Journal of Ecohumanism
2025
Volume: 4, No: 4, pp. 1586 – 1591
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i4.6892

Infiltration as a Special Investigative Technique in Combating Cybercrime

Henni Rachida[1], HAZZAB Nadia[2]

Abstract

Infiltration is a new technique introduced by the legislator in the 2006 amendment to the Code of Criminal Procedure. It is used when the necessities of investigation and inquiry require it in the case of serious crimes previously mentioned. The Algerian legislator dedicated Chapter Five of the Code of Criminal Procedure to regulate this measure.According to Article 65 bis 12/1, infiltration is defined as the act of an authorized investigator monitoring individuals suspected of committing a crime, or penetrating a criminal group by deceiving them into believing that he is a partner. Judicial police officers and agents are allowed, for this purpose, to use a false identity and, when necessary, to commit certain crimes without being held criminally liable. This is aimed at monitoring suspects and uncovering their criminal activities while concealing the officer's true identity.Given the dangerous nature of this procedure, which puts the officers at risk and requires courage, high competence, and precision, the legislator has subjected it to strict legal conditions and controls.

Keywords: *Leakage, Electronic theft, Judicial police officer, Follow-up, Investigation.*

Received: 28.03.2025 **Accepted: 30.07.2025**

Introduction

There is no doubt that cybercrime emerged as a result of the misuse of the Internet, in parallel with the evolving capabilities of criminal thinking and behavior. This has led to the appearance of new forms of prohibited conduct, most notably those related to information technology crimes or more precisely, cybercrimes. Due to the specific nature of these crimes, particularly in terms of their elements and the circumstances under which they are committed, the legislator was compelled to reconsider procedural matters, especially those related to the issue of evidence. Unlike traditional crimes, in which gathering evidence and identifying perpetrators is relatively straightforward, cybercrimes involve a distinct form of evidence—namely, technical evidence. This type of evidence must be extracted from the digital environment, which serves as the crime scene in cyber offenses.

Investigation is one of the most important procedures carried out after a crime has occurred, given its critical role in verifying the incident, establishing material evidence against the perpetrators, and uncovering the truth in order to determine whether the accused is guilty. In the context of cybercrime, the investigative process requires the collection and analysis of a maximum number of digital clues. Thus, the infiltration procedure in this type of crime relies heavily on alertness, intelligence, and the ability to operate undercover. It is entrusted to specialized bodies, namely judicial police officers, to keep pace with criminal activity and uncover the methods used to commit crimes in the virtual electronic environment.

This calls for legislative intervention to develop procedural rules specific to the authorities responsible for investigating and detecting cybercrime, as well as the introduction of new methods to confront such crimes. Accordingly, the following central question arises:

How has the Algerian legislator regulated the infiltration procedure, and how effective is it in detecting cybercrime?

[1] Faculty of Law and Political Science, University of Saida, Dr Moulay Tahar, Algeria, Email : henniracha81@gmail.com ; https://orcid.org/0009-0004-9511-1666

[2] Faculty of Law and Political Science, University of Saida, Dr Moulay Tahar, Algeria, Email : nadia.hazzab@univ-saida.dz ; https://orcid.org/0009-0008-6151-3367

Journal of Ecohumanism
2025
Volume: 4, No: 4, pp. 1586 – 1591
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i4.6892

To answer this question, we have divided this research paper into two main sections:

- The first section is dedicated to the concept of infiltration,
- While the second section addresses the effects of infiltration in cybercrime cases.

Section One: The Concept of Infiltration in Cybercrime

The legislator introduced the infiltration procedure through Law No. 06-22 dated December 2006, which amended and supplemented the Code of Criminal Procedure. Accordingly, we shall address this section in two parts: the first part discusses the definition of infiltration, while the second part will deal with the conditions of infiltration in cybercrime.

First: Definition of Infiltration

Infiltration is considered a newly introduced and highly sensitive technique that poses serious risks to the safety of judicial police forces. It requires courage, a high level of skill, and precision in execution . For this reason, the Algerian legislator included it as part of the strategic plan to combat cybercrime, as reflected in Law No. 06-22 dated 10-12-2006, which amended and supplemented the Code of Criminal Procedure .

