

Crimes of the Unlawful Use of Processed Personal Data under Law No. 18-07 on the Protection of Natural Persons in the Processing of Personal Data

Abbes Rima

PhD in: Law

University of Colonel Akli Mohand Oulhadj, Bouira

r.abbes@univ-bouira.dz

Nadia Zougaghe

Business Criminal Law

University of Colonel Akli Mohand Oulhadj, Bouira

n.zougaghe@univ-bouira.dz

Abstract

The Algerian legislator has kept pace with modern technological developments by enacting and amending numerous legal provisions in the field of information technology. The latest of these is Law No. 18-07 on the Protection of Natural Persons in the Processing of Personal Data. Although this law was adopted relatively late compared with international and Arab legislation, it criminalizes numerous acts that constitute violations of the sanctity of private life, including those involving personal data subject to automated processing. Such violations may occur during the collection of personal data, throughout the processing operation itself, or after the completion of such processing. The latter category represents one of the most serious offences against personal data. Therefore, this research paper seeks to examine the legal framework governing crimes involving the unlawful exploitation of automatically processed personal data.

Keywords: Personal Data, Automated Processing, Law No. 18-07, National Authority, Authorization, Declaration, Crimes of Unlawful Exploitation.

Introduction

In light of the information revolution that characterizes our present era, and given the widespread use of modern information and communication technologies, despite the essential role they play in our daily lives and their having become a defining feature of the digital age, they nevertheless raise numerous concerns regarding the security and privacy of personal data (or personal information) processed and used by natural persons.

Personal data are no longer limited, in light of the developments witnessed by the Internet, to traditional information such as name, surname, and postal address. Rather, they have come to encompass a much broader range of data, including photographs, telephone numbers, voice recordings, financial capacity, email addresses, behaviors and preferences, biometric data, and other information capable of identifying the natural person to whom such data relate.

The European Union initially defined personal data under European Directive 95/46/EC, in Article ² 2, as follows: “any information relating to an identified or identifiable natural person, directly or

Received: 20/04/2026; Accepted: 02/09/2026; Published: 08/10/2026¹

© 2026 The Author. Published by AVADA-CROMA. This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, adaptation, and reproduction in any medium, provided that the original author and source are properly credited.

<https://creativecommons.org/licenses/by/4.0/>

² The European Union was among the earliest entities to take an interest in the criminal protection of personal data. This is evidenced by Recommendation No. 20/85 issued by the Council of Europe concerning the protection of personal data used for direct marketing purposes; European Directive 95/46/EC of 24 October 1995 concerning the protection of individuals with regard to the processing

indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.”³

As for the General Data Protection Regulation (GDPR),⁴ it defines personal data as: “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier (IP address or email address), or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”⁵

The French legislature likewise defined personal data under Law No. 801 of 2004 on the protection of personal data. Article 2 provides that personal data means: “any information relating to an identified or identifiable natural person, directly or indirectly, in particular by reference to an identification number or to one or more elements specific to his or her physical, physiological, genetic, psychological, economic, cultural or social identity.”⁶

The Algerian legislature, for its part, defined personal data in Article 3(1) of Law No. 18-07 relating to the protection of personal data,⁷ as follows: “any information, regardless of its medium, relating to an identified or identifiable natural person, hereinafter referred to as the ‘data subject’, directly or indirectly, in particular by reference to an identification number or to one or more elements specific to his or her physical, physiological, genetic, biometric, psychological, economic, cultural or social identity.” It should be noted that this definition is essentially identical to that contained in the aforementioned European directives, as well as to the definition provided under French law. Consequently, most legal systems worldwide, including Arab legislation, have converged around a common understanding of the concept of personal data.

As for “processing,” Article 3(3) of the aforementioned Law No. 18-07 defines it as: “any operation or set of operations performed, whether by automated means or not, on personal data, such as collection, recording, organization, storage, adaptation, alteration, extraction, consultation, use, disclosure by transmission, dissemination or any other form of making available, alignment or interconnection, as well as closure, encryption, erasure or destruction.”

Accordingly, the law enacted by the Algerian legislature constitutes an effective embodiment of the principle of personal data protection enshrined in the 2016 Constitutional Amendment, through the final paragraph of Article 46, which stipulates: “The protection of natural persons in the field of processing personal data is a fundamental right guaranteed by law, and any violation thereof shall be punishable by law.”

