

The Newly Introduced Mechanisms for the Prevention and Combat of Human Trafficking crimes according to Law 23/04

Dr. Larguet Aziza ^{* 1}, Dr. Larguet Farida ²

¹ Faculty of Law and Political Science, University of Oum El Bouaghi (Algeria), aziza.metatla@yahoo.com

² Faculty of Law and Political Science, University of BATNA 1 (Algeria), larguetfarida593@gmail.com

Received: 29/12/2025

Accepted: 27/03/2026

Published: 22 /04/2026

Abstract:

The advancement of technology and the parallel evolution in the means and methods of committing crimes have prompted the Algerian legislator—through efforts to keep pace with these developments in order to prevent and combat crime in its various forms—to intervene on numerous occasions by amending existing legal provisions or introducing new legal texts that are suitable and capable of addressing crimes that pose a threat to society and individuals. Among the newly introduced texts is Law 23/04, which pertains to the prevention and combat of human trafficking, particularly in the investigation and inquiry phase, where the legislator granted certain powers and authorities to the judicial police despite the potential violations and infringements on rights and freedoms, due to the seriousness of this type of crime.

Keywords: Electronic Leakage; Digital Reporting; Crimes.

* Corresponding author

1. INTRODUCTION

The technological advancements in modern technology have had positive effects, transforming the world into a small village where information flows easily, securely, and abundantly, exchanged among individuals. However, on the other hand, this technology has also produced negative consequences, as it has become a tool exploited by criminals to execute their criminal schemes—particularly those that transcend national borders—such as the crime of human trafficking. This crime is considered a form of modern slavery and an affront to human dignity and humanity, to an extent that it goes beyond being a crime against the state to becoming a crime against society as a whole.

And this is what prompted the international community to seek the conclusion of several agreements to combat the crime of human trafficking, as is the case with the United Nations Convention against Transnational Organized Crime held in Palermo in 2000, along with its supplementary protocol specifically addressing the fight against human trafficking, especially of women and children. In line with these agreements, the Algerian legislator has played a positive role in combating this crime from a substantive legal standpoint through numerous amendments to legal texts aimed at eliminating the crime and punishing its perpetrators by enforcing harsher penalties.

To achieve the objective the state aspires to through these substantive provisions, there must also be procedures that are efficient and sufficient to identify and apprehend the perpetrators of such crimes. This is also the path taken by the Algerian legislator, who introduced procedural measures that respond to the technological advancements exploited by criminals to implement their criminal schemes. This was achieved through Law 23/04 on the prevention and combat of human trafficking, particularly in Chapter Five, which addresses procedural rules such as digital reporting, the preservation of traffic-related data, and electronic leakage, in addition to what is stipulated in the general rules.

According to the above, the central research question revolves around:

What are the newly introduced methods for the prevention and combat of human trafficking crimes, and what are the legal safeguards established for them?

To answer this question, it was necessary to combine both the descriptive and analytical approaches. The descriptive method was used when addressing doctrinal and legislative definitions, while the analytical method was applied to deconstruct legal texts and scholarly opinions.

The study was structured around a two-part framework:

- The first topic was dedicated to digital reporting and the preservation of traffic-related data, by defining each and clarifying the regulations governing them.

- The second topic focused on electronic leakage, identifying its meaning and the substantive and procedural safeguards that regulate it.

1. Digital Reporting and The Preservation of Traffic-Related Data:

The state's development and modernization of the justice sector by leveraging the advantages of technological advancements in modern technology has not been limited to judicial procedural aspects related to investigation, inquiry, and trial in criminal cases. It has also extended to include the process of reporting crimes through the establishment of the electronic prosecution platform "e-nyaba," which allows for the remote submission of complaints and petitions to the Public Prosecution.¹

Accordingly, to clarify the newly introduced procedures by the legislator, it is necessary to address digital reporting in the first subsection, due to its precedence in terms of procedural initiation. The second subsection will then be devoted to the preservation of traffic-related data.

1.1- Digital Reporting:

The Algerian legislator, under Article 34 of Law 23/04, emphasized the necessity of activating digital reporting as a means of preventing and combating human trafficking.² Accordingly, it is essential to address the concept of digital reporting first, followed by the legal safeguards established for it.