Legal scholars have defined infiltration as a special investigative technique that allows a judicial police officer or agent to penetrate and operate within a criminal group, under the supervision of another officer responsible for coordinating the operation. The aim is to monitor suspects and uncover their criminal activities by concealing the infiltrator's true identity and presenting themself as a perpetrator, accomplice, or associate . From a security perspective, infiltration is a carefully prepared and organized operation aimed at penetrating a criminal environment in order to understand it thoroughly by uncovering its major and hidden activities. This environment is pre-identified in order to collect accurate and reliable information and understand its internal dynamics and specific characteristics.

The Algerian legislator has provided a clear definition of infiltration in Article 65 bis 12 of the Code of Criminal Procedure, stating: "A judicial police officer or agent, under the responsibility of the judicial police officer in charge of coordinating the operation, may monitor persons suspected of committing a felony or misdemeanor by making them believe that they are an accomplice, participant, or associate.

The officer or agent may, for this purpose, use a false identity and may, if necessary, commit the acts mentioned in Article 65 bis 14 below. However, under penalty of nullity, such acts must not constitute incitement to commit crimes."

From the reading of the above article, it is evident that the infiltration procedure is an unfamiliar and complex measure that directly touches upon fundamental human rights and freedoms. To better safeguard these rights, legal guarantees have been established to serve as effective safeguards against abuse. Thus, the use of this procedure must comply with a legitimate legal framework and can only be conducted with prior authorization from the competent judicial authority, typically the territorially competent Public Prosecutor or the Investigating Judge, as stipulated in Article 65(11) of the Code of Criminal Procedure. This article authorizes the Public Prosecutor or the Investigating Judge after notifying the Public Prosecutor to grant permission to a judicial police officer or agent to carry out an infiltration operation, by referring to Article 65 bis 05.

Upon review of Article 65 bis 05, we find that it lists specific crimes to which this procedure may apply, including: "...where necessary for the investigation of a crime in flagrante delicto or for preliminary investigation into drug-related offenses, transnational organized crime, offenses against automated data processing systems, money laundering, terrorism, offenses related to exchange regulations, and corruption..."

Journal of Ecohumanism
2025
Volume: 4, No: 4, pp. 1586 – 1591
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i4.6892

From the analysis of this article and the preceding one, we can deduce that infiltration applies only to the offenses explicitly mentioned in Article 65 bis 05, including crimes that target automated data processing systems. Within this context, infiltration can be imagined in cybercrime cases where a judicial police officer or agent enters the virtual world by, for example, infiltrating specific websites, participating in chat rooms, or establishing direct contact with suspects, appearing as one of them while using false identities or pseudonymous profiles thus aiming to gather information from hackers about how they breach systems.

The practical definition of infiltration in cybercrime involves penetrating a difficult-to-access place or target referred to as the "virtual space" in order to uncover the intentions of criminal groups , using disguise and identity theft tactics to gain the suspect's trust and determine the nature and duration of their activities .

Second: Conditions for the Infiltration Procedure in Cybercrime

The Algerian legislator has surrounded the infiltration procedure in cybercrime with a set of formal and substantive conditions, outlined as follows:

1. *Formal Conditions:*

To successfully carry out the infiltration operation, the judicial police officer must observe several essential procedural requirements specific to cybercrime infiltration.

- *Submission of a Report on the Infiltration Operation:*

As a general principle, the judicial police officer must prepare a detailed report addressed to the Public Prosecutor prior to commencing the infiltration operation. This requirement is stipulated in Article 65 bis 13 of the Code of Criminal Procedure, which states that the officer in charge of coordinating the infiltration is responsible for drafting a report that includes the necessary elements to identify the cybercrime, as well as all information obtained by the officer that may support the operation. The report must contain the following elements:

o *Nature of the Crime:*

As defined by the legislator in Article 65 bis 05 of the Code of Criminal Procedure, which includes crimes against automated data processing systems.

o *Justification for Resorting to Infiltration in Cybercrime:*

The officer must specify the reasons and circumstances that warrant the use of this high-risk procedure, especially since it is often linked to the need for in-depth investigation in complex cybercrime cases. The officer must present compelling justifications to the Public Prosecutor by basing the request on several factors that demonstrate the necessity of this operation.

o *Identification of the Judicial Police Officer:*

The officer's full identity must be specified, including name, surname, position, rank, and the department to which they belong.

o *Identification of Cybercrime Elements:*

This includes all relevant information about the crime and its components, such as the identities (real or alias) of suspected individuals, the nature of the criminal acts attributed to each, the place and time of occurrence, and the tools used in committing the crime.

o *Request for Authorization:*

Journal of Ecohumanism
2025
Volume: 4, No: 4, pp. 1586 – 1591
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i4.6892

The officer must submit a request for authorization from the competent judicial authority, in accordance with Article 65 bis 11 of the Code of Criminal Procedure. This request must accompany the report in order for the Public Prosecutor to grant permission. The authorization is issued under the Public Prosecutor's responsibility and supervision, and must contain the conditions specified in Article 65 bis 15, namely:

Written Form:

The legislator requires that the authorization be in written form and issued by the competent judicial authority, under penalty of nullity, as per Article 65 bis 15.