Indeed, Law No. 18-07 introduced numerous acts that constitute violations of the confidentiality and integrity of personal data and that may be committed by persons, whether natural or legal. Such violations may occur during the collection of personal data, during their processing, or during their use.

of personal data; European Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector; European Directive 2002/58/EC concerning the processing of personal data in the context of electronic communications; and Directive 2012/28/EU, among others, culminating in the adoption of Regulation (EU) 2016/679, the General Data Protection Regulation, concerning the protection of natural persons with regard to the processing of personal data and the free movement of such data.

³ European Directive 95/46/EC, available at EUR-Lex, accessed on 08/02/2020 at 21:09.

⁴ The General Data Protection Regulation (GDPR) is an instrument of European Union law concerning data protection and privacy. It was adopted on 14 April 2016, thereby repealing European Directive 95/46/EC, and entered into force on 25 May 2018.

⁵ This is provided for in Article 4 of the General Data Protection Regulation (GDPR), available at GDPR Info, accessed on 08/02/2020 at 19:02.

⁶ This is the same definition contained in the aforementioned European directives. French Law No. 2004-801 of 6 August 2004 concerning the protection of natural persons with regard to the processing of personal data amended Law No. 78-17 of 6 January 1978 relating to information technology, files and freedoms. See: Mohamed Ahmed Al-Maadawi, Protection of Information Privacy of Users Through Social Networking Sites: A Comparative Study, an article published in a journal whose name was not specified, No. 33, Part Four, pp. 1926–2057.

⁷ Law No. 18-07 of 10 June 2018 concerning the protection of natural persons with regard to the processing of personal data, Official Gazette of the People's Democratic Republic of Algeria, No. 34, issued on 10 June 2018.

Accordingly, the following question arises: What is the scope of the criminal protection afforded to personal data against offences involving their unlawful exploitation under Law No. 18-07?

In order to address this issue, we propose the following points:

Part One: Offences Involving Violations of the Terms of the Declaration or Authorization

Section One: The Offence of Changing the Purposes of Processing

(Article 58 of Law No. 18-07)

Section Two: The Offence of Retaining Personal Data Beyond the Prescribed Period

(Article 65(2) of Law No. 18-07)

Part Two: Offences Involving the Disclosure of Personal Data to Unauthorized Persons

Section One: The Offence of Allowing Unauthorized Persons to Access Personal Data

(Article 60 of Law No. 18-07)

Section Two: The Offence of Transmitting Processed or Received Data to Unauthorized Persons

(Article 69 of Law No. 18-07)

Section One

Offences Involving Violations of the Terms of the Declaration or Authorization

This type of offence—as previously indicated—is committed at a later stage of the processing of personal data, namely, the stage of exploiting personal data processed by automated means. Once all the legally prescribed conditions for automated processing have been fulfilled, particularly those stipulated in Article 12 of Law No. 18-07⁸ and once the declaration submitted for the purpose of carrying out the processing has been accepted and authorization has been granted by the National Authority for the Protection of Personal Data the processed data become eligible for exploitation⁹ and use for the specific purposes indicated in the declaration. However, any violation of the conditions and terms set out in such declaration constitutes an offence punishable by law. Among the most important conditions governing the exploitation of such processing is the requirement that it be carried out in accordance with the purposes declared and authorized. Accordingly, any violation thereof constitutes an offence under Law No. 18-07 (First Subsection). Likewise, the processing may only be exploited during the period specified and authorized in the declaration. If the data are retained after the expiry of the prescribed period, this also constitutes an offence under Law No. 18-07 (Second Subsection).

First Subsection

The Offence of Using Processing for Purposes Other Than Those Declared or Authorized

The Algerian legislator provided for this offence in Article 58 of Law No. 18-07, which stipulates:

“Any person who carries out or uses data processing for purposes other than those declared or authorized shall be punished by imprisonment for a period of six (06) months to one (01) year and a fine ranging from DZD 60,000 to DZD 100,000, or by either of these two penalties alone.” This provision constitutes the legal basis of the offence, in addition to the requirement that the other two elements be established, namely, the material element and the moral element.

It also follows from the aforementioned Article 58 that, for this offence to be established, the data controller must have declared the purposes for which the processing is to be carried out and must have obtained approval from the National Authority or been granted authorization to that effect.

⁸ Article 12 of Law No. 18-07 provides: “Unless otherwise provided by law, every processing operation involving personal data shall be subject to a prior declaration before the National Authority or to its authorization, in accordance with the provisions laid down in this Law.”

