ISSN : 2350-0743

www.ijramr.com

International Journal of Recent Advances in Multidisciplinary Research
Vol. 08, Issue 03, pp. 6673-6677, March, 2021

RESEARCH ARTICLE

THE CRIME OF UNLAWFULLY INTERCEPTING DATA AND INFORMATION

***[1]Souraya Bourbaba, [2]Lakhdar Maachou and [3]Abd Elkafi Meriam**

[1]Lecturer in Taheri Mohamed University - Bechar – Algeria, Director of the Laboratory of Legal Studies and Responsibility of Professionals
[2]Lecturer in Taheri Mohamed University - Bechar – Algeria, the head of the legal studies and liability team in the medical field Studies Laboratory-
[3]PhD Researcher, specializing in Business Criminal Law/ Taheri Mohamed University - Bechar – Algeria, Member of the Laboratory of Legal Studies and Responsibility of Professionals

ARTICLE INFO

Article History:
Received 10th December, 2020
Received in revised form
26th January, 2021
Accepted 15th February, 2021
Published online 30th March, 2021

Keywords:

Crime, Unlawfully intercepting, Information, Data.

ABSTRACT

The unlawful objection to the data is considered a serious attack on the freedom of communication and on personal freedoms and their sanctity, freedoms guaranteed by international and national legislation, but the interception of communications on the other hand secures to the judicial and security authorities and is a very important means in the investigation work, and in controlling evidence Or the preparatory work that precedes the criminal act, and to ward off the danger of conspiracies that are prepared against the state and the security of societies, and one of the most important means that helps to uncover crimes and arrest their perpetrators and those involved in them, which requires reconciliation between two conflicting interests, namely: the interest of the individual, his rights and private freedoms, and the interest of State, society and national security.

INTRODUCTION

The exchange of information and data electronically through computers and networks, and various means of communication has become common due to the vast majority of countries linking to the Internet and its increasing dependence on information and communication systems steadily increasing, so that these systems have become an essential and necessary factor in managing all the various sectors Such as the commercial, banking, security, and other fields. The legislation of countries was not limited to criminalizing the penetration of information systems or staying in them, but that protection extended to include information and data circulated or sent through those means, and whether it comes to intercepting this information and impeding its flow and spying ([1]) on it or by pirating and seizing it And exploiting it for specific purposes. The various recent legislations have responded to such acts and criminalized them by expressly stipulating them according to special texts ([2]), or by extrapolating general texts as a crime related to the right to privacy and respect for the confidentiality of communications and correspondence, And because of the confidentiality and privacy of correspondence or the importance attached to it, the information and data sent or circulated through various means of communication may be characterized by the European Convention Budapest for Information Crime through its third article, as stated in its explanatory note regarding this crime that the right to respect The correspondence is guaranteed by Article 8 ([3]) of the European Convention on Human Rights. In addition, the right to respect correspondence is constitutionally guaranteed in the various constitutions of the countries of the world ([4]). We also find the Arab Convention to Combat Information Technology Crimes signed in Cairo in 2010 has stipulated the crime of legal objection through its seventh article to be adopted by Arab

[1]- Information or electronic espionage is limited to eavesdropping on a specific type of information related to national security and foreign policy of other countries, and it is defined as the use of modern information technology methods to enter illegally and illegally into electronic information systems of countries and governments and eavesdrop on them, with the intention of obtaining For its important information related to its system and its secrets, it includes all kinds of military, security, political, economic, scientific and social information.

[2]- Among the recent Arab legislations that stipulated the crime of illegal objection, we find the Jordanian temporary law related to information technology, Article 05 of which is previously mentioned, as well as Royal Decree No. 12 of 2011 related to information technology crimes for the Sultanate of Oman.

[3] - Whereas, Article 8 of the European Convention on Human Rights of 1950 states: "1 - Every human being has the right to respect the inviolability of his private life, the inviolability of his home and his correspondence. The national security of a democratic society, or to protect the safety of people, or for the economic interest, or to prevent situations of chaos or crimes, or to preserve public health and morals, or to protect and care for the rights and freedoms of others.

