

" Objective controls for inspection in cybercrimes"

Bechane Abdenour ^{1*} Faculty of Economics, Business and Management Sciences - Setif - Algeria, *abdenour-bechane@live.fr*

Associate Professor (Grade A)

Received: 18/08/2025

Accepted: 30/09/2025

Published: 01/06/2026Y

ملخص:

يعد التفتيش من بين أهم وأخطر الإجراءات التي ترتبط بالدعوى العمومية، فمن جهة هو سبيل مهم لضبط الأدلة الجنائية، ومن جهة أخرى مرتبط بحساسية حرمة الحياة الخاصة من خلال حرمة المكان محل التفتيش.

ان هذه الفكرة تطرح صعوبة أثناء التحقيقات بصدد جرائم ترتكب في العالم المادي، فما بالك في العالم الافتراضي الذي يطرح عدة إشكالات سواء من حيث صعوبة حصر مكان التفتيش أو من حيث عدم وضوح أليات وطرق لضبط الأدلة الجنائية في العالم الافتراضي بشكل يجعل من إجراءات التحقيق شرعية بما ينعكس إيجابا بشرعية الاتهام ومن ثمة المحاكمة ونتائجها، بذلك موضوع بحثنا تبيان الضوابط الموضوعية للتفتيش بصدد أية جريمة معلوماتية.

كلمات مفتاحية: تفتيش، بيئة معلوماتية، ضوابط موضوعية، تشريع

Abstract:

Search and seizure stands as one of the most critical and intrusive procedures in criminal proceedings. On one hand, it is a vital tool for securing forensic evidence, yet on the other, it clashes with the fundamental This tension presents a significant challenge even when investigating

* Bechane Abdenour

" Objective controls for inspection in cybercrimes"

crimes committed in the physical world. This difficulty is compounded in the virtual realm, which raises numerous issues.

These include the challenge of defining the scope of a search and the lack of clear mechanisms and procedures for seizing digital evidence. Without such clarity, the legitimacy of the investigative process itself is called into question, which in turn compromises the legality of the indictment, the subsequent trial, and its outcome.

Therefore, the objective of this research is to elucidate the substantive controls that govern search and seizure in cases of cybercrime.

Keywords:

Inspection, informatics Environment, Objective Controls, Legislation

1. INTRODUCTION

The situation has been exacerbated by the revolution in information technology, which has created a new spatial and temporal domain with unique characteristics that distinguish it from the physical world. This has also led to a new phenomenon known as cybercrime.

The cybercriminal, operating in the virtual realm, is more dangerous than a criminal in the real world. This heightened danger stems from the ease and speed of attacking individuals' interests within the virtual world on the one hand, and from the absence of geographical boundaries in this world on the other.

A new challenge has thus emerged for legal systems, shifting from a substantive approach to a procedural one in order to address cybercrime. This is evident in the various penal procedures used to prosecute a cybercriminal, from the moment the crime is committed to their trial and subsequent punishment, with search procedures being among the most prominent.

A search is considered one of the primary investigation procedures (Fathi, 1981,P 449). Its purpose is to find evidence of a crime, whether it

involves searching the person themselves or their residence. Its seriousness and importance stem from the constitutional protection of the sanctity of individuals and their homes, based on what is contained in Articles 39 and 40 of the Algerian Constitution (journal, 2016 n 14).

However, a legal issue arises when this procedure is applied to a cybercrime committed in a virtual space.

This issue concerns the extent to which general procedural rules for searches can be applied to cybercrimes. In other words, **is a computer system subject to the search procedures applied within general procedural rules, or are special procedures required that are suitable for the nature and unique characteristics of the digital domain?**

To address this issue, we will focus on the substantive controls for searching in the context of cybercrimes, specifically in two parts: the first covers the justification for searching information systems, and the second examines the subject of the search itself.

2- The Justification for Searching Information Systems

The justification for a search, as a procedure, arises from the occurrence of a cybercrime (Naudin, 2008, p 22). This includes the existence of an accusation against a specific person or several individuals for committing the crime, in addition to strong evidence indicating that the crime's location or a place belonging to the person to be searched exists.

2-1 The Occurrence of a Cybercrime

For search procedures to be undertaken, a cybercrime must have been committed, or as the Algerian legislator calls them, crimes affecting automated data processing systems, which were introduced in the new Section 7 bis as part of the Penal Code amendment (journal, law 04-15, 2004, p 8).

