

Criminal Protection of the Privacy and Confidentiality of Individuals' Private Conversations through Electronic Means

Amamra Mebarka

Email: amamra-mebarka@univ-eloued.dz

University of El-Oued

Received: 14/02/2026 Accepted: 25/04/2026 Published: 01/06/2026

Abstract

This study addresses the criminal protection afforded to the privacy and confidentiality of private conversations through electronic means under Algerian legislation, with the aim of determining the adequacy and effectiveness of the national legal framework in confronting emerging forms of digital eavesdropping and electronic interception that threaten privacy. To achieve this objective, the study adopts descriptive and analytical approaches by examining the legal concept of eavesdropping and identifying its types and digital characteristics, then analyzing the constituent elements of the offence under Article 303 bis of the Penal Code. Its material element is manifested in acts of interception, recording, or transmission using a device and without the consent of the persons concerned, while taking into account the exceptions and procedural safeguards established for judicial police officers under the Code of Criminal Procedure. Its mental element requires criminal intent in both of its components: knowledge and will.

The study concludes that Algerian legislation has established important legal frameworks to curb these offences; however, the covert and transnational nature of electronic eavesdropping requires continued updating of legislative provisions and the development of digital investigation mechanisms in order to keep pace with the rapid technological development in this field.

Keywords: electronic eavesdropping, privacy, Article 303 bis, Algerian Penal Code, material element, criminal intent.

Introduction

The tremendous technological development and the accelerating digital revolution in the modern era have brought about radical changes in the means of human communication and interaction. However, despite the ease that electronic means and modern networks have provided for exchanging information and conversations, they have simultaneously opened dangerous avenues for attacks on individual rights and freedoms, foremost among them the “right to privacy” and the “inviolability of private life.”

Private and confidential conversations of individuals constitute one of the most important manifestations of privacy, which international instruments and the Algerian Constitution have sought to guarantee and protect against any infringement. Nevertheless, technological development and the emergence of electronic interception and eavesdropping devices have made these conversations vulnerable to intrusion, recording, and interception without the knowledge or consent of their owners, thereby posing a direct threat to the psychological and social security of individuals.

This evolving situation has nevertheless confronted criminal policy with major challenges, prompting the Algerian legislator to intervene to address these emerging forms of crime through the general provisions of the Penal Code, as well as the specific provisions relating to the prevention and combating of offences connected with information and communication technologies, with the aim of providing criminal protection that criminalizes and restrains every conduct intended to intercept, record, or disclose private conversations.

From this standpoint, the central problem of this study is defined by the question of the extent to which the Algerian legislator has succeeded in providing effective criminal protection to safeguard the privacy and confidentiality of individuals' private conversations in the face of the emerging risks and violations resulting from the use of electronic means. This central question gives rise to a number of subsidiary questions concerning the nature of eavesdropping in the digital environment and its principal forms and characteristics that distinguish it from traditional forms of infringement, as well as the legal elements constituting the offence of electronic eavesdropping under Algerian legislation, in addition to the nature of the criminal sanctions prescribed to confront this conduct and their adequacy in achieving the required deterrent effect.

For a precise examination of this problem and to answer its questions, we adopted the descriptive and analytical approaches to the relevant legal provisions in Algerian legislation, with reference to doctrinal opinions. Our study is organized into three integrated sections: the first addresses the concept of eavesdropping; the second examines the elements of the offence of electronic eavesdropping under Algerian law; and the third concludes the study by addressing the penalty prescribed for this offence.

Section One: The Concept of Eavesdropping

The criminal study of any prohibited conduct requires determining its conceptual nature and examining its legal dimensions, since defining the scope of the criminal protection afforded to the privacy of private conversations remains dependent on the precise identification of the terms and meanings defining the forms of infringement. There is no doubt that the act of "eavesdropping" is no longer confined to its simple traditional forms; rather, it has evolved alongside technological developments and modern electronic media, making it a means of violating privacy and threatening the confidentiality that individuals seek to preserve.