[4] -Article 39 of the Algerian Constitution of 1996 amended and complemented states that "the sanctity of the citizen's private life and the sanctity of his honor may not be violated, and the law protects them."The secrecy of private correspondence and communication in all its forms is guaranteed. "

countries in their penal laws or laws to combat information technology crimes ([5]), which called on Arab countries to cooperate in This field and combating this type of crime. The crime of unlawful interception is a crime that affects information circulated through information systems and is criminalized legally, and therefore is it permissible legally to intercept data, as we wonder about the nature of this crime and how it happened and what is its consequence, and is the text of the Algerian legislator against it compared with other legislation? We respond to the above and clarify it by following a comparative analytical and methodological methodology according to the following elements and axes:

The first requirement: What is illegal objection

The meaning of the objection was mentioned in the framework of Article Three of the Budapest Convention as eavesdropping or data transfer that takes place inside the computer or that is done via two remote devices via various information networks, or by translating the electromagnetic emissions from the computer carrying this data or that are done via wireless devices And by any of the non-public technical means. The explanatory note to this agreement indicated that the aim of this article is to protect the right to respect data transmission, and that this crime represents a violation of the right to respect communications such as eavesdropping and the traditional recording of telephone conversations between people. As for the Arab Convention against Information Technology Crimes, it was defined in Article Seven as: "deliberate and unjustly objecting to the data flow line by any of the technical means and cutting the transmission and reception of information technology data." Also, the crime stipulated applies this principle to all forms of electronic transmission of data, whether this transmission was by phone, fax, email or file transfer ([6]).

Therefore, an unlawful interception constitutes a crime of interception through the information system or the data sent through the information systems for the purpose of eavesdropping, recording, or obstructing its flow, and that this crime constitutes an aspect of the attack on the right to privacy, which is prejudice to the freedom of communication and correspondence, this right that It is stipulated in the constitution and assaulting it constitutes a crime punishable by a penalty ([7]). And if it is decided in accordance with the general rules that the law decides to protect correspondence and telephone intelligence, as it guarantees its confidentiality, it is not permissible to monitor it or access it except in exceptional cases which are set forth in the law and that also applies to electronic communication messages, including messages circulated via e-mail ([8]) And Skype calls or other communication applications. protection is clear in the Algerian legislation through the general provisions of the legislator mentioned in Articles 303 bis and what follows from the Penal Code and Article 137 of the same law, where he indicated through his amendment for the year 2006 of crimes that violate the sanctity of private life and any The technique was the following:

- ✓ Capture, record, or transmit private or confidential conversations or conversations without the permission of its owner or his consent.
- ✓ To take, record or transfer a picture of a person in a private place without the permission or consent of its owner.

objection is in its content is to capture, eavesdropping, recording or controlling communications or correspondence that are carried out by technical or electronic means ([9]), and therefore any objection to any data that was sent or circulated electronically and without right is a crime that deserves to be punished. In addition to this, we find the Law of Post and Telecommunication No. 2000-03 has stipulated this form of abuse through Article 127, and this will be clarified in the following elements.

The second requirement: the elements of the crime of illegal objection

The crime of unlawful interception arises with every act that impedes the flow of information, its capture or registration, eavesdropping on communications or what is transmitted over the network or any means of transmission or correspondence, and this crime like every crime has its elements that we explain in the following:

The first branch: the physical pillar of the crime of unlawful interception

The physical element of the crime of unlawfully intercepting data is the act of interception, which includes acts of eavesdropping or capture ([10]), monitoring of communications, obstructing the flow of data or electronic information sent over the information network, or through the means of information technology, or cutting its transmission or reception ([11]). these actions, according to what was stated in the Budapest Agreement and the aforementioned legislation, are carried out by the perpetrator without the right and using non-public technical means, so for this pillar to exist, certain conditions must be met according to Article III of the Budapest Agreement and Article Seven of the Arab Agreement with The possibility of adding other conditions in the internal laws of countries that operate these agreements, and according to what it considers appropriate for their internal entity:

The first item: the use of non-public technical means to make the objection

[5] A group of Arab countries ratified this agreement, among them Jordan on January 08, 2013, and recently Iraq on September 3, 2013, and Algeria on September 8, 2014, according to Presidential Decree No. 14-252, which includes ratifying the Arab Convention to Combat Information Technology Crimes Edited in Cairo. 2010, JR No. 57 issued on September 28, 2014, p. 04 -

[6] Dr. Hilali Abd Allah Ahmed, The substantive and procedural aspects of information crime, in light of the Budapest Agreement signed on November 23, 2001, first edition, the Arab Renaissance House, Cairo - Egypt, 2003, pp. 78.79.

[7] See Articles 303 bis and later of the Algerian Penal Code, amended, supplemented, and added according to Law 06_23 of December 20, 2006, J.R. No. 84, p. 23.

[8] Dr. Zia Ali Ahmad Noman, information fraud, phenomenon and applications, a series of legal studies in the field of information, first edition, the national paper, Marrakech - Morocco - 2011, p. 123.

[9] -The Algerian legislator defined electronic communications in Law No. 09-04 containing the special rules for preventing and combating crimes with information and communication technologies in Article 02, paragraph and as "any correspondence, transmission or reception of signs, signs, writings, pictures, sounds or various information." By any electronic means.

[10] -The Arab Convention against Information Technology Crime defines the act of capture through Article 2/8 as "viewing or obtaining data or information"

[11] -Article 7 of the Arab Convention to Combat Information Technology Crime, as well as Article Eight of the Royal Decree of 2011 of the Sultanate of Oman, previously referred to.

In order for this crime to take place, data and information must be intercepted using certain non-public technical means related to eavesdropping, controlling or monitoring the content of communications, and obtaining the latter may be done directly through accessing and using the information system, or indirectly through the use of Eavesdropping devices, and interceptions to record data may also include any of the tapes or magnetic supports intended for recording ([12]).

That the scope of technical means can extend to even technical devices related to transmission or communication lines, such as devices for collecting and recording wireless communications, and may also include logical entities, passwords and codes ([13]). the crime of unlawful interception in accordance with the aforementioned text of the agreement requires that the data or information in question of the crime be transmitted by means of non-public means of communication, that is, non-public, so that it is noted that the term non-publicity is a trait that follows the means of transportation or communication of devices and equipment, and Methods intended for transfer, registration, eavesdropping, or to capture data and information ([14]), and not the nature of the data and information sent per se, this may be available to all people, but the owners of the conversation or messaging want to contact or send it in a confidential manner, for certain considerations that may be Personal, economic or commercial Or political ...

However, the term non-publicity does not exclude communications per se that are available to any person wishing to use these methods for these purposes. What is also noticed on the text of Article Three of the Budapest Agreement and Article Seven of the Arab Convention in criminalizing this behavior is not required for a certain type of data or information, as these may be related to the security of the state or political or military information spied on it, or economic, or private information By a natural or legal person or otherwise, and by this national legislators may define certain conditions related to the nature of the information or data subject to espionage or its dependence on a certain body. from it the text can be general to include all types of information and data, whether they are affiliated with a governmental or private entity. This is what is also noted on some modern Arab legislation ([15]) that criminalized this behavior in legislation related to combating information technology crimes, which did not set conditions related to the nature of data and information subject to espionage and whether it was financial, personal or other.

