

Penal protection of the right to privacy in the digital environment Under Algerian legislation "Crime of not obtaining prior consent"

Laouarem Wahiba¹

¹Mohamed El-Bachir El-Ibrahimi University Bordj Bou Arreridj (Algeria).

The E-mail Author: wahiba.laouarem@univ-bba.dz

Received: 02/03/2024

Published: 16/11/2024

Abstract:

Private life is one of the fundamental interests and values that the Criminal Code is concerned with protecting through texts that criminalize assault, in close connection with individuals' freedoms and the resulting preservation of their dignity and the preservation of their perpetuity. The risk of infringing on private life has increased after the wider use of computers to gather information about individuals, which has made the individual's life so open to all that he can no longer cover up this previously earned advantage. Therefore, legislation, including Algerian legislation, restricts bodies and institutions to procedural and substantive rules governing the collection and storage of individuals' information, and it is a punishable offence to bypass or ignore these rules.

Keywords: private life; digital environment; personalized data; processing; consent of the person concerned; responsible for processing.

1. INTRODUCTION

Accelerated technological development has made it easier to collect and store people's information, thus facilitating access to and circulation of data. The majority of countries have adopted the e-governance project with the aim of bringing the Department closer to the citizen electronically, using information technology systems, so that personal data is easy to trade in as the data is developed, stored and processed.

However, to the extent that modern communication technology has facilitated communication between persons or between persons and departments, it has, in turn, demolished the divide between public life and individual specificities, thereby threatening the individual's private life, as personal data have become available through such technology to be collected and defamed unjustifiably or without the consent of the person concerned.

This has driven international, regional and national efforts to find principles and norms that will safeguard the right to private life and necessarily strike a balance between society's needs to collect, store and process personal data, and ensure that such data is protected from the risks of unlawful use of processing techniques.

Recent legislation has therefore reviewed its statutory regulations by promulgating special laws that are protected and regulating the processing of personal data and penalizing those who violate the constitutional principle of the inviolability of privacy. Under the terms of Act No. 18-07, the National Authority for the Protection of Personal Data was established to protect individual freedoms.

The problem posed requires examining the scope and effectiveness of the system of criminal protection of personal data by extrapolating the new law, Act No. 17-08, specifically the offence of violating the obligation to obtain a person's prior consent.

2. The Emergence of the Idea of the Right to Private Life

The right to private life is one of the manifestations of fundamental rights and freedoms enshrined in most international instruments as well as in national constitutions.

The right to private life is the cornerstone of personal liberty and a fundamental pillar of human rights and public freedoms. Accordingly, this right requires respect by the authorities and individuals and, at the same time, protection against unlawful violation of this right.

2.1 justification for adopting a special legal regulation

Information about individuals may be stored in traditional ways by being placed in ordinary files, any paper, and may be collected in computer files or automated cards. Different companies and institutions have moved towards using the second method given the computer's great ease in processing this data and the large volume of information they may absorb, as well as the high accuracy and skill in dealing with it in terms of classification, arrangement, retrieval and transmitted and traded from one place to another through regional and international communication networks.

While these benefits have been remarkable, they have also raised significant legal and, in particular, individual rights and freedoms, challenges. Given that these advantages may be misused as a way in which a computer can be a very dangerous means of infringing a fundamental right to the level of the right to privacy's ability to permanently preserve information has made it impossible for the element of time to enter it into oblivion, and its ability to mix and integrate information Make it possible to

give a clear and complete picture of the individual's personality and aspects, and to exploit them for what they have been collected for.

This has resulted in a review of the content of the right to privacy, since this right was considered in material terms, i.e. the right of individuals to be protected from all forms of physical abuse of their lives and property, such as the right to inviolability of the home and the right to confidentiality of correspondence,

The concept of privacy extends to the so-called moral privacy that recognizes individuals' right to protect their moral values such as the protection of honour, reputation and dignity. It covers all aspects of infringement on the individual's personal rights and freedoms, whatever their form or nature, including the right to digital privacy.

Hence the urgency of establishing a legal regime to regulate the use of individuals' personal information, which has been confirmed that the general rules of professional confidentiality cannot protect people against computers, as computer-contained information may be known by a very large number of computer staff and users.