In order to provide a comprehensive understanding of the legal and doctrinal features of this conduct, the conceptual treatment of this section is based on tracing the semantic development of eavesdropping, beginning with defining its boundaries by distinguishing between its linguistic, terminological, and legal meanings, followed by identifying the various patterns and forms through which this infringement is committed, whether in its traditional or digital form, and ultimately clarifying the distinctive characteristics of this phenomenon in the digital environment that give it a particular criminal character requiring a specific legislative response.

First: Definition of Eavesdropping

There are several conceptual approaches to determining the intended meaning of eavesdropping, given the different linguistic, terminological, and legal perspectives from which this conduct has been examined.

1. Linguistic Definition: The Arabic term for “eavesdropping” is derived linguistically from the triliteral verb “nasata” or “ansata.” In Arabic, “ansata lahu” or “ansata ilayhi” means to listen to him attentively and silently; “al-nasat” means silence for the purpose of listening.¹

It is worth noting that there is a linguistic distinction between “hearing” and “eavesdropping.” Hearing occurs as an automatic physiological process when sound waves reach the ear without requiring voluntary effort,² whereas eavesdropping requires intent and deliberately directing the sense of hearing toward sound sources in order to comprehend them. In criminal usage, the concept of eavesdropping generally carries the meaning of secrecy and secretly listening without the knowledge of the speaker.³

2. Terminological Definition: In general terminology, eavesdropping means directly or indirectly listening, secretly and unlawfully, to the conversations or communications of others without their knowledge or consent.⁴

In the digital and technological environment, the terminological concept of eavesdropping has expanded to mean the physical or technical interception of means of transmitting audio data and information through electronic networks and systems, with the aim of accessing the content of private and confidential conversations and communications.⁵

3. Legal and Doctrinal Definition (in Algerian and Comparative Legislation):

- In criminal legal doctrine: Electronic eavesdropping is defined as an intentional criminal conduct in which the perpetrator uses modern technical means or devices to intercept, capture, record, or transmit private or confidential conversations and calls made by individuals in private places or through communication networks, without legal or judicial authorization and without the consent of the parties to the conversation.⁶
- Under Algerian legislation: The Algerian legislator has not provided an abstract and direct definition of eavesdropping as an independent element. Instead, it has criminalized the material acts and conduct constituting it. The legal concept of eavesdropping is reflected in Article 303 bis of the Algerian Penal Code, which criminalizes the act of capturing, recording, or transmitting private or confidential conversations or calls without the permission or consent of their owner,⁷ as well as in Law No. 09-04 (concerning the specific rules on the prevention of offences related to information and communication technologies and their suppression), which regulates the mechanisms and procedures of “electronic interception,” the capture of data, and the interception of communications transmitted through electronic networks under judicial supervision, in protection of rights and freedoms.⁸

Second: Types of Eavesdropping

As a crime affecting the privacy of private conversations, eavesdropping takes multiple forms that vary according to the means used and the environment in which it is committed. Academically and legally, eavesdropping may be divided into several principal types:

1. Eavesdropping according to the means and instrument used: It is divided into:

A. Traditional eavesdropping (direct and personal): This is the primitive form of eavesdropping, carried out by secretly listening through direct personal effort without the use of complex technologies, such as when the

perpetrator hides near the place where the conversation is taking place, spies from behind doors and walls, or uses simple sound-amplification tools for direct interception.⁹

B. Electronic eavesdropping (technical and digital): This is the more recent and dangerous form, carried out through the use of advanced technological means and devices, such as planting miniature microphones, using wireless spying devices, or employing cyber programs and intrusions (such as spyware and eavesdropping software targeting smartphones and applications).¹⁰

2. Eavesdropping according to the environment and type of communication: It is divided into:

A. Eavesdropping on direct oral conversations: This means capturing or recording conversations taking place face-to-face between individuals in private places (such as homes and closed offices) without their consent.¹¹

B. Eavesdropping on wired and wireless communications and conversations: This is carried out by intercepting telephone calls over fixed lines, or capturing the signals and wireless frequencies of mobile phones and communication through radio networks.¹²

C. Eavesdropping on electronic conversations and data (via the Internet): This consists of intercepting data packets exchanged over the Internet or through instant communication applications and voice messages, using packet-sniffing programs or direct intrusion into servers and systems.¹³