⁹ The National Authority for the Protection of Personal Data was established pursuant to Law No. 18-07, under Title III thereof. It is an independent administrative authority whose functions include granting authorizations and receiving declarations relating to the processing of personal data. See Article 25 of Law No. 18-07.

The controller must then alter those purposes or broaden their scope to include other objectives that had not previously been declared¹⁰

The purpose of this provision is to prevent any unlawful use by the data controller for purposes other than those for which the data were collected, even though most of the provisions of this law are derived from European directives, French legislation, and certain Arab laws that preceded it in this field. Indeed, authorization to process personal data does not transform such data from private information into public information. Likewise, the consent of the data subject to the processing of their personal data does not imply unrestricted freedom to circulate or transfer such data to everyone

¹¹The elements of this offence are as follows:

First Branch: The Material Element of the Offence

The material element of this offence consists in the commission of criminal conduct through the unlawful use of personal data processed by automated means. This is established by referring to the declaration submitted by the data controller and comparing it with the acts or purposes subsequently pursued. If the subsequent use does not correspond to the purposes stated in the declaration, the offence is established. This would be the case, for example, where the processing is carried out for the purpose of creating a medical file for therapeutic purposes and is subsequently exploited for the commercial advertising of a particular medicine¹²

As for judicial applications of this offence, German courts ordered the suspension of the population census in 1984 after establishing that the Ministry of the Interior had been able, through the census forms, to obtain the addresses of a group of extremist terrorists. This was regarded as a misuse of the data that had been collected for a specific purpose, namely, conducting the population census¹³

Under Article 58, the persons held responsible in this regard are all those who possess the data and who have participated in any of the stages of processing, from collection and organization to those who have received the processed data or the processing itself for the purpose of using such data. In all cases, the National Authority has the power to assess whether the purpose actually pursued constitutes a modification of or departure from the purposes declared to it.¹⁴

Subsection Two: The Mens Rea of the Offence

This offence is considered an intentional offence, which necessarily requires the existence of criminal intent in both its elements, namely knowledge and intent. In other words, the offender must know that he or she is using the processed data for a purpose other than the one previously specified, and his or her will must be directed towards achieving that purpose. Accordingly, once these elements are established, the offence is deemed to have been committed and is punishable by the Algerian legislator, pursuant to the aforementioned Article 58, either by imprisonment for a period ranging from six months to one year (the offence being classified as a misdemeanour), in addition to a fine ranging from DZD 60,000 to DZD 100,000. The court may also impose only one of these two penalties.

Furthermore, the supplementary penalties provided for under the Penal Code may be imposed, or an order may be issued for the deletion of part or all of the personal data subject to processing, the

¹⁰ Tabache, Azzeddine, "Criminal Protection of Personal Data in Algerian Legislation: A Study in Light of Law No. 18-07 on the Protection of Natural Persons in the Processing of Personal Data," article published in Academic Journal of Legal Research, No. 02, 2018, pp. 26–60, p. 53.

¹¹ Hamoudi, Nasser, Criminal Protection of Electronic Commerce, Master's Thesis submitted in fulfillment of the requirements for a Master's degree, Criminal Law, Faculty of Law, University of Algiers 1, 2015, p. 114.

¹² Tabache, Azzeddine, op. cit., p. 53.

¹³ Ben Saïd, Sabrina, Protection of the Right to Privacy in the Age of Technology: Information and Communication, Doctoral Dissertation submitted in fulfillment of the requirements for a PhD in Legal Sciences, Constitutional Law specialization, Faculty of Law and Political Science, University of Batna, 2014/2015, p. 140.

¹⁴ The French legislator has criminalized the alteration of the purposes of processing pursuant to Article 226-21 of the French Penal Code, imposing a more severe penalty consisting of imprisonment for a period of two to five years, in addition to a fine, without allowing a choice between the two penalties. The Tunisian legislator likewise penalizes the same conduct under Article 94(2) of the 2004 Law on the Protection of Personal Data, while the Moroccan legislator has criminalized the same conduct under Article 54 of Moroccan Law No. 08-09 concerning the protection of individuals with regard to the processing of personal data.

processing of which resulted in the commission of the offence.¹⁵ A legal person that commits this offence, where the data controller is a legal person, shall be subject to the general rules laid down in the Penal Code.¹⁶