" Objective controls for inspection in cybercrimes"

It is noted that these crimes were classified as misdemeanors only, not felonies. This renders Article 44 of the Code of Criminal Procedure inapplicable to searches concerning these crimes. In fact, Article 45 of the same code explicitly exempted search procedures stipulated in Article 44 from being applied when the case involves a range of crimes, including those affecting automated data processing systems (Abdenour Bechane, 2018,P304) (law18-06, 2018) (Official, 2006, p4).

The legislator then introduced a special provision, Article 5 of Law No. 09-04, which outlines specific rules for the prevention and combat of information and communication technology-related crimes. This article refers to Article 4, stating: "Competent judicial authorities as well as judicial police officers, within the framework of the Code of Criminal Procedure and in the cases stipulated in Article 4 above, may access, for the purpose of searching, even remotely, the following: a- An information system or a part thereof, as well as the information data stored within it. b- A data storage system..."

Article 4 permits the use of technical surveillance in several cases, including case (b), which is referred to in Article 5. This case involves the availability of information about fraud and attacks on an information system in a manner that threatens public order, national defense, state institutions, or the economy.

A negative point to note is that the Code of Criminal Procedure, in its 2006 amendment, exempted searches related to crimes affecting automated data processing from the application of its Article 44. This was before the issuance of Law No. 09-04 concerning the prevention and combat of IT-related crimes in August 2009. This raises the question of which law was applied to searches concerning cybercrimes during the period from December 2006 to August 2009, considering that Section 7 bis of the Penal Code was introduced by Law No. 06-23 in December 2006.

This issue implies one of two things: either searches were not conducted at all for this type of crime, which is unlikely, or the rules stipulated in Article 44 of the Code of Criminal Procedure were applied

despite the explicit exception in Article 45 of the same law, which would be in violation of it.

On a positive note, the Algerian legislator permitted the search of an information system upon the mere possibility of an attack, not just the attack itself. This reflects the legislator's commitment to protecting important interests by safeguarding the information systems linked to them (Tariq Ibrahim Al-Desouki Attia, 2005, p 382).

2-2 Attributing the Criminal Act to the Cybercriminal

By cybercriminal, we mean the natural or legal person who carries out the attack on the information system. There must be strong and sufficient evidence to suggest their commission or participation in the cybercrime. This means there must be clear and unambiguous signs, indications, and evidence that confirm the attribution of the criminal act to the cybercriminal, whether as a principal perpetrator or an accomplice Bachan Abdel Nour, 2018, p. 80) (Ma'touq, 2014,p92) (Qahwaji, 2009,p50).

2-3 The Availability of Strong and Sufficient Evidence of the Commission of a Cybercrime

To carry out a search, it is a prerequisite to have strong and sufficient evidence that makes the commission of a cybercrime by the perpetrator likely. Evidence is revealed by inferring an unknown fact from a known one based on probability and weighing the evidence. The sufficiency of the evidence means there are certain indications based on rational logic that appear at the beginning of the emergence of circumstances or facts, from which the criminal act can be inferred, suggesting at first glance that a criminal act has been committed or was committed by a specific person (Tariq Ibrahim Al-Desouki Attia, 2005, p386) Sami Jalal Faqi Hussein, 2011, p121) (Al-Fil, 2012,p50).

A search procedure is only conducted if there is strong and sufficient evidence that a particular location or the cybercriminal possesses any tools

" Objective controls for inspection in cybercrimes"

used in or facilitating the commission of the cybercrime. These could be physical tools like a computer and its accessories, or intangible ones like electronic documents seized within the information system or the network (Al-Hayt, 2011,pp51-52).

3- The Subject of the Search in Cybercrimes

As previously stated, the Algerian legislator addressed searches in Chapter 3 of Law 09-04, which contains special rules for the prevention and combat of information and communication technology-related crimes. Specifically, Article 5 uses the phrase **"search of information systems."**

This term is defined in Article 2 of the same law as "any separate system or group of interconnected or linked systems, where one or more of them perform automated data processing in execution of a specific program."

This definition is supported by Article 19/1 of the Budapest Convention, which, under Chapter 4 titled "Search and Seizure of Stored Computer Data," states:

"1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a- A computer system or a part thereof as well as the computer data stored therein and on its territory; b- A computer storage medium that allows for the storage of computer data..."

Therefore, an information system comprises both a physical and a non-physical (intangible) component. This raises the question of whether these components are subject to a search. To answer this, we must examine the searchability of the physical components of the information system, and then its intangible components.

3-1 The Searchability of the Physical Components of an Information System

By the physical components of an information system, we mean the tangible side through which data and information are handled for

processing, storage, input, and output. This includes computers and related elements such as input/output devices and processing units (Al-Halabiq, 2001, p 41).