1.1.1- The Concept of Electronic Reporting:

Through Article 34 of Law 23/04, the Algerian legislator authorized the competent judicial police officer, for the purpose of combating human trafficking, to establish technical mechanisms for reporting any of the crimes specified in the aforementioned law via electronic networks. This must be accompanied by the immediate notification of the competent Public Prosecutor, who, according to the principle of discretionary authority, may either order the continuation of the investigation and inquiry into the reported crime or decide to halt it.

Accordingly, we will first present the definition of electronic reporting, followed by a discussion of its means.

A) Definition of Electronic Reporting:

The Algerian legislator did not define digital (or electronic) reporting nor explicitly designate it as a judicial procedure, despite referencing it in Article 9 of Law 15/03 on the modernization of justice.³ That article included the possibility of serving and transmitting documents, judicial writs, and records through modern technology—what came to be known as the electronic method—while respecting the conditions and procedures stipulated by that law. This, however, did not eliminate or replace the

1- Tarek Yahiaoui, Karima Khemghani, *The Newly Introduced Digital Safeguards in the Justice Modernization Law No. 15/03: Evidentiary Value for Establishing the Provisions of Electronic Notification as a Proposed Judicial Procedure*, Vol. 06, No. 02, *Journal of Legal and Economic Research*, 2023, pp. 414–431.

2- Law No. 23/04 of May 7, 2023, on the Prevention and Combat of Human Trafficking, Official Gazette No. 32, May 9, 2023.

3- Law No. 15/03 of February 1, 2015, on the Modernization of Justice, Official Gazette No. 06, February 10, 2015.

traditional methods established by the Code of Civil and Administrative Procedures and the Code of Criminal Procedure.

Additionally, Law 23/04 on the prevention and combat of human trafficking permits digital reporting in the case of crimes stipulated in the law, but it does not provide a definition for it. Therefore, one must refer to general legal principles and doctrinal definitions.

According to Article 406 of the Code of Civil and Administrative Procedures, official notification is defined as the process carried out by a judicial officer through a formal report, by visiting the residence of the person to be notified.¹ It applies to both judicial and non-judicial documents, including orders, rulings, and decisions issued by judicial authorities. This definition applies to traditional notification methods.

From a doctrinal perspective, electronic reporting is defined as:²

"Notifying the person concerned with judicial documents and the procedures taken against them through electronic means, in accordance with the principles established by applicable laws and regulations."

Thus, it becomes clear that electronic reporting does not differ from traditional notification in essence—only in the medium used to deliver the information. Hence, it is important to identify the authorized means of electronic notification.

B) Means of Electronic Reporting:

Upon reviewing Law 15/03 on the modernization of justice and Law 23/04 on the prevention and combat of human trafficking, it is evident that the legislator did not specify the electronic means that may be used for digital reporting. Therefore, it becomes necessary to refer to comparative legislation.

For instance, in the context of economic courts, the Jordanian and Egyptian legislators have recognized email and mobile phone as valid tools for electronic notification.³ These means can also be applied for reporting human trafficking crimes via the digital platform established by the judicial police officer, as stipulated by Article 34 mentioned above. This facilitates the reporting process and ensures the necessary protection for informants.

Other means may also be used, as long as they achieve the intended purpose—namely, informing the competent authorities of the occurrence of a crime covered under the law on the prevention and combat of human trafficking.

1.1.2- Justifications for Electronic Reporting and Its Safeguards:

The state's new orientation toward modernizing all sectors, including the justice sector, and utilizing technology in this context is driven by its many advantages in supporting investigation, detection of crimes, and expediting judicial decisions. However, this modernization may also infringe upon constitutionally guaranteed rights

1- Law No. 08/09 of February 25, 2008, including the Code of Civil and Administrative Procedure, as amended and supplemented, Official Gazette No. 21, April 23, 2008.

2- Tarek Yahiaoui and Karima Khemghani, op. cit., 421.

3- Nour Akef Al-Dabbas, "Provisions of Electronic Judicial Notification in the Jordanian Code of Civil Procedure," *Al-Balqa Journal for Research and Studies*, Al-Ahliyya Amman University 23, no. 2 (2020): 79.

and freedoms. Therefore, it is necessary to establish sufficient safeguards that protect these rights and freedoms, while also ensuring the procedural legitimacy of all actions aimed at uncovering the truth.