Section Two: Offence of Retaining Data Beyond the Specified Period

This offence is provided for by Article 65(2) of Law No. 18-07. It is also referred to as the offence of retaining personal data beyond the authorized period. This offence is committed whenever personal data are processed by automated means and retained for a period exceeding the authorized period. The purpose of criminalizing such conduct is to reaffirm that personal data may not be retained indefinitely, except in exceptional cases provided for by law.¹⁷

The Algerian legislator has classified this offence as a simple misdemeanour, criminalizing the act of retaining or keeping processed data after the expiry of the specified period, pursuant to Article 65(2) of Law No. 18-07, which constitutes the legal basis of this offence, while requiring the existence of both the material element and the mens rea of the offence.

Subsection One: The Actus Reus of the Offence

The material element of this offence is established where personal data that have been subject to automated processing are retained for a period exceeding that specified in the declaration or authorization submitted to the National Authority for the Protection of Personal Data. The offence is deemed to have been committed even where the processing itself was carried out in accordance with the applicable legal procedures, provided that the data were retained beyond the specified period.

The National Authority may not arbitrarily intervene in determining a specific retention period for the data. However, Article 9(e) of Law No. 18-07 provides that:

“Personal data must be:

e- Retained in a form allowing the identification of the persons concerned for a period not exceeding the period necessary to achieve the purposes for which they were collected and processed.”

Article 14(6) further requires that this period be specified in the declaration submitted to the National Authority.¹⁸ However, as an exception, such data may be retained for historical, statistical, or scientific purposes beyond the previously specified period, upon a request submitted by the data controller to the National Authority for the protection of such data. The latter has the power to assess whether a legitimate interest exists that justifies extending the retention period.¹⁹

In addition to specifying the retention period in the declaration, this period may also be established by a legislative or regulatory provision, as provided, for example, under Law No. 16-03 concerning genetic fingerprinting.²⁰ Article 14 thereof establishes a retention period of twenty-five (25) years for genetic data relating to the genetic fingerprints of the ascendants and descendants of missing persons, as well as suspects who have been prosecuted and have benefited from an order of dismissal or a final acquittal judgment. A period of forty (40) years applies to convicted persons, calculated from the date on which the judgment becomes final, as well as to missing persons and deceased persons whose identities are unknown.²¹

Subsection Two: The Mens Rea of the Offence

¹⁵ Pursuant to Article 71(1) of Law No. 18-07.

¹⁶ This is provided for under Article 70 of Law No. 18-07.

¹⁷ This is because the electronic storage of personal data has become easy, and data can be retained in a system indefinitely. Hammoudi Nasser, *op. cit.*, p. 112.

¹⁸ Article 14(6) of Law No. 18-07 provides: “The declaration must include the following: 6- The period for which the data are retained...”

¹⁹ The final paragraph of Article 9 of Law No. 18-07.

²⁰ Law No. 16-03 of 19 June 2016, concerning the use of genetic fingerprinting in judicial proceedings and the identification of persons, Official Gazette, No. 37, published on 22 June 2016.

²¹ Tebache Ezzeddine, *op. cit.*, p. 55.

The mens rea of this offence consists in the requirement that criminal intent be established through its two elements, namely knowledge and intent. This act is not punishable when committed through negligence. Accordingly, the offender's intent must be directed towards retaining the processed data for a period exceeding the period prescribed by law or specified in the declaration, while being aware that such conduct is punishable by law and nevertheless proceeding to commit it.²²

The French legislator criminalized this conduct under the aforementioned Law No. 78-17 relating to Information Technology, Files and Liberties, referring to it as the "right to be forgotten."²³ Similarly, Arab legislation has criminalized the offence of retaining personal data beyond the prescribed period. This is the case, for instance, with the Tunisian legislator under Article 94 of the 2004 Personal Data Protection Act, Article 55 of Moroccan Law No. 08-09, and the Jordanian legislator under Article 19 of the 2018 Data Protection Law.

The penalty for this offence consists of a fine ranging from DZD 200,000 to DZD 500,000, without prejudice to more severe penalties. It is one of the least severe penalties provided for under this Law, while the offender may also be subject to the supplementary penalties stipulated in Article 9 of the Penal Code.

Chapter Two: Offences of Disclosing Personal Data to Unauthorized Persons

This category of offences is considered among the most serious forms of unlawful conduct, for which the Algerian legislator has imposed stringent penalties, whether under the Penal Code, pursuant to Article 301 concerning the disclosure of professional secrets,²⁴ or under Article 40 of Law No. 18-07, which requires anyone who gains access to personal data by virtue of their duties to maintain professional confidentiality.