The ruling on searching the physical components of an information system is tied to the places where they may be found, which opens up a discussion about searching physical IT components in a person's possession or placed in a private location like a residence.

The first case relates to a person being the subject of an IT search. The person could be a computer user, a service provider (Al-Hiti, 2006,p2)(Siab,2014,p23) (Hassouna, 1993,p407), a software expert, or someone who works in maintenance or as a manager of an information system. This makes them the possessor of devices, equipment, and information for mobile phones and laptops that can be considered the individual's belongings without distinguishing if they are their property or someone else's, or if they are carrying them or have them in their car or on a public road (Ibrahim, 2009,p214-215).

It is worth noting that legal scholars have differed on considering a car a searchable location based on a personal search. Some have tied it to the necessity of a search based on searching a residence, or including it within belongings if it is on a public road. However, French and subsequently Egyptian jurisprudence has considered a search warrant to include everything connected to the person, including a private car (. T. I.-D, 2005,p394).

In the second case, if the physical components related to the cybercrime are located inside a person's residence, they are subject to a search only as part of a residential search procedure, since a physical search of these materials requires entry into the residence itself, unless there is a special provision to the contrary.

The Algerian legislator did not explicitly provide for this in Law 09-04 concerning the organization of specific rules for the prevention and combat of IT-related crimes, although the wording of Article 5 suggests opening the door to searching information systems by accessing the information network.

3-2 The Searchability of the Intangible Components of an Information System

Opinions have differed on the acceptability of searching logical or intangible components. Some have permitted the seizure of electronic data in its various forms, justifying this by arguing that the permission to search physical items legitimizes the search of the non-physical aspects, such as programs and other data (Harwal, 2013,p238-239).

A second opinion suggests that it is not possible to deal with an information system directly in its non-physical form as is the case with its physical materials (Col, 1993,p111).

This highlights a shortcoming in legislative texts on this matter. This school of thought proposes the possibility of searching for and seizing processed materials via the computer or data, with the goal of modern technical development being to search for physical evidence while intangible evidence takes the form of material processed by the computer (Hegazy, 2002,p379-380)

Returning to Algerian legislation, particularly the texts of the Code of Criminal Procedure, we find that the legislator, through Article 50 et seq. of Law No. 18-07 of July 10, 2018, concerning the prevention and combat of cybercrimes, granted judicial police officers the authority to examine and handle digital evidence, including the searching of electronic devices, under the supervision of the Public Prosecution or investigative judges.

As the case may be. This applies in cases where a cybercrime is suspected, a matter confirmed by Article 45/7 of the Code of Criminal Procedure when it implicitly referred to Law 18-07.

Furthermore, the Code of Criminal Procedure, through Article 65 bis 5, authorized the Public Prosecutor or the investigative judge in crimes affecting automated data processing systems to permit the interception of wired and wireless communications, recording calls, and capturing images, all without the need for the consent of the monitored person, while respecting the issue of privacy within the framework of professional secrecy.

Thus, the Algerian legislator expanded the scope of a search to encompass another computer connected to the accused's computer, whether inside or even outside the country, when necessary. This is always in the context of working to uncover those involved in the crime by mandating the search for this data to achieve this goal.

4. RESULTS AND DISCUSSION

It is evident from this study that the international community is always striving to enact laws that criminalize all acts that could destabilize society in its virtual world, both substantively and procedurally. This is similar to the Algerian legislator, who issued Law 18-07 on July 10, 2018, regarding the prevention of cybercrimes and introduced amendments to the Code of Criminal Procedure via Ordinance 15-02 of July 23, 2015.

However, these amendments are insufficient, especially concerning search procedures, due to the lack of a precise and comprehensive definition of the powers and procedures related to searching information systems. This is particularly true for searches that extend their effect outside the country's territory to preserve the probative value and legitimacy of digital evidence, and consequently its validity for use in proving the criminal act.

Based on this, the following recommendations can be made:

- Precisely define the powers and procedures related to searching information systems.
- Establish a specialized field for investigating cybercrimes.
- Provide training courses for judicial police in the field of cybercrimes.
- Move towards having specialized judges for cybercrime cases.
- Establish special laboratories and units to analyze both physical and intangible digital evidence, operating under the supervision of specialized technical personnel.

" Objective controls for inspection in cybercrimes"

- Work on concluding international cooperation agreements for the collection of evidence and for digital searches.