3. Eavesdropping according to legality and legal authorization: It is divided into:

A. Unlawful (criminal) eavesdropping: This is any act of intercepting, recording, or capturing private conversations undertaken for espionage, curiosity, or extortion without the knowledge of the parties and without authorization from the competent judicial authority. It is the act prohibited and criminalized under Article 303 bis of the Algerian Penal Code.¹⁴

B. Lawful (procedural/judicial) eavesdropping: This is the lawful interception of correspondence and communications carried out by investigative and judicial police authorities on the basis of a reasoned judicial authorization and under strict statutory safeguards, where absolutely necessary for investigating serious crimes or offences of terrorism and corruption, in accordance with Law No. 09-04 concerning the prevention and suppression of offences related to information and communication technologies.¹⁵

Third: Characteristics of Electronic Eavesdropping

In the digital age, eavesdropping is characterized by a set of inherent and distinctive features that distinguish it from traditional forms of infringement of the privacy of private life. These characteristics are highly significant in view of the practical and procedural difficulties they impose on investigative authorities and the criminal justice system:

1. Covert and invisible nature (physical absence of the perpetrator): The offence of electronic eavesdropping is characterized by being committed without the perpetrator having to be physically present at or near the crime scene or the victim. Interception and capture can be performed remotely through smart software and sophisticated devices, leaving the victim completely unaware that the infringement is occurring at the time.¹⁶

2. Transnational nature: Digital eavesdropping operations transcend the geographical and political borders of states. A perpetrator located in one country may eavesdrop on private conversations taking place between individuals in another country through the global Internet and encrypted applications, thereby raising

complex legal issues concerning the “territorial application of criminal law” and conflicts of judicial jurisdiction.¹⁷

3. Ease of committing the offence and difficulty of detecting it and preserving its evidence: Modern technologies make it possible to conduct eavesdropping operations and record conversations with a few simple keystrokes without leaving tangible physical traces of the kind left by traditional crimes. Electronic evidence resulting from such acts is also fragile and can easily be erased, altered, or encrypted, making the detection of the crime and its proof by conclusive evidence procedurally difficult.¹⁸

4. Seriousness and broad impact (expansion of the scope of harm): Unlike traditional eavesdropping, whose harmful effects are limited to a small number of individuals within a defined geographical setting, electronic eavesdropping has an enormous capacity to record, retain, and disclose vast quantities of confidential conversations and information and disseminate them through social media within seconds, thereby multiplying the psychological and social harm suffered by victims.¹⁹

5. Technical nature and continuous development (flexibility and complexity): This crime is closely linked to the development of technology, encryption methods, artificial intelligence, and protection and confidentiality mechanisms. Whenever more sophisticated security software and vulnerabilities are developed, more complex software and security weaknesses are created in parallel for infiltrating and eavesdropping on conversations, which requires continuous updating of legislative provisions and procedural skills to keep pace with this development.²⁰

Section Two: Elements of the Offence of Electronic Eavesdropping under Algerian Law

Affording criminal protection to the privacy and confidentiality of private conversations requires a precise criminalizing formulation that defines the legal elements and conditions upon which the criminal structure of the offence is based. The Algerian legislator has followed this approach in Article 303 bis of the Penal Code, protecting the individual’s right to preserve the confidentiality of communications and private information against any unlawful technical infringement.

The general principles of criminal law and doctrine provide that there can be no crime or punishment unless the constituent structure of the offence is established in both its material and mental aspects. Therefore, for the offence of electronic eavesdropping to exist and for the criminal liability of its perpetrator to arise, there must be material conduct involving the capture, recording, or transmission of conversations by means of a technical device and without the consent of the right-holder or authorization under the law, provided that the conduct is not covered by the exceptions and procedural safeguards prescribed for judicial police authorities. This is accompanied by a mental element in the form of criminal intent, consisting of knowledge and will, excluding cases of unintentional fault or accidental interception.

First: The Material Element of the Offence of Electronic Eavesdropping

The material element is purely physical conduct directed against the privacy of private life. The material element of this offence consists of three elements: capturing, recording, or transmitting the conversation; the requirement that these acts be carried out through a device; and the requirement that they be performed without the victim’s consent or without authorization under the law.