The second clause: That the objection is unlawful

It is also required in this behavior that it be unlawful or unlawfully, this crime may occur from any person, whatever his characteristic, whether he works in the field of information systems ([16]) or has nothing to do with it, but the perpetrator must not be from those authorized By obtaining that information. If the person accused of eavesdropping on conversations or capturing the data or information sent or recording it is from those who have the right or have been previously authorized to do so from the parties to the conversation or contact, or based on what he has derived from a certain authority that has the right to monitor communications, or based on a permit Among the parties involved in the testing of communication devices, personal computers and information systems of an institution or company, through which he was able to listen to the conversations or view the data and record it for purposes related to the experiment and test the devices and equipment to develop the best security means to protect this data and information [17]It resulted from acts of abuse. Also, an act of unlawful objection is not considered if it is based on a permit from competent authorities for considerations related to the national security of the state or for the purposes of investigations and judicial investigations in order to seize evidence and criminal facts or preparations that precede the criminal act, and to ward off a special danger of conspiracies that are being tried against the state And its apparatus, and the fight against terrorism and other attacks that threaten the security of society, and this is what we will explain when talking about the procedural side of these crimes.

In all of these cases, the data or information is intercepted by a legitimate way, either on the basis of a prior agreement or according to the cases excluded by law due to the existence of some necessity.

The second branch: The moral pillar of the crime of unlawful objection

The crime of unlawful objection is based on what is stated in the previous texts. The general criminal intent is provided by its elements of knowledge and will. As for the special intention, it was not extracted from those texts, as stated in Article Three of the Budapest Convention that "the objection is intentionally and without right ...", as well as the agreement The Arab Anti-IT Crime stipulated: “Deliberate objection without right ...” ([18]) Accordingly, the perpetrator must be informed that his obtaining that information or data and that eavesdropping on conversations or recording or capturing information data was done illegally and against the will of the contact person or against the desire of the owner of the control; But if this knowledge is not available, such as someone who believes that the parties to the communication have authorized him to do so, or from his authority to monitor communications ([19]) in a manner that has an error in the interpretation of the limits of his authority and competence, or that he entered the scope of communication by chance, then in this case the element of knowledge has Exiled, and accordingly, the moral element of

[12]Bilal Amin Zain Al-Din, Crimes of Automatic Data Processing Systems in Comparative Legislation and Islamic Sharia, University House of Thought, Alexandria, 2008, p. 307.

[13]Dr. Hilali Abd-Allah Ahmed, previous reference, p. 80.

[14]Bilal Amin Zainuddin, previous reference, p. 307.

[15]Article 05 of the Jordanian Provisional Law No. 30 of 2010 stipulates that “Anyone who clears without lawfully captures, intercepts, or eavesdrops on what is sent through the information network or any information system, is punishable by imprisonment for a period of no less than a month and not exceeding a year Or by a fine of no less than (200) two hundred dinars and not more than (1,000) thousand dinars, or with both of these penalties ". Article 08 of the Royal Decree No. 12/2011 previously mentioned also states that "A penalty of imprisonment for a period of no less than a month and no more than a year and a fine of no less than five hundred Rial Omani and not more than two thousand Rial Omani or one of these two penalties, shall be imposed on him. Anyone who intentionally and unlawfully interferes with the use of information technology means the itinerary of data and electronic information sent through the information network or information technology means, or cut off its broadcast or reception, by telephone.

[16]The penalty will be more severe if the objection is from the telecommunications and telecommunications staff, according to Article 127 of the Law of Post and Transport No. 2000_03 which is canceled according to the law issued in 2018.

[17] Bilal Amin Zainuddin, previous reference, p. 309

[18]Article 07 of the Arab Convention to Combat Information Technology Crimes mentioned earlier, and the same is in relation to Article 05 of the Jordanian Temporary Law No. 30 of 2010, and Article 08 of Royal Decree No. 12/2011 referred to earlier.

[19] Bilal Amin Zainuddin, previous reference, p. 310.

this crime is negated. This is on the one hand, and on the other hand, the will of the perpetrator must be directed to take this act in violation of the law and the will of the author of communication or communication, if he is forced to do so by others because of his experience or skill in using eavesdropping and recording devices, for example, it is not Done intentionally Criminal also, and therefore no crime ([20]).