Justification of the Authorization:

The Public Prosecutor must explain the reason for authorizing the procedure, in order to justify the need for further investigation into the circumstances of the cybercrime, pursuant to Article 65 bis 05.

Identification of the Officer in the Authorization:

The authorization must contain the officer's full identity, including name, surname, rank, and affiliation, as he is the responsible party for this critical operation.

Specification of the Duration of the Infiltration:

The Public Prosecutor must set a specific duration for the operation, which cannot exceed four (4) months, as stipulated in Article 65 bis 15. The authorization must also include the starting and ending dates of the operation . Notably, the start of the operation does not necessarily coincide with the date the authorization is issued, since the operation may require at least a week of preparation, especially given that cybercrime investigations demand advanced tools and techniques.

The Public Prosecutor or Investigating Judge who authorized the operation may extend it for an additional 4 months if the officer has not achieved the intended objectives or if investigative necessity requires it, according to Article 65 bis 14. If another 4-month extension proves insufficient, a final extension of 4 additional months may be requested under Article 65 bis 17. After this final period, the officer must withdraw from the operation, even if the objective has not been reached. The judicial authority may also order the termination of the operation at any time depending on the circumstances. The officer must preserve professional secrecy and the confidentiality of the authorization, which must be placed in the file even after the operation has concluded.

2. *Substantive Conditions for Infiltration in Cybercrime:*

The substantive conditions for implementing infiltration in cybercrime include the following:

- *Identification of the Crime and Its Nature:*

The crime must relate specifically to cyber offenses so that the judicial police officer may classify it under crimes against automated data processing systems, in accordance with Article 65 bis 05.

- *Motivation for Resorting to Infiltration:*

The officer must support the report with a legitimate reason for conducting the infiltration, often based on the necessity of investigating cybercrime. If the report lacks convincing justification, the judicial authority may reject the request and declare the entire procedure null and void.

- Confidentiality:

Journal of Ecohumanism
2025
Volume: 4, No: 4, pp. 1586 – 1591
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i4.6892

The officer must adhere to professional confidentiality as a general rule and to the confidentiality of the infiltration procedure as a specific rule, regardless of circumstances. According to Articles 65 bis 16 and 65 bis 18, failure to maintain confidentiality results in the nullity of the procedure and disciplinary action against the officer by their employing body. Criminal liability may also be imposed by the Indictment Chamber.

Examples of confidentiality requirements include:

o Use of a false identity as per Article 65 bis 12.

o Non-inclusion of the authorization document in the procedural file until after the operation has fully concluded, as per Article 65 bis 15.

- *Determination of the Competent Authority to Conduct the Operation:*

According to Article 65 bis 12, the competent authority to conduct infiltration is the judicial police officer, who bears primary responsibility for the operation. The officer must ensure thorough and careful preparation, assisted by subordinate agents.

Section Two: Effects of Infiltration in Cybercrime

Once authorization has been granted by the Public Prosecutor for the judicial police officer to execute the infiltration operation, in accordance with the conditions specified in the permit, a number of legal consequences arise from this procedure. We will address two key aspects: first, the mobilization of material and legal means; and second, exemption from liability.

First: Mobilization of Material and Legal Means

According to Article 65 bis 14 of the Code of Criminal Procedure, the Algerian legislator allows the infiltrator to mobilize material means in favor of the criminal cell. This includes providing support in various forms, such as transportation, delivery, possession, or shelter.

With regard to legal means, this refers to the provision of official documents when necessary—such as issuing a driver's license or national identity card without going through the competent administrative authority. In such cases, the officer may resort to forgery in order to maintain the complete confidentiality of the infiltration operation.