1. Capturing, recording, or transmitting private calls or conversations: The legislator identifies the criminal activity as capturing, recording, or transmitting private calls or conversations. This means secretly listening—that is, eavesdropping on or listening to a conversation covertly—which may be done using the

ear alone without any instrument, or by using a specialized device. Recording a conversation means preserving it on media designated for that purpose so that it can be replayed later. Transmitting a conversation means secretly listening through a device in order to send it from the place where it is spoken to another place through listening devices or transmitting microphones.²¹

2. The foregoing acts must be performed through a device: This means that the offence is committed only if the perpetrator uses a device in committing it. It is sufficient that the device be used merely for eavesdropping even if no recording takes place. It is also sufficient that the device be used to transmit conversations from one place to another; the type of device is immaterial.

3. The act must be performed without the victim's consent and without authorization under the law: For the offences stipulated in Article 303 bis of the Penal Code to arise, the legislator requires that they be committed against the victim's will or without authorization under the law.

The consent of the right-holder means the individual declaration of will by which a person legally capable of giving consent waives an interest protected by law and over which the law grants that person the right of disposition.²²

The general rule in criminal matters is that a crime constitutes an infringement of a right protected by law. This right may belong exclusively to society or may belong to an individual member of society. Nevertheless, when a crime infringes an individual's right, it necessarily also affects society's interest in that right. Accordingly, the characterization of an act as a punishable crime does not depend on the will of the victim. However, the legislator has, in some circumstances, attached criminal legal effects to the will of the holder of the right and the interest infringed, making that will a ground for permitting the infringement. The general rule is therefore that the victim's consent is not a ground of justification; if it has such an effect with respect to certain offences, this is only by way of exception. The rationale is that crimes infringe rights of social importance, and without such importance there would be no need to protect them through criminal sanctions.²³

Consent must be given by the right-holder, that is, by the person who owns the right. Since a right is an interest recognized and protected by law, an infringement of it constitutes an offence requiring deterrence. Accordingly, consent must emanate from the right-holder who has full authority to dispose of it. Where there are multiple right-holders, consent must be given by all of them.

It should be noted that personal conversations ordinarily take place between two persons, at a minimum, each being a speaker and listener to the other. The privacy of such conversations belongs to all parties without exception because it forms part of all their private lives. Therefore, the consent of one party to record the conversation that he or she conducts with another does not concern only that party's private life; it also affects the private life of the other party, over which the first party has no authority. If a person wishes to remove a conversation with another from the sphere of his or her protected private life and permit its recording, this may not be done without the consent of the other parties to the conversation, who participate in it within the sphere of their protected private lives. Likewise, none of the parties to a personal conversation may record it without the consent of the remaining parties.

Consent is presumed to arise from a sound will; that is, it must be expressed by a will free from defects, unaffected by coercion, fraud, mistake, or deception. All such circumstances negate consent and deprive it of its legal value.

Consent also presupposes that the will is legally valid, which is the case only when discernment, awareness, and freedom of choice are present. Consent must also precede or be contemporaneous with the conduct, because subsequent consent does not erase the crime and has no legal value in the formation of the offence.²⁴

As for cases authorized by law, these are cases in which the act derives its lawful character directly from the law, since the law itself has granted and authorized it. In such cases, all conditions required by law for carrying out the act must be satisfied. The legal basis creating the authority must exist, and the authorization or license must comply with the formal and substantive requirements prescribed by law. These are cases in which the law permits secretly listening to or recording conversations in order to uncover a crime or avert an imminent danger threatening state security or for military intelligence purposes. This constitutes an exception to the general rule, because an absolute prohibition of such acts could hinder authorities in their search for truth and consequently prevent them from uncovering crimes and apprehending their perpetrators, especially when offenders use modern technical devices enabling them to commit their crimes without easy detection unless the authorities are permitted to carry out such an infringement against a person who permits himself or herself to violate the rights of others.²⁵

Accordingly, a person's right to the privacy of private conversations is not absolute. Monitoring, accessing, or seizing the content of such conversations may be authorized in circumstances permitted by law. The Algerian legislator provided in Article 65 bis 05 of the Code of Criminal Procedure: "Where the necessities of the investigation in a flagrante delicto or the preliminary investigation into offences of narcotics, transnational organized crime, offences affecting automated data-processing systems, money laundering, terrorism, offences relating to the legislation on foreign exchange, as well as corruption offences so require, the competent Public Prosecutor may authorize the following:

- Interception of correspondence transmitted by wired and wireless means of communication.
- The establishment of technical arrangements, without the consent of the persons concerned, for capturing, fixing, broadcasting, and recording words spoken privately or confidentially by one or more persons in private or public places, or for capturing images of one or more persons present in a private place.
- ... In the event that a judicial investigation is opened, the aforementioned operations shall be carried out on the basis of authorization from the investigating judge and under his direct supervision."²⁶

Under the new Code of Criminal Procedure, Article 114 provides as follows: "Where the necessities of the investigation in a flagrante delicto or the preliminary investigation into offences of intentional homicide, narcotics and psychotropic substances, transnational organized crime, offences connected with information and communication technologies, money laundering and terrorism, offences relating to legislation on foreign exchange and the movement of capital to and from abroad, corruption offences, smuggling offences, human trafficking offences, organ trafficking offences, migrant smuggling offences, and kidnapping offences so require, the competent Public Prosecutor may authorize the following:

- Interception of correspondence transmitted by wired and wireless means of communication;
- Establishment of technical arrangements, without the consent of the persons concerned, for capturing, fixing, broadcasting, and recording words spoken privately or confidentially by one or more persons in private or public places, or for capturing images of one or more persons present in a private place;
- ... In the event that a judicial investigation is opened, the aforementioned operations shall be carried out on the basis of authorization from the investigating judge and under his direct supervision."²⁷

Since covert monitoring of telephone calls constitutes an exception, it is subject to restrictions and safeguards. Among the safeguards established by the Algerian legislator for the legality of monitoring telephone conversations is the competent authority responsible for issuing the monitoring order as a primary guarantee. The power to authorize the monitoring of telephone conversations through interception of correspondence conducted by wired and wireless means of communication belongs to the investigating judge when a judicial investigation has been opened and under his direct supervision.

The Public Prosecutor may also issue authorization to monitor conversations in *flagrante delicto* cases or during the preliminary investigation of offences involving narcotics, transnational organized crime, offences affecting automated data-processing systems, money laundering, terrorism, offences relating to foreign-exchange legislation, and corruption.

Accordingly, a judicial police officer may not monitor telephone conversations unless the officer has been directly delegated to carry out this procedure by the investigating judge or the Public Prosecutor, as applicable. On this basis, if judicial police officers initiate the interception or recording of conversations before obtaining prior authorization from the Public Prosecutor or investigating judge, the procedure is unlawful and illegal, and the report prepared by the judicial police officers on the basis of this unlawful monitoring must be declared null and void.²⁸

The second safeguard is that the authorization to monitor conversations must be in writing and adequately reasoned. The requirement that judicial authorization for monitoring be reasoned is justified by the fact that monitoring conversations is a serious procedure that affects individual freedom and violates their natural right to confidentiality. It is an exceptional procedure that constitutes an exception to the general rule established by the Algerian Constitution, namely the inviolability of citizens' private lives and their right to the confidentiality of communications; this exception is justified by the public interest.

It should be noted that Article 65 bis 07 specified the conditions of the authorization referred to in Article 65 bis 05, providing that the authorization must contain all elements permitting identification of the communications to be intercepted, the places concerned, whether residential or otherwise, the offence justifying recourse to these measures, and their duration. The authorization must be in writing for a maximum period of four months, renewable according to the requirements of the investigation. In addition, application of the general rules requires that the authorization contain its date of issue, the name and capacity of the person who issued it, his or her seal and signature, and that it expressly indicate an operation involving the capture, recording, or transmission of private or confidential calls or conversations.

Second: The Mental Element of the Offence of Electronic Eavesdropping

The mental element of this offence takes the form of criminal intent, as demonstrated by Article 303 bis of the Penal Code: "... every person who intentionally infringes the privacy of persons ...". There is therefore no punishment for a person who secretly listens to, records, or transmits a conversation through negligence, lack of foresight, or carelessness, however serious, such as a person who inadvertently leaves a recording device switched on, resulting unintentionally in the recording of a conversation. Likewise, the offence does not arise when a person accidentally intercepts telephone conversations as a result of crossed lines caused by a defect in the telephone network, because the element of criminal intent is absent in such a case.