5. Bibliography List :

1. Books :

- 1- Ahmed Fathi Sorour (1981), *Al Wasit in Criminal Procedures*, Dar Al Nahda Al Arabiya, Egypt, p. 449. Also see: Mahmoud Naguib Hosny (1988), *Explanation of the Code of Criminal Procedure*, Dar Al Nahda Al Arabiya, Egypt ;
- 2- Moulai Miliani Baghdadi (1992), *Penal Procedures in Algerian Legislation*, National Book Foundation, Algeria;
- 3- Christophe Naudin (2008), *Cybercriminalité identitaire*, Revue Cahiers de la sécurité “La Criminalité numérique”, N6, published by the National Institute for Advanced Security Studies (INHES), France ;
- 4- Tariq Ibrahim Al-Desouki Attia (2005), *Information Security (The Legal System for Protecting Information)*, Dar Al Jami'a Al Jadida, Alexandria, Egypt ;
- 5- Jamal Ma'touq (2014), *An Introduction to Criminal Sociology (The Most Important Theories Explaining Crime and Deviance)*, Dar Al Kitab Al Hadith, First Edition, Cairo, Egypt ;
- 6- Ali Abdel Qader Al Qahwaji (2009), *Criminology and Penology*, Al Saadani Press, Egypt ;
- 7- Sami Jalal Faqi Hussein (2011), *Search in Cybercrimes (An Analytical Study)*, Dar Al Kutub Al Qanouniya, Egypt ;
- 8- Ali Adnan Al-Fil (2012), *Procedures for Investigation, Evidence Collection, and Preliminary Investigation in Cybercrime (A Comparative Study)*, Dar Al Kutub wa Al Wathaiq Al Qawmiya, Mosul, Iraq ;
- 9- Adel Azzam Saqf Al-Hayt (2011), *Crimes of Slander, Libel, and Contempt Committed via Electronic Media (Internet and Mobile Phone Networks and through Traditional and Automated Media and Publications - A Comparative Study)*, First Edition, Dar Al Thaqafa wa Al Tawzi, Amman, Jordan ;
- 10-: Khalid Ayad Al-Halabi (2001), *Investigation and Inquiry Procedures in Computer and Internet Crimes*, First Edition, Dar Al Thaqafa for Publishing and Distribution, Amman, Jordan ;

" Objective controls for inspection in cybercrimes"

- 11-Hammad Muhrij Al-Hiti (2006), *Computer Crimes (Their Nature, Key Forms, and Difficulties They Face) An Analytical Study of the Locations of Attacks on Computers and the Position of Criminal Legislations*, First Edition, Dar Al Manahij for Publishing and Distribution, Amman ;
- 12-Hakim Siab (2014), *IT and the Law*, First Edition, Dar Wael for Publishing, Jordan ;
- 13-Zaki Zaki Amin Hassouna (October 1993), *Computer Crimes and Other Crimes in the Field of Information Technology*, The Sixth Conference of the Egyptian Society for Criminal Law, Cairo ;
- 14-Khalid Mamdouh Ibrahim (2009), *The Art of Criminal Investigation in Electronic Crimes*, First Edition, Dar Al Fikr Al Jami'i, Alexandria ;
- 15-Nabila Heba Harwal (2013), *The Procedural Aspects of Internet Crimes - in the Phase of Evidence Collection (A Comparative Study)*, Dar Al Fikr Al Jami'i, Alexandria ;
- 16-Durham Col (1993): "The Emerging Structures of Criminal Information Law Tracing the contours of Newparading," R.I.D.P ;
- 17-Abdelfattah Bayoumi Hegazy (2002), *Principles of Criminal Procedure in Computer and Internet Crimes*, Dar Al Kutub Al Qanouniya, Egypt ;

2-Law:

- 1- Articles 39 and 40 of the Algerian Constitution, amended by Law 16-01 of March 6, 2016, Official journal published on March 7, 2016 ;
- 2- Section 7 bis by virtue of Law No. 04-15 of November 10, 2004, amending and supplementing Ordinance No. 66-155 of June 8, 1966, which includes the Penal Code, Official journal of November 10, 2004, No. 71 ;

- 3- Article 44 of Ordinance 66-155 of June 8, 1966, as amended and supplemented by Law 18-06 of June 10, 2008, concerning the Code of Criminal Procedure.
- 4- Article 45, paragraph six of the second part, amended by Law 06-22 of December 20, 2006, Official Gazette of December 24, 2006, No. 84 ;
- 5- Law 09-04 of August 5, 2009, containing specific rules for the prevention and combat of crimes related to information and communication technology, Official journal of August 16, 2009, No. 47 .

3- Doctoral Thesis :

- 1- Bachane Abdel Nour (2018), *The Substantive Aspects of Addressing -Cybercrime*, PhD Thesis in Sciences, University of Algiers-1-.