Accordingly, we will first outline the justifications for digital reporting, followed by the safeguards for electronic reporting.

A) Justifications for Digital Reporting:

The technological advancement in modern technology and the positive outcomes it has generated have necessitated its integration into various sectors, including the justice sector. Accordingly, it is essential to clarify the justifications and motives that led the legislator to adopt digital reporting, which can be summarized as follows:

a) Speed and Ease of Electronic Reporting:

Digital reporting is one of the tools that contribute to the prevention of human trafficking crimes and the identification of perpetrators. As previously mentioned, this type of crime inflicts harm on individuals and society by violating human dignity and humanity. Digital reporting helps by saving effort and time, and ensuring speed in execution—factors that encourage individuals to use it and not hesitate in reporting crimes, especially those related to human trafficking.

b) Effectiveness of Electronic Reporting in Exceptional Circumstances:

An individual may find themselves in exceptional circumstances that prevent them from reaching police stations to report human trafficking crimes. These circumstances may be due to health issues, natural disasters, or the victim's own situation, which may hinder them from carrying out traditional reporting procedures. In cases where the victim is under the control and surveillance of criminals, digital reporting allows them to inform the judicial police of the crime without needing to physically go to the authorities, due to their inability to do so.

Digital reporting also proves effective in unexpected exceptional circumstances that render existing methods unresponsive—such as during the COVID-19 pandemic and the implementation of quarantine measures. These conditions played a significant role in the increase of certain crimes, such as domestic violence, where victims were unable to move or report the crimes using traditional methods.

c) Transition from a Paper-Based System to an Electronic System:

One of the advantages of modern technology is the ability to store information and documents in an information system or in electronic formats, which differ from paper documents in terms of ease of retrieval within seconds. In contrast, paper documents are stored in archives and require considerable time to locate. Moreover, technology reduces the financial burden on the state treasury that would otherwise be spent on paper used for recording reports or procedures related to crimes—especially since the legislator explicitly requires documentation and written records during investigation and inquiry procedures so that the judge can exercise oversight and verify their legality. In addition, the lifespan of electronic documents is significantly longer than that of paper documents.

B) Safeguards for Digital Reporting:

By analyzing the provisions of Law 23/04 on the prevention and combat of human trafficking, it is clear that the Algerian legislator has established a set of safeguards to ensure the legality and integrity of digital reporting, as well as the protection and safety of the reporting individual. These include:¹

a) Notification of the Public Prosecutor:

Article 34 of Law 23/04 stipulates that the judicial police officer may implement digital reporting mechanisms provided that the Public Prosecutor is notified. The Public Prosecutor then has the authority either to stop or to authorize the continuation of the investigation and inquiry procedures. Accordingly, it is evident that the legislator allowed the competent judicial police officer to set up a mechanism based on modern technology through which individuals can report a crime of human trafficking. However, the officer is obligated to immediately inform the competent Public Prosecutor, who—according to the general rules—has the discretionary authority to initiate or halt public prosecution.

b) Confidentiality of Electronic Reporting:

Digital reporting preserves the confidentiality of electronic communications by limiting access to the reporting platform to the judicial police officer only. Furthermore, the legislator explicitly emphasized the need to maintain the anonymity of the informant, as stated in Article 29 of Law 23/04, which provides: "At all stages of evidence collection, investigation, or trial, measures must be taken to ensure the protection of victims, witnesses, and informants, including non-disclosure of their identity and maintaining the confidentiality of the public prosecution, without prejudice to the right of defense and the principle of adversarial proceedings, in accordance with the legally established provisions."

Likewise, Article 35 of the same law obliges the judicial police officer to maintain the confidentiality of the identity of victims, witnesses, and informants. From these two provisions, it is clear that the legislator stressed the importance of maintaining confidentiality in digital reporting in order to protect informants from potential harm or retaliation. However, as stated in Article 29, this protection is conditioned upon not infringing upon the right of defense or violating the principle of adversarial proceedings, since the priority remains the protection of the public interest, particularly in light of the recent surge in crimes that pose a real threat to all countries.

