecution can follow up the person concerned with the detected crimes in accordance with the procedures specified in the law, in accordance with the text of Article 75, the last paragraph of the Criminal Procedure Law, which stipulates that (If crimes other than those mentioned in the judge's permission are discovered during these operations, this shall not be a reason for the nullity of the interlocutory procedures.

In order to protect the right to privacy and non-defamation, the legislator, in accordance with the provisions of Article 45 of the Code of Criminal Procedure, obligated anyone who attends the inspection procedure, whether the investigating judge, the judicial police officer, or qualified persons who were accompanied to conduct the inspection and who have access to papers, documents, physical electronic evidence or moral evidence, to withhold professional secrecy. A penalty of imprisonment from two months to two years and a fine ranging from 2,000 to 20,000 dinars shall be imposed on anyone who discloses a document resulting from the inspection or informs a person who has no legal capacity to view it, without the permission of the accused, his rights holders, the signatory to this document or the addressee⁵⁸, unless the necessities of the investigation require otherwise. Article 9 of Law 09/04 stipulates that anyone who uses the information obtained through surveillance or search outside the limits necessary for judicial investigations or investigations shall be subject to penalties stipulated in the applicable legislation.

Conclusion:

This study dealt with the subject of inspection in information systems as an innovative measure of investigation procedures to detect and seize electronic evidence

to prove the occurrence of some traditional crimes and electronic crimes resulting from the illegal use of information and communication technologies and their attribution to the accused, which are characterized by being located in a non-traditional electronic environment and are focused on physical and non-physical components that include electronic data and data, and require privacy in the inspector who needs scientific and technical knowledge, as well as privacy in the procedures and tools of searching for them and seizing them given the specificity of the obtained evidence and its nature, which is characterized by its characteristics over the traditional physical evidence.

Although the Algerian legislator has stipulated that it is permissible to inspect information systems, data storage systems and electronic data within the provisions of Law 09/04, it has not defined it and has not singled out its own provisions that are in line with the specificity of the procedure, and the electronic evidence extracted from it has not been known and has not included special provisions within the materials related to evidence. However, according to the Code of Criminal Procedure, it can be accepted as useful in uncovering the truth, taking into account that the inspection is carried out in accordance with the controls stipulated by the legislator upon inspection, the most prominent of which is the need to obtain judicial permission. If the inspector is faced with the problem of the interconnectedness of the devices, it varies according to whether the devices are within the country, then they may be inspected under the same conditions necessary to search the non-accused. If the scene of cybercrime extends outside the country, the matter is governed by international security and judicial cooperation agreements and rules of reciprocity.

Some of the most important findings that we can draw are :

- The Algerian legislator did not know the procedure for inspecting electronic systems and data storage systems, and did not regulate it by its own provisions, and was satisfied with the general rules stipulated in the Code of Criminal Procedure
- The Algerian legislator has adopted electronic evidence as a means of proving crimes, whether traditional or electronic, despite the absence of an explicit text stipulating the electronic evidence or regulating its provisions with special rules within the rules of evidence, whether in the provisions contained in Law No. 09/04 or in the provisions related to the rules of evidence stipulated in Article 212 et seq. of the Code of Criminal Procedure, despite its specificity, whether in terms of its electronic nature, or in terms of procedures or mechanisms for searching and seizing it, or in terms of the scene of evidence that may extend outside the country to include several countries, considering that electronic crime is a transnational crime, as it has only stipulated various procedures for seizing evidence of an electronic nature such as surveillance, electronic surveillance, recording of sounds, taking pictures, inspecting electronic systems, data storage systems and data.

- Obtaining permission to inspect an information system allows the search of all files in the system, and that the discovery of evidence and crimes other than those mentioned in the judge's permission is not a reason for the nullity of interlocutory procedures .

Therefore, we suggest:

1- The need to achieve a balance between the requirements of justice and security on the one hand and on the other hand the protection of electronic privacy as a constitutional right of persons through the strict legal regulation of the electronic inspection procedure, especially with regard to the judicial supervision and control of the procedure to ensure that the powers are not exceeded or the rights of individuals are violated, and to ensure that the personal data collected during the inspection is dealt with securely and confidentially , and with giving individuals whose devices or data are inspected the right to challenge the procedures whenever their electronic rights are violated.