Second: Exemption from Liability

It is well established in law that any person who engages in unlawful conduct commits an offense and is subject to legal liability both criminal and disciplinary. This is the general rule. However, the exception to this rule is that some individuals may commit unlawful acts and not be held liable, as explained below:

Criminal Liability:

According to Article 65 bis 14 of the Code of Criminal Procedure, "Judicial police officers and agents authorized to carry out the infiltration operation, as well as persons recruited for this purpose, shall not be criminally liable..."

From this provision, it is clear that judicial police officers and their agents are not subject to criminal liability for the acts committed during the infiltration operation, as long as these acts fall within the scope of the legal authorization granted. This aligns with the exceptions stipulated in Article 39 of the Algerian Penal Code , whereby such acts are considered justified (grounds for justification). Therefore, any unlawful actions committed by the officer or agent during the operation do not subject them to criminal prosecution.

Journal of Ecohumanism
2025
Volume: 4, No: 4, pp. 1586 – 1591
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i4.6892

Civil Liability:

This concerns all actions taken by the infiltrator whether civil or commercial while executing the infiltration operation, such as entering into contracts that create legal obligations (e.g., sales contracts, marriage contracts, etc.).

Here, it is worth noting that the Algerian legislator has remained silent on the matter of civil liability, offering no legal provisions or clarifications. This raises an important question:

What is the legal status of contracts concluded by the infiltrator, and do their effects continue even after the infiltration operation ends?

Conclusion

Through our examination of the topic concerning the infiltration procedure in cybercrime as a specific and modern investigation technique provided for in the Code of Criminal Procedure as amended by Law No. 06-22 we concluded that the Algerian legislator, within the framework of combating cybercrime, has established effective mechanisms and tools that keep pace with the evolution of criminal methods. These mechanisms assist in uncovering the plans of organized, covert, and complex criminal groups by introducing new investigative techniques that did not previously exist, and which, when used unlawfully, would render the resulting evidence inadmissible.

Therefore, the infiltration procedure is considered a legally authorized and operationally critical measure for the officers and agents involved, as it is carried out within criminal groups without them being aware of the infiltrator's true identity. This is done only after obtaining authorization from the competent judicial authority, namely the territorially competent Public Prosecutor and, following notification of the Public Prosecutor, the Investigating Judge. Additionally, all formal and substantive conditions related to conducting infiltration operations in cybercrime must be met.

It is also worth noting that any criminal acts committed by the officer or one of their agents during the execution of the infiltration procedure do not subject them to criminal liability, as such acts fall within the scope of legal authorization and are therefore considered justified acts (grounds for justification).

References

Books:
Ahmed Ghai, The Essentials of the Organization and Duties of the Judicial Police, 5th edition, Houma Publishing, Algeria, 2011.
Zbikha Zidan, Cybercrime in Algerian and International Legislation, 2011 edition, Dar El-Houda, Algeria.
Abdelrahman Khalfi, Criminal Procedures in Algerian and Comparative Legislation, 2nd edition, 2016, Belkess Publishing, Algeria.
Abdallah Ouhaibia, Explanation of the Algerian Code of Criminal Procedure, 2nd edition, Houma Publishing, Algeria, 2011.
Mohamed Abbas Mansour, Covert Operations in the Fight Against Drugs, Arab Center for Security Studies and Training Publishing, Riyadh, 1993.
Articles:
Chouiref Youssef, Infiltration as a Method of Investigation, Inquiry, and Evidence, Al-Mustaqbal Journal, Police School, Sidi Bel Abbes, 2007.
Fawzi Amara, Interception of Correspondence, Voice Recording, Image Capturing, and Infiltration as Judicial Investigation Procedures in Criminal Matters, Journal of Human Sciences, Mentouri University – Constantine, Issue 33, June 2011.
Laws:
Ordinance No. 66-155 on the Code of Criminal Procedure, amended and supplemented by Law No. 06-22 dated December 2006.
Law No. 15-19 dated 18 Rabi' al-Awwal 1437 AH corresponding to 30 December 2015, amending and supplementing Ordinance No. 66-156 dated 18 Safar 1386 AH corresponding to 8 June 1966 on the Algerian Penal Code.
Presentations / Conference Contributions:

Journal of Ecohumanism
2025
Volume: 4, No: 4, pp. 1586 – 1591
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i4.6892

Loujani Nour Eddine, Investigation and Inquiry Methods and Procedures, Study Day on the Relationship Between the Public Prosecutor and the Judicial Police, held on 12-12-2007, Algeria.