Criminal intent is intention with regard to the conduct and awareness with regard to the circumstances of the conduct necessary for it to constitute a crime. It is clear that while intention belongs to the sphere of will in the mind, awareness belongs to the sphere of cognition.²⁹

The perpetrator's knowledge means perceiving matters correctly and in accordance with reality. The perpetrator must therefore know that the elements of the act exist. It is a psychological state in the perpetrator's mind whose essence is awareness of the reality of the elements and facts constituting the criminal conduct. That is, the perpetrator must know the subject of the right protected by criminal law and the person against whom the infringement is directed. In the subject matter of our study, this is the right to privacy; therefore, the perpetrator must know the private nature of the conversation at the time of capturing, recording, or transmitting private or confidential calls or conversations.

Will is a positive psychological state directed toward achieving a particular purpose through a particular means. It is a fundamental condition for criminal responsibility in general, and criminal intent exists only when the will is directed toward undertaking the criminal conduct.³⁰

Section Three: The Penalty Prescribed for the Offence of Electronic Eavesdropping

With the aim of protecting the privacy of telephone calls and individuals' private conversations, the legislator has imposed a penalty for violating their confidentiality, as provided in the first paragraph of Article 303 bis. The legislator has also criminalized attempt to commit this offence under the third paragraph of Article 303 bis. Since the right to privacy is a personal right, the legislator has provided that criminal proceedings may terminate when the victim pardons the perpetrator. All these points are addressed below:

The penalty prescribed for the offence of violating private or confidential calls or conversations differs depending on whether the perpetrator is a natural person or a legal person.

First: Penalty Prescribed for a Natural Person in the Offence of Electronic Eavesdropping

The legislator has prescribed for a natural person who commits the offence of violating the privacy of telephone calls and private or confidential conversations both principal and supplementary penalties.

1. Principal penalties prescribed for a natural person: Article 303 bis provides: "Any person who intentionally infringes the privacy of persons by any technique whatsoever shall be punished by imprisonment for six (6) months to three (3) years and a fine of DZD 50,000 to DZD 300,000, by: capturing, recording, or transmitting private or confidential calls or conversations without the permission or consent of their owner..."

Under this provision, the penalty prescribed for the offence consists of deprivation of liberty in the form of imprisonment for 6 months to 3 years, in addition to a fine ranging from DZD 50,000 to DZD 300,000.

It is noteworthy that the legislator did not provide aggravated circumstances for this offence. It would have been appropriate to impose a more severe punishment, for example, on persons with a certain level of education that enables them to use modern technologies to violate the privacy of private or confidential calls or conversations.

2. Supplementary penalties prescribed for a natural person: Article 303 bis 1 provides that the court may prohibit a person convicted of the offences stipulated in Articles 303 bis and 303 bis 1 from exercising one or more of the rights provided for in Article 9 bis 1 for a period not exceeding five (5) years. It may also order publication of the conviction in accordance with the procedures set out in Article 18 of this Code.

The confiscation of the things used in committing the offence must always be ordered.

With reference to Article 9 bis 1, this penalty consists of deprivation of the exercise of national, civil, and family rights, as follows:

- Dismissal or exclusion from all public functions and positions connected with the offence;
- Deprivation of the right to vote or stand for election and of the right to wear any decoration;
- Ineligibility to serve as a sworn assistant, expert, or witness to any contract, or as a witness before the courts except for purposes of corroboration;
- Deprivation of the right to possess weapons, to teach, to manage a school, or to serve in an educational institution as a professor, teacher, or supervisor;
- Ineligibility to act as a guardian or custodian;
- Loss of all or part of parental authority.

The supplementary penalty for this offence is discretionary and subject to the judicial authority of the trial judge. The judge may order the convicted person to be deprived of one or more rights, or may decide not to impose such deprivation.

Second: Penalty Prescribed for a Legal Person in the Offence of Electronic Eavesdropping

The modern trend in penal legislation establishes the liability of legal persons for offences committed by their representatives and for their benefit. With regard to the offence of violating private or confidential calls or conversations, the legislator has likewise prescribed principal and supplementary penalties for the legal person.