The Algerian legislator has also criminalized other forms of professional secrecy breaches under Law No. 18-07, identifying two principal forms: allowing unauthorized persons to access personal data (First Section), or transmitting such processed or received data to unauthorized persons (Second Section).

As for the unlawful disclosure of data, it refers to "the transfer of personal data by the person controlling such data in the course of its processing, storage, or transmission to a person or entity not authorized to receive such data."²⁵

First Section: The Offence of Allowing Unauthorized Persons to Access Personal Data

The Algerian legislator provided for this offence under Article 60 of Law No. 18-07, classifying it as a misdemeanour for which all persons who, by virtue of their duties, possess personal data may be held liable. Such persons may include members of the National Authority for the Protection of Personal Data, the data controller, the data processor,²⁶ and all persons responsible for the various stages of processing, including persons designated by the data controller to have access to such data.²⁷

Subsection One: The Actus Reus of the Offence

The criminal conduct constituting this offence consists in allowing third parties to access the data. Article 03-14 defines a "third party" as: "any natural or legal person, public or private, or any other entity other than the data subject, the controller, the processor, and persons authorized to process the data who are subject to the direct authority of the controller or the processor."

²² Tabach, Azzeddine, op. cit., p. 55.

²³ Hammoudi, Nasser, op. cit., p. 113.

²⁴ The "right to be forgotten" refers to "the individual's right not to have the controller retain their personal data for a period exceeding the original purpose or objective for which such data were collected."

²⁵ This is provided for in Article 301 of the Algerian Penal Code. The disclosure of a secret means disseminating and transmitting information, making it known to third parties, or communicating it to a large number of people. Generally, it consists in removing information from the sphere of confidentiality and secrecy after it had been restricted to its holders or to persons entrusted with it by virtue of their professional duties, without the knowledge or consent of the person concerned. This is what the law seeks to protect against unlawful disclosure. See: Hammoudi, Nasser, op. cit., p. 116.

²⁶ Ben Saïd, Sabrina, op. cit., p. 141.

²⁷ Article 03-13 defines the processor as: "any natural or legal person, public or private, or any other entity that processes personal data on behalf of the controller."

This conduct may take any form expressing the acceptance of the persons referred to above that third parties gain access to the data by any means whatsoever, such as providing a password, leaving the system open, or failing to object to access despite being aware of it.

It should be noted that the Algerian legislator used the term “access,” which is generally employed in the context of automated processing, whereas Law No. 18-07, in general, was enacted to protect personal data processed both automatically and by traditional means.²⁸ This therefore raises the question of whether this offence may be established where the data are processed automatically or otherwise, and unauthorized persons are subsequently allowed to access such personal data through non-automated means, particularly given that criminal law does not permit broad interpretation or analogy.

As regards determining whether the persons who have accessed the processed data are authorized to do so or not, this may be verified through the declaration submitted to the National Authority.²⁹ Article 14-04 stipulates that the data controller must identify the persons to whom the processed data may be disclosed. Accordingly, the absence of their names from the declaration renders them unauthorized to access such data.³⁰

Section Two: The Mens Rea of the Offence

Like the other offences discussed above, this offence is intentional in nature and requires the presence of criminal intent in its two elements, namely knowledge and intent. The perpetrator must know that the person is not authorized to access personal data, while nevertheless intending to engage in the prohibited conduct. However, this offence is not established where access to such data is permitted by mistake, such as when the perpetrator mistakenly believes that the person is authorized to access personal data. In such a case, the perpetrator shall instead be subject to the provisions of Article 65 or Article 69 of Law No. 18-07, respectively concerning the breach of the obligation of confidentiality and data security, and the negligent disclosure of data.

It should also be noted that the unauthorized person who accesses the processed data may be regarded as an accomplice to the offence. Where the processing is carried out automatically, such person may also be prosecuted for the offence of unlawfully accessing an automated data-processing system, punishable under Article 394 bis of the Penal Code, which provides: “Any person who fraudulently accesses or remains in all or part of an automated data-processing system, or attempts to do so, shall be punished by imprisonment for a term of three (03) months to one (01) year and a fine ranging from DZD 50,000 to DZD 100,000”³¹

The penalty for this offence is imprisonment for a term of two (02) to five (05) years and a fine ranging from DZD 200,000 to DZD 500,000, in addition to the possibility of imposing supplementary penalties. As for a legal person, it shall be subject to the penalties compatible with its legal nature and provided for under the Penal Code.