1.2- Preservation of Traffic-Related Data:

The United Nations General Assembly, through its Resolution No. 55/63 dated January 22, 2001, concerning the Combating of the Criminal Misuse of Information Technologies, stated in paragraph "(f)" of Article One the necessity of allowing the preservation of electronic data subject to criminal investigations, and of enabling

1- Mohamed Fawaz Abdel Fattah Hamed, Provisions of Electronic Judicial Notification (Master's thesis, Middle East University, Faculty of Law, Private Law, 2021), 12–13, available at: <https://shorturl.at/OhkTX> (accessed May 9, 2025).

investigative authorities to access such data upon urgent request. Therefore, states are required to incorporate this principle into their domestic legislation.¹

Before addressing the concept of this procedure, it is essential to clarify the meaning of service providers, as they are the holders of such data, as well as to outline the obligations and responsibilities imposed on them, as follows:

1.2.1- Definition of Service Providers:

Article 2, paragraph (d) of Law 09/04 defines service providers as: Any natural or legal person who provides internet services to users, or in other words, offers their services and ensures the ability to connect via an information system and/or a telecommunications network. This includes processing or storing digital data for the benefit of the mentioned communication service or its users.

There are individuals who contribute to the access, collection, transmission, and transfer of data across the internet. These individuals play the role of intermediaries, whether their work is limited to technical and functional aspects only or extends to what is known as a hosting provider (*Le fournisseur d'hébergement*).²

From a doctrinal perspective, a service provider is defined as: "A natural or legal person who acts in the course of their profession, aiming for profit and engaging in commercial activity professionally. The act of professionally engaging in commerce is what grants a person the status of a provider. Thus, the definition of a provider is tied to the nature of the activity they perform."³

Consequently, an email exchange, for example, necessarily passes through an electronic communications service provider, where it remains stored until it is received and accessed by the recipient. At this point, the service provider is faced with two options: either delete the message or store it.⁴

1.2.2- Obligations of Service Providers and Applicable Penalties:

Given the critical role service providers play in uncovering human trafficking crimes, the legislator has imposed several obligations upon them. In the event of non-compliance, specific criminal penalties have been prescribed. Accordingly, we will first address the obligations of service providers, followed by the penalties imposed for violations of these obligations.

A) Obligation of the Service Provider Regarding Data Retention Duration:

Like many other legal systems, the Algerian legislator addressed the procedure of data retention in Article 10 of Law No. 09/04⁵ on the specific rules for the prevention

1- United Nations General Assembly Resolution No. 55/63 of January 22, 2001, available at: http://www.un.org/arabic/documents/GARes/55/A_RES_55_063.pdf (accessed March 28, 2025).

2- Aed Raja Al-Khalaileh, *Electronic Tort Liability – Liability Arising from the Misuse of Computers and the Internet*, 1st ed. (Jordan: Dar Al Thaqa for Publishing and Distribution, 2009), p. 55.

3- Abdullah Dheeb Mahmoud, *Consumer Protection in Electronic Contracting – A Comparative Study*, 1st ed. (Jordan: Dar Al Thaqa for Publishing and Distribution, 2012), p. 44.

4- Rachida Bouker, *Crimes of Attacks on Automated Data Processing Systems in Algerian Comparative Legislation*, 1st ed. (Beirut: Halabi Legal Publications, 2012), p. 447.

5- Law No. 09/04 of August 5, 2009, on the Special Rules for the Prevention and Combat of Crimes Related to Information and Communication Technologies, Official Gazette No. 47, August 16, 2009.

and combat of crimes related to information and communication technologies, under the section titled "Obligations of Service Providers," which mandates that service providers, in accordance with Article 11 of the same law,¹ retain data and make it available to judicial investigation authorities and provide all necessary assistance to facilitate this process.

With regard to human trafficking crimes, the legislator stated in Article 31, paragraph 1 of Law 23/04 that the competent judicial authority, during the investigation of a human trafficking crime:

- May order service providers or any other person to deliver any relevant information or data stored using information and communication technologies, under penalty of sanctions stipulated in the applicable legislation.
- Also, Article 11 of the aforementioned law obliges service providers, under the penalty provided by law, to retain the mentioned data for one year starting from the date of registration.

Accordingly, it is clear that the Algerian legislator, in order to preserve the right to privacy, made the obligation of service providers to retain data a temporary procedure, requiring that after a specific period, the stored data must be removed and deleted. This period was set by the legislator at one year from the date of registration.