1. Principal penalties prescribed for a legal person: Article 303 bis 1 provides that a legal person is criminally liable for the offences specified in Sections 3, 4, and 5 of this Chapter, in accordance with the conditions stipulated in Article 51 bis.

The legal person is subject to a fine in accordance with the procedures provided for in Article 18 bis and, where applicable, Article 18 bis 2.

Thus, a legal person bears criminal liability for offences committed on its behalf by its organs or legal representatives. The principal penalty applicable in this case is a fine equal to one to five times the maximum fine prescribed for a natural person under the law punishing the offence, pursuant to Article 18 bis.

Given that the offence under study is a misdemeanor, and since the maximum fine prescribed for a natural person is DZD 300,000, the penalty applicable to the legal person consists of a fine ranging from DZD 300,000 as a minimum to DZD 1,500,000 as a maximum.

2. Supplementary penalties prescribed for a legal person: In addition to the foregoing penalty prescribed for the legal person, the final paragraph of Article 303 bis 3 provides that the legal person shall be subject to one or more of the supplementary penalties stipulated in Article 18 bis.

With reference to this provision, these penalties are as follows:

“Dissolution of the legal person;

Closure of the establishment or one of its branches for a period not exceeding five (5) years;

Exclusion from public contracts for a period not exceeding five (5) years;

Prohibition from directly or indirectly engaging in one or more professional or social activities, permanently or for a period not exceeding five (5) years;

Confiscation of the thing used in committing the offence or resulting from it;

Publication and posting of the conviction;

Placement under judicial supervision for a period not exceeding five (5) years, with the supervision applying to the activity that led to the offence or in connection with which the offence was committed.”

Conclusion

On the basis of the foregoing analytical study of the criminal protection afforded to the privacy and confidentiality of private conversations through electronic means under Algerian legislation, it is clear that technological development, while contributing to the facilitation of human communication, has simultaneously imposed unprecedented legal and security challenges in limiting emerging violations resulting from eavesdropping and digital interception.

The conceptual, procedural, and structural examination of electronic eavesdropping offences has shown that the Algerian legislator has not remained passive, but has sought to establish a preventive criminalization and penal system by combining the provisions of the Penal Code (particularly Article 303 bis and subsequent provisions), special legislation on the prevention and suppression of offences related to information and communication technologies, and the amendments introduced into the Code of Criminal Procedure.

The study reached a number of findings, which are presented together with certain proposals as follows:

First: Findings

1. Development of the concept and means: Eavesdropping is no longer limited to secretly listening through direct traditional means. Its scope has expanded to become cyber conduct based on complex technologies and transnational digital interception, making it a covert danger affecting the psychological and social security of individuals.

2. The requirement of a device as an essential condition: For the offence of electronic eavesdropping to be established under Article 303 bis, the perpetrator must use a device or technical tool to capture, record, or transmit a private conversation without the authorization or consent of its parties.

3. Balancing privacy protection with the requirements of investigation: Algerian legislation balances the criminalization of eavesdropping as the general rule with its exceptional permissibility under the heading of “electronic interception of correspondence and procedural eavesdropping,” provided that it is subject to written and reasoned judicial authorization issued by the Public Prosecutor or investigating judge and is limited to specifically defined offences, thereby safeguarding procedural legality.

4. Intentional nature of the offence: The offence is based on criminal intent in its two components (knowledge and will), and punishment is excluded in cases of unintentional fault or accidental interception resulting from network vulnerabilities or interference.

Second: Proposals

1. Amendment and updating of legislative wording: It is recommended that Article 303 bis of the Penal Code be redrafted to expressly incorporate modern concepts and forms of infringement (such as artificial intelligence, encrypted instant communication applications, and advanced spyware), in order to ensure that perpetrators do not escape liability on the grounds of “insufficiency of the legal text.”
2. Strengthening international coordination and cooperation: Given the transnational nature of the offence of electronic eavesdropping, it is advisable to activate extradition agreements and mutual legal assistance in the cyber domain in order to enable the prosecution of perpetrators located outside the national territory.
3. Developing judicial police capabilities: Judicial police bodies and officers specializing in cybercrime should be supported with advanced technical mechanisms and high-level training that enable them to detect and analyze digital evidence without departing from the requirements of legal safeguards.
4. Increasing financial and supplementary penalties: Consideration should be given to increasing the value of financial fines and supplementary penalties (such as the final confiscation of digital means and deprivation of the right to use communication networks), particularly when the offence is committed for purposes of extortion or within organized gangs.