Subsection Two

The Offence of Disclosing Processed or Received Data to Unauthorized Persons

This is the conduct punishable under Article 69 of Law No. 18-07. One of the distinctive features of this offence is that the Algerian legislator has limited the persons subject to its provisions to: the data controller, the data processor, and any person who, by virtue of their duties, is entrusted with processing personal data.

The scope of this offence is therefore limited to persons who have submitted applications for authorization or declaration concerning the processing, as well as persons appointed to carry out

²⁸ Tabach, Azzeddine, op. cit., p. 56.

²⁹ This is expressly provided for in Article 03-03 of Law No. 18-07, which defines processing as: “any operation or set of operations carried out by automated means or otherwise on personal data.”

³⁰ Tabache, Ezzeddine, op. cit., p. 56.

³¹ Tabache, Ezzeddine, op. cit., p. 57.

such processing. The commission of this offence, like other offences, requires—in addition to the legal element represented by the aforementioned Article 69—the existence of both the material element (*actus reus*) and the mental element (*mens rea*).

First Subsection: The Material Element of the Crime

The criminal conduct constituting this offense consists of several acts specified in Article 69 referred to above, namely the abusive use, fraudulent use, or communication of the processed or received data to persons who are not authorized to access such data.

It may be observed from this provision that, for this crime to be established, the legislator does not require the data to have been fully processed. The perpetrator may commit the act merely upon receiving the data, for example, at the collection stage, and subsequently communicate it to persons who are not authorized to access it.³²

Part of the legal scholarship considers this offense to be a formal crime, which is established merely by disclosure or communication, without requiring the occurrence of any specific harm to the data subject, since the purpose of criminalization is to preserve the confidentiality and privacy of personal data rather than to require the occurrence of a criminal consequence.³³

Second Subsection: The Mental Element of the Crime

The mental element of this offense consists of either general criminal intent or unintentional fault. The legislator penalizes this offense whether it is committed intentionally or through negligence (unintentionally), and imposes the same penalty provided for under Article 69 of Law No. 18-07. One application of this situation concerns a case in which the offense of unlawfully disclosing data³⁴ through error was found to have been committed by a person responsible for processing personal data who submitted a document to one of the authorities containing, by mistake, the telephone number of an individual. The courts considered the telephone number to constitute personal data enabling the direct identification of its holder, and the data controller was consequently convicted of this offense.³⁵

As for the penalty prescribed for this offense, it consists of imprisonment for a term of one (01) to five (05) years and a fine ranging from DZD 100,000 to DZD 500,000, in addition to the application of the same provisions relating to supplementary penalties and the penalties applicable to legal persons referred to above.

With regard to all the offenses addressed in this research paper and provided for under Law No. 18-07, the subject matter of the offense may be confiscated for the purpose of reallocation or destruction, pursuant to Article 72-01. Article 71-02 of the same Law provides for the possibility of erasing all or part of the processed data that resulted in the commission of the offense. Furthermore, Article 73 of the same Law provides for the punishment of attempts to commit all these offenses by the same penalty prescribed for the completed offense. In the event of recidivism, the penalty is aggravated pursuant to Article 74 of Law No. 18-07.

Conclusion

In conclusion, it can be argued that, by enacting Law No. 18-07 on the protection of natural persons in the processing of personal data, the Algerian legislator has filled the legislative gap that had previously existed within the Algerian legal framework governing information technology, particularly in light of the information revolution and the emergence of electronic tools and software, applications, social networking platforms, computers, and other technologies that have become an

³² Tabach, Azzedine, *op. cit.*, p. 58.

³³ Hammoudi, Nasser, *op. cit.*, p. 117.

³⁴ It may be argued that the security and police sectors constitute an environment particularly conducive to retaining large amounts of personal information and data. Consequently, the risk of disclosure by persons entrusted with such information is significant. An example of this is the case of an Austrian police officer who provided a private informant with technical information concerning certain individuals, relating to their criminal records and stored in the computer system used by the police. This also applies to other sectors that are no less sensitive than the security and police sectors, such as banks, financial institutions, hospitals, and others. See: Ben Said, Sabrine, *op. cit.*, p. 141.