Recourse to traditional provisions of the Penal Code that protect and consider individuals' reputation and honour is also futile, as personal information may include the reputation and perception of individuals, as well as other data, as long as a person does not wish to access such information to others, his will must be respected.

2.2 Legislative evolution in the protection of the right to personal life

Legislative attention has been given to regulating the collection and processing of individuals' personal data following a sense of information risks at the international level, thanks to the efforts of international and regional organizations that urge the need to impose special protection of the right to privacy against information risks, followed by initiatives at the national level. The protection of the right to digital privacy has been significantly developed in Algerian legislation.

2.2.1 At the international level

The first initiatives began specifically with organizations concerned with the defence of human rights and personal freedoms, such as the Stockholm Conference of 1967 and the 1968 Tehran Conference of the United Nations, which examined the impact of technological development on the protection of individuals' rights and freedoms against the dangers of aggression. ¹

¹ Osama Abdallah Gaid, *Criminal Protection of Private Life and Information Banks, Comparative Study*, Arab Renaissance House, Cairo, 3rd Edition, 1994, p. 81.

In 1989, the United Nations adopted a manual on the use of computing in the flow of personal data, and the 14/12/1990 date of the General Assembly's adoption of the Manual on the Regulation of the Use of Automated Processing of Personal Data. As well as the Organization for Economic Cooperation and Development (OECD), which has been developing guides and guidelines on privacy protection and data transfer since 1978,

In addition to providing guidance on data protection, the European Union highlighted the 1995 Handbook on the Protection of Individuals in Relation to the Processing of Personal Data and Their Freedom of Transmission, as well as the 1997 Handbook on the Protection of Communications Data.

As early as the 1970s, States began adopting laws to protect individuals' personal data, beginning with Germany under the Act of 7/10/1970 and then Sweden under the Act of 11 May 1973, followed by the United States of America in its Act of 31/12/1974 as well as France, which enacted the law known as the "Informatics and Freedoms Act".¹

The enactment of these laws was motivated by the framing of the collection and processing of individuals' personal data in such a way as to ensure that the constitutionally enshrined fundamental rights and freedoms are not compromised, as well as by the legislative will of those States to ensure a great deal of protection for individuals through the rights accorded to them .²

Jurisprudence considers personal data protection laws to be the defender of individual freedoms because they enshrine the protection of many rights and freedoms. Most of these rights are of constitutional value, thereby enhancing the value of these laws³.

This was not the case, but the Council of Europe concluded the first global convention on the protection of personal data on 28 January 1981, called the Strastburg Convention 108, which entered into force on 1 October 1985 .⁴

The European Council then adopted European Recommendation No. 95/46 of 24 October 1995 on the protection of natural persons in the face of the processing of

¹ Alain Bensoussen, Computer legal guide and freedoms, Francis Lefebvre, France, ed 2008, p 15, n° 5.

² Vincent Fauchoux, Pierre Deprez, Jean-Michel Bruguière, Internet Law (laws – contract and usages), 2 ed, Lexisnexis, Paris, 2013, p314.

³ Celine Castets Renard, Internet law, Montchrestien, Lextenso, France, 2010, p 14.

⁴ Council of Europe, convention for the protection of individuals with regard to the automated processing of personal data, European Treaties Series n° 108, Strasbourg, 28 January 1981.

personal data and the freedom of movement of data known as the "European Recommendation for the Protection of Personal Data"¹ .

This recommendation was made with a view to harmonizing European States' legislation with regard to the protection of personal data. This recommendation has been repealed to be replaced by Regulation No. 2016/679 of 27 April 2016 on the protection of natural persons towards the processing of personal data and the freedom to transmit such data ².

2.2.2 At the national level

The protection of the right to personal privacy was initially enshrined in Algerian legislation through the provisions of the Penal Code relating to the protection of the right to privacy, as well as those enacted by the Algerian legislature concerning the protection of automated data-processing systems, after which legal regulation in this area was introduced under Act No. 18/07 on the protection of individuals' personal data .