Footnotes

1. Ibn Manzur, *Lisan al-Arab*, Vol. 5, Dar Sader, Beirut, 1990, entry (Nasata), p. 242.
2. Ibn Manzur, same source, p. 242.
3. Abd al-Fattah Murad, *Criminal Investigation and the Search for Evidence in Cybercrimes*, Mansha’at al-Ma’arif, Alexandria, 2004, p. 85.
4. Farid al-Zughbi, *Penal Encyclopedia: Crimes of Infringement of Privacy and the Sanctity of Private Life*, Vol. 3, Dar Sader, Beirut, 2001, p. 203.
5. Mansour Rahmani, *Cybercrimes in Algerian Legislation*, Dar al-Ulum for Publishing and Distribution, Annaba, 2010, p. 46.
6. Omar Khouri, *Crimes Resulting from the Use of Computers in Algerian Legislation*, Parliamentary Thought Journal, No. 04, Algeria, 2004, p. 64.
7. Ordinance No. 66-156 dated 8 June 1966, containing the Algerian Penal Code, as amended and supplemented.
8. Law No. 09-04 dated 5 August 2009, containing the specific rules on the prevention and suppression of offences related to information and communication technologies, Official Gazette of the People’s Democratic Republic of Algeria, No. 47.
9. Farid al-Zughbi, *op. cit.*, p. 210.
10. Mansour Rahmani, *op. cit.*, p. 52.
11. Ahsan Bousqi’a, *The Concise Guide to Special Criminal Law: Crimes against Persons and Crimes against Property*, 15th ed., Dar Houma, Algeria, 2018, p. 115.

12. Abd al-Fattah Murad, *op. cit.*, p. 92.
13. Omar Khouri, *op. cit.*, p. 68.
14. Article 303 bis of Ordinance No. 66-156 containing the Algerian Penal Code, as amended and supplemented.
15. Articles 3, 4, and 6 of Law No. 09-04 dated 5 August 2009, containing the specific rules on the prevention and suppression of offences related to information and communication technologies.
16. Farid al-Zughbi, *op. cit.*, p. 218.
17. Mansour Rahmani, *op. cit.*, p. 60.
18. Abd al-Fattah Murad, *op. cit.*, p. 105.
19. Ahsan Bousqi'a, *op. cit.*, p. 118.
20. Omar Khouri, *op. cit.*, p. 73.
21. Zaki Abu Amir, *Criminal Protection of Personal Liberty*, Mansha'at al-Ma'arif, Alexandria, 1979, p. 9.
22. Youssr Anwar Ali, *Commentary on the Penal Code, Principles of the General Theory, Part One*, Dar al-Nahda al-Arabiyya, Cairo, 1985, p. 139.
23. Ali Ahmed Saleh, *The Crime of Infringing the Sanctity of Personal Conversations*, Algerian Journal of Legal, Economic and Political Sciences, Faculty of Law and Political Science, University of Algiers 1, Vol. 54, No. 2, Algeria, 2017, p. 377.
24. Mamdouh Khalil Bahr, *Protection of Private Life in Criminal Law (A Comparative Study)*, without edition, Dar al-Nahda al-Arabiyya, Cairo, 2010, p. 35.
25. Ali Ahmed Saleh, *op. cit.*, p. 379.
26. Article 65 of Ordinance No. 66-155, Code of Criminal Procedure, old law.
27. Law No. 25-14, new Code of Criminal Procedure.
28. Ali Ahmed Saleh, *op. cit.*, p. 381.
29. Abd al-Rahman Jamal al-Din Hamza, *Privacy and Freedom of Information*, Egyptian General Book Organization, Egypt, 2000, p. 199.
30. Raouf Obaid, *Principles of the General Part of Penal Legislation*, 3rd ed., Dar al-Fikr al-Arabi, Egypt, 1966, p. 221.