³⁵ Tabach, Azzedine, *op. cit.*, p. 58.

integral part of the daily life of every natural person. There are hardly any risks greater than those posed by infringements upon privacy and individual freedoms, particularly the right to private life, in view of the tremendous technological advances in modern means of communication and their use in ways that may encroach upon individuals' personal rights. This law largely mirrors the European directives issued in the field of personal data protection, as well as the French law enacted in 2004 concerning personal data, in addition to most Arab legislative instruments adopted prior to this law, such as the Tunisian Law of 2004, Moroccan Law No. 08-09, and the Jordanian Law of 2009.

This law embodies several constitutional principles, including the right to privacy and the principle of respect for the law. It stipulates that the processing of personal data may not be carried out without the explicit consent of the data subject, who has full freedom to withdraw such consent. It also provides for the establishment of the National Authority for the Protection of Personal Data, whose task is to ensure the implementation of the provisions of this law. Among the main advantages introduced by the law are the following:

It adopts a broad concept of personal data, corresponding to the definition found in most comparative legislation, as well as in the General Data Protection Regulation of 2016.

It broadens the scope of processing to include both automated and manual processing of data.

It identifies various acts that constitute offences under this law, most of which are classified as misdemeanours punishable by imprisonment and fines.

As for the recommendations that may be proposed, the following can be highlighted:

The first recommendation that may be made in this regard is that there can be no effective protection of private life, no guarantee of the security of personal data, and no genuine freedom of opinion or institutional freedom as long as the data subject is uncertain about the circumstances under which their personal data are collected and the purposes for which such data are processed automatically.

It is impossible to provide absolute or complete security for the confidentiality of personal data, given the possibility of remotely penetrating computer or mobile-phone memory and using the data unlawfully, thereby resulting in violations of individuals' privacy and rights.

There is a need to expedite the establishment and effective operation of the National Authority for the Protection of Personal Data.

Greater awareness should be raised among individuals regarding the need to protect their personal data themselves by avoiding excessive disclosure and use thereof, given the risks to which they may be exposed as a result of entering the virtual world, despite the existence of criminal protection for such data, which nevertheless remains insufficient.

There is a need for cooperation among different States, including the establishment of an international body tasked with monitoring the methods of automated processing of personal data carried out by various global companies and websites.

Greater efforts are required to address the phenomenon of the lack of a culture of filing complaints and reporting violations committed against personal data processed by automated means.

The specific nature of Muslim Arab societies, including Algerian society, should be taken into consideration by providing that the purpose of processing personal data must not be contrary to public order or public morals.

References

Theses and Dissertations:

Ben Saïd Sabrina, Protection of the Right to Privacy in the Age of Information and Communication Technologies, PhD Dissertation in Legal Sciences, Constitutional Law specialization, Faculty of Law and Political Sciences, University of Batna, 2014/2015.

Hamoudi Nasser, Criminal Protection of Electronic Commerce, Master's Dissertation, Criminal Law specialization, Faculty of Law, University of Algiers 1, 2015.

Articles:

Mohamed Ahmed Al-Maadawi, "Protection of Users' Informational Privacy through Social Networking Sites: A Comparative Study," published in a journal whose name is not specified, No. 33, Part Four, pp. 1926–2057.

Tabache Azzedine, "Criminal Protection of Personal Data in Algerian Legislation: A Study in Light of Law No. 18-07 on the Protection of Natural Persons with Regard to the Processing of Personal Data," *Academic Journal of Legal Research*, No. 02, 2018, pp. 26–60.

Legal Texts:

Law No. 16-03 of 19 June 2016, concerning the use of genetic fingerprinting in judicial proceedings and the identification of persons, *Official Gazette*, No. 37, published on 22 June 2016.

Law No. 18-07 of 10 June 2018, concerning the protection of natural persons with regard to the processing of personal data, *Official Gazette*, No. 34, published on 10 June 2018.

European Directive 95/46/EC, available at: EUR-Lex, accessed on 08/02/2020 at 21:09.

General Data Protection Regulation (GDPR), a European Union legal framework governing data protection and privacy. It was adopted on 14 April 2016, thereby repealing European Directive 95/46/EC, and entered into force on 25 May 2018.

French Personal Data Protection Act of 2004.

Tunisian Personal Data Protection Act of 2004.

Moroccan Law No. 08-09 on the Protection of Individuals with Regard to the Processing of Personal Data