B) Applicable Penalties:

In addition to the obligations defined by the legislator under Law No. 09/04, there may be other obligations stipulated in the terms of reference (specifications document), as these service providers often interact with specific bodies that impose additional requirements. In the event of non-compliance, service providers may face measures such as license withdrawal or other administrative sanctions.

This is inferred from Article 11 of Law No. 09/04, which states that in addition to the administrative penalties that may be imposed for breaching the obligations set forth in Article 11, criminal liability may also apply to both natural and legal persons in cases where they hinder the proper conduct of judicial investigations.

The law sets the penalty for natural persons at imprisonment ranging from six (6) months to five (5) years, and a fine ranging from 50,000 DZD to 500,000 DZD. As for legal persons, the applicable penalties are those specified in Article 18 bis and subsequent articles of the Penal Code.

1.2.3- The Concept of Preserving Traffic-Related Data:

It is defined as: "An order issued by the competent authority to service providers to retain stored digital data in their possession or under their control, pending further legal procedures such as a search or an order to hand over digital data."²

1- Article 11 of Law No. 09/04 provides: "Taking into account the nature and type of services, service providers shall retain: A/ Data that allows the identification of service users. C/ Technical characteristics as well as the date, time, and duration of each communication. E/ Data that allows the identification of the recipient and the websites accessed."

2- Aïcha Kara Mostafa, *The Evidentiary Value of Electronic Evidence in the Field of Criminal Proof* (n.ed.) (Alexandria: Dar Al-Jami'a Al-Jadida, 2010), p. 159.

In Algerian law, traffic-related data is defined under paragraph "h" of Article 2 of Law No. 09/04 as: "All data related to communication conducted through an information system, generated by said system as part of a communication chain, which reveals the source of the communication, the destination, the route taken, the time, date, volume, and duration of the communication, and the type of service used."

It is noted that the legal definition includes terminology unfamiliar to criminal law, such as "source of the communication," which refers to, for example, a phone number or an Internet Protocol address (IP); "destination" refers to identifying the communication device through which the service provider is delivering its services; while "route taken" refers to the type of service and indicates the method used within the network, such as sending a file via email.¹

The Algerian legislator has identified several categories of traffic data that are subject to a unified legal system, meaning they fall within the scope of the retention obligation by service providers and are limited according to the provisions of Article 11 of Law No. 09/04.

In this context, it is important to point out the distinction between the terms "preservation of data" and "retention or archiving of data".

Although the two phrases have similar meanings in common language, they have different meanings in the language of information technology. The phrase "preservation of data" means keeping existing data in stored form and protecting it from anything that could lead to its damage or loss of status.

Whereas the phrase "retention of data" means keeping the data by its holder in relation to data that is in the process of being generated, and therefore the collection of data in the present and its storage or possession in an archive.

Accordingly, retention refers to archiving and storing data, while preservation of data refers to the activity that ensures the safety and confidentiality of the data.²

The measure of data preservation is considered in most countries a completely new legal procedure within domestic law. It is a new tool for investigating crimes, particularly those committed via the internet, due to the following reasons:³

A) Rapid alteration of computer data:

The ease of manipulation and alteration of information using modern technology may lead to the loss of elements that prove the crime, either due to negligence and inaccurate storage practices, or through the normal process of deleting information that is no longer needed. Therefore, the method that ensures the integrity of this data is the issuance of an order to preserve the data.

B) Identifying the perpetrator of human trafficking crimes:

1 Rachida Bouker, op. cit., p. 449.

2- Tarek Ibrahim El-Dessouki Atiya, Security Encyclopedia: Information Security – The Legal System for Informatics Protection (Alexandria: Dar Al-Jami'a Al-Jadida, 2015), p. 479.

3- Ibid., pp. 480–482.

Human trafficking crimes are often committed using technological means through the transmission of communications via an information system. These communications may contain viruses that damage information. Thus, verifying the identity of the source or destination of the communication allows and helps in identifying the perpetrator of the crime.

C) The role of communications in revealing the crime committed through them:

When communications contain illegal content or evidence of criminal acts, copies of these communications are preserved by service providers, such as email providers.