2- The need to keep pace with substantive and procedural national legislation, including Algerian legislation, for the rapid development of information and communication technologies in order to achieve the principle of legality, especially with the increasing complexity of electronic crimes, with the need for the basic and specialized training of law enforcement agencies, including judges, investigative judges and judicial police officers, with the need to give a more important role to the National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies in the field of assisting inspection in the electronic environment.

3- The need for international security and judicial coordination and cooperation in the field of prevention and combating cross-border cybercrimes, especially with regard to cooperation in the field of implementing international judicial letters or in the field of investigators' work regarding the inspection of information systems, data storage systems and data when the inspection extends beyond the national borders of the state.

Citations:

- 1 -Law No. 09/04 of the Special Rules for the Prevention and Combating of Crimes Related to Information and Communication Technology, Official Gazette, No. 47 of 16/8/2009.
- 2-Adel Azzam SAQF AL hit, Jurisdiction in Cybercrimes : A Comparative Study, Journal of Law, Policy and Globalization, published by IISTE, Vol 22, 2014, p83. (pp75,84) (doi.org/10.7176/JLPG)
- 3-Awad Mohammed Awad, Code of Criminal Procedure, Part I, University Culture Foundation, 1989, p. 475.
- 4 -خبيلة هبة هروال، الجوانب الإجرائية للجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2007، ص 221 و ما يليها
- 5- Article2 of Law No. 09/04 on the prevention of crimes related to information and communication technologies.
- 6-Article 2 of Law No. 09/04 on the prevention of crimes related to information and communication technologies.
- 7-Article 3 of Law No. 18/07 dated 10/6/2018, relating to the protection of natural persons in the field of processing data of a personal nature. Official Gazette No. 34 dated 10/6/2018.
- 8-هلالى عبد الله أحمد، تفتيش نظم الحاسب الآلى وضمانات المتهم المعلوماتي، دار النهضة العربية القاهرة 2006، ص69.
- 9-Ali Hassan Al-Tawalbeh, Criminal Inspection of Computer Systems and the Internet, World of Modern Books, Irbid ,2004,p. 11.
- 10-The constitutional founder guaranteed legal protection for ordinary and even digital private life, which is a new concept in legal jurisprudence and approved by comparative legislation after the spread of the use of media and communication technologies by individuals and the emergence of what is known as the digital society and digital electronic life. Article 47 of the constitutional amendment of 2020 stipulates that everyone has the right to protect his private life and honor.
Everyone has the right to the confidentiality of his private correspondence and communications in any form, including digital and electronic private life.
- 11-Mahougnon Franc Kai, La preuve numérique à l'épreuve de la cybercriminalité, Mémoire de stage, Faculté de Droit et des Sciences Économiques, Université à Limoges, France, Année académique 2020/2021,p10 And what follows it.
- 12-Elsa Miha, Iris Pekmezi, Electronic evidence in the criminal process, Academic Journal of Business, Administration Law and Social Sciences, Vol. 10 No2, July, 2024,p4. (doi.org/10.2478/ajbals-2024-0010).
- 13-Orin S. Kerr, searches and seizures IN A digital world, The Harvard Law Review, Vol. 119 2 (Dec., 2005),Published By The Harvard Law Review Association ,p543 (pp. 585
- 14-ليندا بن طالب، التفتيش في الجريمة المعلوماتية،مجلة العلوم القانونية و السياسية،عدد 16 ،جوان 2017،ص491.
- 15-هلالى عبد الله أحمد، المرجع السابق،ص69.
- 16-Hussein Saeed Al-Ghafri , Criminal Policy in the Face of Cybercrime , Comparative Study, Dar Al-Nahda Al-Arabiya,2009, p. 470 .
- 17 -عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية، 2006، ص78.
- 18- Articles 76 and 78 of Law No. 25/14, dated 3/8/2025, enacting the Code of Criminal Procedure, Official Gazette No. 54, dated 13/8/2025.
- 17-Aisha bin Qarah Mustafa Hajiye, Electronic Evidence in the Field of Criminal Evidence, Comparative Study, New University House, Alexandria, 2009, p. 54.
- 18-هلالى عبد الله أحمد،المرجع السابق، ص 76.