The third requirement: illegal objection in the Algerian legislation

Eavesdropping on communications or on what is sent through the information network or any information system or any technology is a serious attack on the sanctity and sanctity of private life, specifically freedom of communication and correspondence, these freedoms guaranteed by the Universal Declaration of Human Rights ([21]) (1948) and text I have to protect it European Convention on Human Rights ([22]) (1950). Also, these rights are guaranteed by the constitutions of states, including the Algerian constitution, as it says "the confidentiality of correspondence and communications in all their forms is guaranteed" ([23]). a new article in the Penal Code amended by Law 06_23 includes an attack on the inviolability of private life stating that: "Whoever deliberately infringes on the inviolability of the private life of persons with any technology whatsoever shall be punished:

- ✓ To pick up, record, or transfer private or confidential calls without the owner's permission or consent
- ✓ by taking, recording or transmitting a picture of a person in a private place, without the permission or consent of its owner ... "([24])

Accordingly, he did not refer to the frankness of the Algerian legislator, just as the French legislator added when adding a section on crimes of automated data-processing systems to a provision or text specific to the crime of information interception, but he added that the matter protected the attack on communications and correspondence with any technology whatsoever and expanded the field of communications protection And correspondence through Article 303 bis added to the Penal Code 2006 and included within the protection of private life. Also, the legislation that explicitly provided for the crime of unlawful objection in special punitive texts ([25]) was aimed at encouraging the use and spread of information systems and information networks by protecting its users who are keen to ensure confidentiality, privacy and protection of their financial, personal and other information. we find that the legislator has also criminalized this act through special legislation, such as what we find in the Post and Telecommunication Law No. 2000_03, as amended and supplemented, as stated in Article 127 that: "The penalties stipulated in Article 137 of the Penal Code apply to Every person authorized to provide the international express mail service or any aid he works for and who, in the exercise of his duties, opens, converts, sabotages the mail, violates the confidentiality of correspondence, or assists in committing these acts, The same penalties apply to every person who is authorized to provide a wired and wireless transportation service and every worker with public telecommunications network operators who, in the exercise of his duties and in addition to legally established cases, violates and in any way the confidentiality of correspondence sent, sent or received by The way of wired and wireless transportation, or who ordered or helped to commit these acts. Punished either by jail from two months to year or by a financial penalty from 50.000Da or 1.000.000 DA or by both of them . Any person other than the persons mentioned in the previous two paragraphs, who commits one of the acts punishable under these two paragraphs .... "([26]) Accordingly, the Algerian legislator has tried to surround all the data to protect the data and information processed automatically or sent through the information network or the means of information and communication technology, or to interrupt it and intercept it, whether in the penal law or special laws such as the telecommunications law.

He also identified cases of unlawful surveillance and cases in which electronic electronic surveillance was permitted for the purposes of investigation and investigation or for the prevention of notices that might affect the security of the state and its institutions through what was stated in Law No. 09_04 containing special rules for the prevention of crimes related to information and communication technologies and Combating it, as a dangerous measure and a violation of people's freedoms in exchange for preserving state security and protecting society. As for the French legislator, Law No. 91-646 was issued on July 10, 1991 regulating the monitoring of talks, as amended by Law No. 669/2004, where the first article of it stipulated "the confidentiality of correspondence that is transmitted by phone or other means of electronic communication, the law guarantees protection." ". An exception provided for in the second paragraph of the first article responds to this rule by saying: "This secret may only be assaulted by public authorities, in cases of necessity justified by the public interest stipulated in the law and within the limits set forth therein" ([27]).

Conclusion

The goal of legislation that penalizes the crime of intercepting information or data is to encourage the use and spread of information systems and information networks by protecting its users who are keen to ensure the confidentiality, privacy and protection of their financial and personal information. However, the legislator, in criminalizing this act, may find himself before two or two duties protecting the rights and freedoms of people in protecting their information and correspondence that takes place through information systems,

[20] -Bilal Amin Zainuddin, previous reference, p. 310.