2. Electronic Infiltration:

Most national legislations have taken the path of establishing procedural methods aimed at detecting crimes even before they occur. One of these methods, which must keep pace with the technological developments in modern digital technology, is electronic infiltration. This method is intended to play an effective role in investigating and detecting human trafficking crimes, which is explicitly stipulated by the Algerian legislator in Article 32 of Law 23/04 on the prevention and combat of human trafficking.

Due to the seriousness of this measure and its impact on rights and freedoms, the Algerian legislator surrounded it with a set of substantive and procedural safeguards. Therefore, it is necessary to address its definition and legal basis, followed by the regulatory constraints that govern its implementation, as follows:

2.1- The Concept of Electronic Infiltration:

In order to combat certain crimes that pose a threat to the interests of individuals and society at large, the Algerian legislator has introduced special procedures—despite their gravity and the clear infringement on rights and freedoms. Among these procedures is infiltration, as provided by Law 25/¹14, which includes the Code of Criminal Procedure, particularly in Chapter Five, Articles 120 to 127. However, a question arises:

While infiltration can be imagined in other crimes through the physical penetration of lawfully authorized persons into criminal groups, how does electronic infiltration occur using digital means in human trafficking crimes?

Accordingly, we will first address the definition of electronic infiltration and then explain its legal basis. The regulatory constraints governing electronic infiltration will be discussed in the second part.

2.1.1- Definition of Electronic Infiltration and Its Legal Basis:

As previously stated, the seriousness of human trafficking crimes and their harmful effects on human dignity and humanity—especially with the misuse of modern technology by criminals to serve their criminal schemes—has made it necessary to introduce the procedure of electronic infiltration, in order to detect crimes either before

¹ - Law No. 25/14 of August 3, 2025, which includes the Code of Criminal Procedure, Official Gazette No. 54, August 13, 2025.

or after their occurrence. Accordingly, we will address first its definition, then its legal basis.

A) Definition of Electronic Infiltration:

Article 121 defines infiltration as: The act of misleading a criminal group by a judicial police officer or agent, under the responsibility of a judicial police officer who coordinates between the agent and the Public Prosecutor, by pretending to be an accomplice or participant with them, in order to monitor individuals suspected of committing acts classified as felonies or misdemeanors.

In order to convince criminal groups and be accepted among them, the law permits the judicial police officer or agent to use methods such as a false identity, and, when necessary, to commit the acts mentioned in Article 123, without incurring legal liability in general. However, under penalty of nullity, such acts cannot be considered incitement to commit human trafficking crimes.

Based on this, infiltration is an extremely sensitive technique for officers of the judicial police, requiring a high level of precision and competence.

Thus, infiltration is defined as: A special investigative technique that allows a judicial police officer or agent to penetrate a criminal group under the supervision of another officer responsible for coordinating the infiltration operation, with the aim of accompanying suspected individuals and uncovering their criminal activities by concealing their true identity and presenting themselves as a perpetrator or accomplice.¹

As for electronic infiltration, it is realized, according to this concept, when the competent judicial police officer penetrates the virtual world—through discussion forums, streaming rooms, and direct communication platforms—using aliases, fake profiles, and false identities in order to search for crimes and perpetrators, and to bring the offenders to justice.

B) The Legal Basis of Electronic Infiltration:

The Algerian legislator explicitly provided for the procedure of electronic infiltration as a tool for the prevention and combat of human trafficking crimes in Law 23/04 on the prevention and suppression of human trafficking, specifically in Article 32, which states: "In accordance with the provisions of the Code of Criminal Procedure, the Public Prosecutor or the Investigating Judge, after notifying the Public Prosecutor, may authorize under their supervision a judicial police officer to carry out electronic infiltration into one or more information systems or electronic communication networks, with the aim of monitoring persons suspected of committing any of the offenses set forth in this law, by pretending to be an accomplice or associate with them. Judicial police officers are strictly prohibited, under penalty of nullity of the procedures, from committing any act or behavior, in any form, that could incite suspects to commit a crime for the purpose of obtaining evidence against them."

1- Abdelrahman Khelfi, Lectures on Criminal Procedure Law (Ain M'lila: Dar Al-Houda, 2012), p. 74.