19-Samir awed Mahmoud, Preuve de la criminalité sur Internet, Dar Al Nahda AlArabia l'édition et la distribution, édition2020,p233.

20 -Article 05, paragraph 2, of Law 09/04 .

21-Vergucht Pascal, La répression des délits informatiques dans une perspective internationale, thèse, Montpellier, 1996, p 336

22 -Article 05, paragraph 3, of Law No. 04/09 stipulates that " ... If it is previously found that the sought data that can be accessed from the first system is stored in an information system located outside the national territory, it shall be obtained with the assistance of the competent foreign authorities in accordance with the relevant international agreements and in accordance with the principle of reciprocity.

23- Service providers, according to the text of Article 2 of Law No. 09/04 :

1- Any public or private entity whose services users provide the ability to communicate through an information system and / or a communication system

2- Any other entity that processes or stores information data for the benefit of the said communication service or its users.

24-Articles 10 and 11 of Law No. 09/04.

25 -The jurist Alan Westin is among the pioneers who addressed the issue of privacy in the context of information processing as early as 1967, conceptualizing it as informational privacy and defining it as the right of individuals to determine when, how, and to what extent information about them is communicated to others. Similarly, the scholar Miller defines it as the individual's ability to control the life cycle of information pertaining to them. Consequently, electronic or digital privacy constitutes a modern iteration of privacy intrinsically linked to information systems and the Internet. Digital privacy aims to empower users exclusively to either prevent or permit third parties from accessing their data or disposing of information relating to their private lives.

See in this regard:

- مباركية مفيدة، الحماية الجنائية للحق في الخصوصية الرقمية في القانون الجزائري، مجلة الشريعة والاقتصاد، جامعة الأمير عبد القادر الإسلامية، المجلد 7 العدد13، الإصدار 1 لسنة 2018، 461.

26- On digital privacy: Benou, Zineb, Protection of Digital Privacy in Light of International Legislation, International Law Journal for Research Studies, Arab Center, Vol. 6, No. 17, November 2024, p 26.

Posted on the site <https://democraticac.de/?p=101118>.

27حطاب كمال،خصوصية التفتيش في البيئة الالكترونية،مجلة البحوث في الحقوق والعلوم السياسية،جامعة بن خلدون تيارت، المجلد 09،العدد01 السنة 2023(ص590- 608) ،ص592.

28- Mahougnon Franc KAI, Ibid , p18

29 -Article 48 of the 2020 Constitutional Amendment.

30 -See: Benou, Zineb, op. cit., pp. 29, 31.

31 -Article 12 of the Universal Declaration of Human Rights, adopted by the United Nations on 10 December 1948, provides: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

32 -Article 17 of the International Covenant on Civil and Political Rights (1966), adopted by the United Nations, stipulates: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence... Everyone has the right to the protection of the law against such interference or attacks."

33- Article 295 of the Penal Code provides: "Any person who enters a citizen's home suddenly, by deception, or by breaking in shall be punished by imprisonment from one to five years and a fine from 20,000 to 100,000 DZD."