[21] -Article 12 of the Universal Declaration of Human Rights, adopted and published by UN General Assembly Resolution 217 of December 10, 1948, states: "No one shall be subjected to arbitrary interference with his private life, family, home, correspondence, or campaigns in his honor and reputation, and everyone has the right to Protect the law from such interference or campaigns..

[22] --Article 08 Convention for the Protection of Human Rights within the scope of the Council of Europe (Rome, November 4, 1950).

[23] - Article 39/2 of the Algerian Constitution of 1996, as amended and supplemented**.**

[24] -Article 303 bis of the amended and complemented Penal Code.

[25] -From these legislations, we find Jordanian and Omani law.

[26] -The Jordanian legislator also criminalized the act of objection in the Provisional Law No. 30 of 2010 amending 2015 and 2019 and before him in the Telecommunications Law No. 13 of 1995 amending and supplementing until 2011, as stated in Article 76 thereof as follows: Striking out the contents of a message through the telecommunications network or encouraging others to do this work is punishable by imprisonment for a period of no less than a month and not exceeding six months or by a fine not exceeding (200) dinars or by both penalties

[27] -Moussa Attou, protecting the right to privacy in Algerian law in light of the scientific and technological development - a comparative study - a thesis for a doctorate in science with a specialization in legal science, a branch of commercial law, Jalali Liyabis University, Faculty of Law and Political Science, Sidi Bel Abbas, 2014 P. 299.

and between intercepting that information in a case that posed a threat to the security of the state and society, which made him decide on electronic judicial control As a new measure through the amended and complemented Algerian Code of Criminal Procedure.

Recommendations:

- ✓ It is better for this crime to be explicitly stated in the crimes against the automated data-processing systems in the Algerian Penal Code, as long as the Algerian legislator has ratified the Arab Convention against Information Technology Crime
- ✓ Unifying information crimes in the Algerian legislation and comparative legislation, especially those that ratified the Arab agreement.
- ✓ The unification of crimes necessitates the unification of procedures to follow up on this type of crime, which may be in cases of espionage and interception of state institutions 'information as a cross-border crime.
- ✓ The necessity of establishing international bilateral or collective agreements to facilitate procedures for following up on crime and criminals wherever they are, so that they do not escape impunity.

REFERENCES

Algerian Penal Code, amended, supplemented, and added according to Law 06_23 of December 20, 2006, J.R. No. 84.

Arab Convention to Combat Information Technology Crime Convention for the Protection of Human Rights within the scope of the Council of Europe (Rome, November 4, 1950).

Dr. Hilali Abd Allah Ahmed, The substantive and procedural aspects of information crime, in light of the Budapest Agreement signed on November 23, 2001, first edition, the Arab Renaissance House, Cairo - Egypt, 2003.

Dr. Zia Ali Ahmad Noman, information fraud, phenomenon and applications, a series of legal studies in the field of information, first edition, the national paper, Marrakech - Morocco - 2011.

Jordanian temporary law related to information technology.

Law No. 09-04 containing the special rules for preventing and combating crimes with information and communication technologies.

The European Convention on Human Rights of 1950 the Jordanian Provisional Law through the information network or any information system.

Bilal Amin Zain Al-Din, Crimes of Automatic Data Processing Systems in Comparative Legislation and Islamic Sharia, University House of Thought, Alexandria, 2008.

Decree No. 14-252, which includes ratifying the Arab Convention to Combat Information Technology Crimes Edited in Cairo. 2010, JR No. 57 issued on September 28, 2014.

Moussa Attou, protecting the right to privacy in Algerian law in light of the scientific and technological development - a comparative study - a thesis for a doctorate in science with a specialization in legal science, a branch of commercial law, Jalali Liyabis University, Faculty of Law and Political Science, Sidi Bel Abbas, 2014.

Royal Decree No. 12 of 2011 related to information technology crimes for the Sultanate of Oman.

The Algerian Constitution of 1996 amended and complemented

The Universal Declaration of Human Rights, adopted and published by UN General Assembly Resolution 217 of December 10, 1948.

****