From the wording of the article, it is clear that the Algerian legislator sought to ensure the integrity, legality, and soundness of the procedures, in line with the fundamental principles governing criminal investigations, the uncovering of crimes, and attributing responsibility to the perpetrator. This is achieved by explicitly prohibiting judicial police officers, during electronic infiltration, from inciting suspects to commit crimes covered under Law 23/04 for the purpose of gathering evidence against them.

2.2- Regulations Governing the Procedure of Electronic Infiltration:

The Algerian legislator surrounded the infiltration process—including electronic infiltration, which may be necessitated by investigative or inquiry requirements in one of the crimes specifically enumerated—with a set of conditions that serve as safeguards, due to the seriousness of this procedure and its infringement upon individuals' privacy. These regulations may be formal safeguards or substantive safeguards.

2.2.1- Procedural Safeguards:

The Algerian legislator, in Article 32 of Law 23/04, referred to the procedure of electronic infiltration without specifying the procedural and formal safeguards for this measure. Therefore, it is necessary to revert to the general provisions set out in the Code of Criminal Procedure. Accordingly, Article 120 of the Code of Criminal Procedure includes a set of procedural conditions whose absence results in the nullity of the procedure and any consequences arising from it, in application of the principle of legality, as addressed in Article 124 of the same law. To clarify further, these conditions are as follows:

- The issuance of judicial authorization for the electronic infiltration operation by the Public Prosecutor or Investigating Judge, depending on the stage of the case file, in order to avoid infringement of rights and freedoms.
- The authorization must be in writing, in line with the procedural principle that for the infiltration process to be valid, the authorization must be written, in accordance with Article 124 of the Code of Criminal Procedure.
- The duration of the infiltration operation must be specified. The authorization must include the duration and time limit for carrying out this procedure. Article 124 of the Code of Criminal Procedure sets this period at four months, which may be renewed under the same formal and time conditions depending on the needs of the investigation or inquiry. The same article also gives the judge who authorized the infiltration the right to order its cessation even before the specified period ends.
- Qualification: Article 32 of Law 23/04 defines the qualification of the person conducting the electronic infiltration operation, limiting it to a judicial police officer under the supervision of the Public Prosecutor or Investigating Judge, depending on the stage of the investigation.

2.2.2- Substantive Safeguards:

In addition to the procedural safeguards required for the validity of the electronic infiltration operation, there are substantive safeguards and guarantees that can be

summarized in two main conditions, according to the provisions set by the Algerian legislator:

- Justification of the Authorization: Due to the seriousness of this measure, the authorization must be justified, whether issued by the Public Prosecutor or the Investigating Judge, since justification is the foundation of any judicial action. Accordingly, the authorization for infiltration must be based on an assessment of the elements obtained by the judicial police, and must clarify that the requirements of investigation and inquiry, as well as the nature of the crime, necessitate the use of this procedure, and that other legal methods are insufficient to uncover the truth. Moreover, the authority empowered by law to issue the authorization must justify the basis upon which the decision to resort to this measure was made.
- Specification of the Type of Crime: It must be a crime related to human trafficking.
- Effects of Infiltration: The acts committed by the infiltrator are considered justified acts, exempting them from legal liability.
- Confidentiality of the Electronic Infiltration: This is essential to protect the life and safety of the judicial police officers and agents who carried out the infiltration, as well as their families.

Conclusion:

The development of the tools used in committing crimes—and the need to detect them and identify the perpetrators—has prompted the Algerian legislator to introduce methods that align with the means employed, in order to keep pace with technological advancements and harness their benefits to achieve criminal justice and combat crime in all its forms, including human trafficking.

In line with this, the Algerian legislator introduced the procedures of digital reporting, preservation of traffic-related data, and electronic infiltration, and sought to regulate the legal framework for each procedure in terms of the circumstances under which it may be applied, how it is carried out, and the safeguards surrounding it to avoid violating one of the most fundamental constitutionally protected rights: the right to privacy.

From this study, the following findings and recommendations were reached:

Findings:

- The digital environment and its use by criminals to commit human trafficking crimes—and the presence of technical evidence within it—have made electronic infiltration one of the most appropriate and compatible procedures with this nature, to detect crimes and identify perpetrators, even before they occur.
- The legislator requires, for the execution of electronic infiltration, that the judicial police officer obtains prior written authorization from the Public Prosecutor or Investigating Judge, depending on the stage of the case, and that

the operation be conducted under their supervision, confirming the seriousness of the measure and the necessity of its application within the framework of procedural legality.