- 34 -Law No. 04/15 dated of 10/11/2004, amending and supplementing Ordinance No. 66/156 of 8/6/1966 enacting the Algerian Penal Code, Official Gazette No. 71 dated of 10/11/2004
- 35 -Law No. 18/07 dated of 10/6/2018 on the Protection of Natural Persons in the Processing of Personal Data, Official Gazette No. 34 dated of 10/6/2018.
- 36 -Roger Merle et Andre Vitu, traite de droit criminel, Tome2, quatrième édition, édition Cujas, Paris, 1989, p. 757.
- 37 -Elsa Miha, Iris Pekmezi, Ibid, pp 4, 6.
- 38 -In accordance with the provisions of Articles 4 and 5 of Law 09/04 on the prevention of crimes related to information and communication technologies.
- 39 -The Algerian legislator stipulated many crimes committed by or through automated treatments, whether in the Real Estate Law No. 66/156 or in special laws such as Law No. 18/07 of 10/6/2018 on the protection of natural persons in the field of processing data of a personal nature, and Law 20/05 of 28/4/2020, on preventing and combating discrimination and hate speech. and others, which gave the legislator to the judicial authority or its delegate to conduct electronic searches in order to seize the electronic evidence to detect the crime and seize the perpetrators.
- 40- Article 76 of the Criminal Procedure Law No24/14 stipulates that (seized objects or documents shall be closed and stamped, if possible. If it is not possible to write on them, they shall be placed in a container or bag on which the judicial police officer shall place a strip of paper and stamp it with its seal . Inventory of seized items and documents shall be made.)
- 41- Adel Azzam SAQF AL hit,ibid,p75.
- 42 -Iris Pekmezi, Lirime Çukaj Papa., Criminal offenses in the field of Cybernetics related to computer – Computer forgery and computer fraud. European Journal of Economics, Law and Social Sciences, Vol 8, No2, June 21, 2024, p5. (doi.org/10.2478/ejels-2024-0010).
- 43 -Article 48 of the Constitutional Amendment of 2020 stipulates that no inspection shall be carried out except in accordance with the law and within the framework of respecting it. No search except by a written order issued by the competent judicial authority.
- 44 -Article 141 of law no 24/14 containing the Code of Criminal Procedure stipulates that (If it is not possible for the investigating judge to carry out all investigation procedures himself, he may assign judicial police officers to carry out all necessary investigation work within the conditions stipulated in Articles 234 to 238 .)
- 45- Aisha bin Qarah Mustafa, op. Cit., P. 63.
- 46 -Article 5 of law no 09/04.
- 47- Sami Hosni Al-Husseini, The General Theory of Inspection in Egyptian and Comparative Law, Dar Al-Nahda Al-Arabiya ,Cairo, 2003, p. 100.
- 48 -Jameela Said Musbah Shouran, Inspection Permission in Electronic Circles, Abhat Journal, Faculty of Arts, Sirte University, Libya, Volume. ISSUE 1. March 2023,p116. (129)
- 49- Jameela Said Musbah Shouran,Ibid,p116.
- 50 -Article 75/p3 of law no 24/14 containing the Code of Criminal Procedure" The aforementioned warrant must include a statement describing the offense that is the subject of the search for evidence, as well as the addresses of the premises to be visited, searched, and subjected to seizure, failing which it shall be null and void."
- 51 -Aisha bin Qarah Mustafa, op. Cit., P. 63
- 52 -Articles 16 and 17 of Law No. 09/04
- 53- Article 18 of Law No. 09/04
- 54 -Article 76 of Code of Criminal Procedure24/14
- 55 -Yann Padova, Un aperçu de lutte contre la cybercriminalité en France, revue de science criminelle et de droit pénale, n° 4, Dalloz, 2002, p770.
- 56 -Elsa Miha, Iris Pekmezi, Ibid,p p 6,7.

57- Article 73 of the Code of Criminal Procedure stipulates that: "The judicial police officer shall seize everything that may lead to the truth." Article 160 stipulates: It is not permissible for the investigating judge to seize only things and documents that are useful in revealing the truth or whose disclosure may harm the course of the investigation)

58- Articles 161 of law No24/14 containing the Code of Criminal Procedure"shall be punishable by imprisonment ranging from two (2) months to two (2) years and a fine ranging from 20,000 DZD to 200,000 DZD, any person who discloses or disseminates a document obtained through a search to an individual lacking legal authority to access it, without the consent of the accused, their successor, the signatory of the document, or the intended recipient thereof; likewise, any person who makes use of information that has come to their knowledge therefrom, unless such disclosure or use is necessitated by the exigencies of the judicial investigation."

.