- The legislator introduced the procedure of digital reporting out of necessity, due to technological advancements and circumstances that the state may face, particularly in exceptional situations.
- The legislator surrounded the procedures of digital reporting and electronic infiltration with a set of safeguards to protect individuals' rights and freedoms, especially in their digital communications, and to prevent abuse and unlawful infringement.
- The Algerian legislator imposed an obligation on service providers to hand over any relevant information or data stored through information and communication technologies, under penalty of the sanctions prescribed by law.

Recommendations:

Based on these findings, the following recommendations are proposed:

- It is necessary to grant the status of judicial police officer to qualified professionals in the field of IT, such as service providers, due to their expertise and competence required for conducting electronic infiltration and digital reporting—but always under judicial oversight to protect individual rights and freedoms.
- The legislator must intervene to regulate electronic infiltration through specific provisions, as electronic infiltration possesses characteristics that differ from general infiltration.
- The legislator should revise certain legal provisions that contain vague and undefined terms that hinder effective judicial oversight, such as Article 65 bis 13.
- The duration authorized for conducting the procedure should not be fixed, but rather subject to the discretionary authority of the Public Prosecutor or Investigating Judge, depending on the circumstances.

Bibliography List

A- The Sources:

- United Nations General Assembly Resolution No. 55/63 of January 22, 2001, available at: http://www.un.org/arabic/documents/GARes/55/A_RES_55_063.pdf
- Law No. 08/09 of February 25, 2008, including the Code of Civil and Administrative Procedure, as amended and supplemented, *Official Gazette* No. 21, April 23; 2008.
- Law No. 09/04 of August 5, 2009, on the Special Rules for the Prevention and Combat of Crimes Related to Information and Communication Technologies, *Official Gazette* No. 47, August 16; 2009.
- Law No. 15/03 of February 1, 2015, on the Modernization of Justice, *Official Gazette* No. 06, February 10; 2015.

- Law No. 23/04 of May 7, 2023, on the Prevention and Combat of Human Trafficking, *Official Gazette* No. 32, May 9; 2023.
- Law No. 25/14 of August 3, 2025, which includes the Code of Criminal Procedure, *Official Gazette* No. 54, August 13, 2025.

B – the references:

B1- Books:

- Aed Raja Al-Khalaileh, *Electronic Tort Liability – Liability Arising from the Misuse of Computers and the Internet*, 1st ed., Jordan; 2009.
- Abdullah Dheeb Mahmoud, *Consumer Protection in Electronic Contracting – A Comparative Study*, 1st ed., Jordan; 2012.
- Rachida Bouker, *Crimes of Attacks on Automated Data Processing Systems in Algerian Comparative Legislation*, 1st ed., Beirut; 2012.
- Aïcha Kara Mostafa, *The Evidentiary Value of Electronic Evidence in the Field of Criminal Proof*, (n.ed.), Alexandria; 2010.
- Tarek Ibrahim El-Dessouki Atiya, *Security Encyclopedia: Information Security – The Legal System for Informatics Protection*, Alexandria; 2015.
- Abdelrahman Khelfi, *Lectures on Criminal Procedure Law*, Ain M'lila; 2012.

B2 – Theses:

- Mohamed Fawaz Abdel Fattah Hamed, *Provisions of Electronic Judicial Notification*, Master's thesis, Private Law, Middle East University, Faculty of Law; 2021.

B3 –Journal article:

- Mohamed Fawaz Abdel Fattah Hamed, *Provisions of Electronic Judicial Notification*, available at: <https://shorturl.at/OhkTX>
- Nour Akef Al-Dabbas, "Provisions of Electronic Judicial Notification in the Jordanian Code of Civil Procedure," *Al-Balqa Journal for Research and Studies*, Al-Ahliyya Amman University, Vol. 23, No. 2; 2020.
- Tarek Yahiaoui, Karima Khemghani, "The Newly Introduced Digital Safeguards in the Justice Modernization Law No. 15/03: Evidentiary Value for Establishing the Provisions of Electronic Notification as a Proposed Judicial Procedure," *Journal of Legal and Economic Research*, Vol. 06, No. 02; 2023.