2.2.2.1 Before Law No. 18-07

Algerian legislation protects the right of individuals to privacy, whether in the provisions of the Constitution or in the legislative texts. Article 39 of the 1996 Constitution enshrines the principle of respect for private life and related conversations and correspondence by stating: "The inviolability of a citizen's private life and the inviolability of his honour shall not be violated and protected by law. The confidentiality of correspondence and communications of all forms is guaranteed ", as is the intervention of the legislature under the constitutional amendment of 2016 ³.

The right of individuals to protect their personal goods is regarded as constitutional rights, article 46/4 of which states that "the protection of natural persons in the processing of personal data is a fundamental right guaranteed by law and punishable by law."

This principle is also enshrined in the Penal Code in its provisions on the protection of privacy and the protection of professional confidentiality, article 303 bis of which states that "... Whoever deliberately infringes upon the inviolability of a person's private life by whatever technique¹ : - Capture, record or transmit private or confidential calls or conversations, without the owner's permission or consent.

¹ Council of Europe, Directive 95/46, 24 October 1995 on the protection of individuals and the processing of personal data and the free movement of such data, OJ 1995 L 281, p 31.

² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EU. Available on the website, <https://eur-lex.europa.eu>

³ Law N° 16/01 of 6 March 2016 amending the Constitution, No. 14 of 2016.

By taking, recording or transmitting a photograph of a person in a private place, without the permission or consent of the owner "...

The phrase "by any technique whatsoever" through the article was intended to impose protection on all types of private communications, including those caused by accelerated technological development, and article 301 of the Penal Code criminalized the disclosure of professional secrecy.

The legislature has also provided protection for digital data in general and this applies to personal data, under articles 394 bis to 394 8 bis of the Penal Code, which criminalizes acts of prejudice to the automated data processing system .¹

In addition, the Legislature on Protection has singled out the information of individuals in areas of particular, such as data of individuals collected in the field of statistics and censuses. Article 5 of the General Population and Housing Statistics Act states that "the State shall ensure to the natural persons who are counted that the individual information they declare is in any way used only for statistical purposes" .²

Legislative Decree No. 94-01 of 15 January 1994 on the statistical system also contains provisions protecting statistical confidentiality and, in particular, individuals' data relating to their personal and family life, article 37 of which states that "The flagrant breach of the statistical confidentiality specified in articles 23 to 26 shall be subject to the penalties provided for in the Penal Code without prejudice to disciplinary sanctions" .³

However, while these texts can be used to resolve certain legal issues relating to the protection of personal data, they may not contain others. The legal provisions established for the protection of the right to private life in relation to the taking, recording or transmission of the image are essentially in conjunction with the inviolability of the private place, While the assault on personal data takes place in a virtual world that goes beyond the idea of the particular place specified in the criminalization text,

The provisions on occupational confidentiality were also designed to protect the confidentiality required by the nature of certain occupations, such as justice and medicine. Protection of personal data is a broad idea, including the protection of all personal information relating to individuals, Confidentiality or non-confidentiality of such information, such differences may constitute a major obstacle to the application of

¹ Moufida Mibarkia, Criminal Protection of the Right to Digital Privacy in Algerian Legislation, Journal of Shari' a and Economics, published by the Faculty of Shari' a and Economics, Prince Abdelkader University of Islamic Sciences, Constantine, vol. VII, 1st Edition, 2018, p. p.(481 - 469) .

² Law N^o. 86-09 of 29 July 1986 on the General Population and Housing Statistics, No. 31 of 1986.

³ Legislative Decree N^o. 94-01 of 15 January 1994 on the Statistical System, No. 3 of 1994.

these provisions to legal matters relating to personal data, on the grounds that the Penal Code prohibits the use of analogy ;It also prevents further interpretation of the penal text to contain unless it is provided for ¹.

On the basis of these considerations, an integrated legal regulation was required, as embodied in Algerian legislation under Act No. 18-07 on the protection of personal data.

2.2.2.2By Act No. 18-07

Since individuals must be recognized as entitled to the protection of their personal gowns, the legislature intervened initially under the constitutional amendment of 2016. Law No. 18-07 of 10 June 2018 on the Protection of Natural Persons in the Handling of Personal Data . ²

2.2.2.2.1Quality of personal data

Article 2 stipulates that: "Personal data, regardless of their origin or form, must be processed in the context of respect for human dignity, private life and public freedoms and must not prejudice the rights, honour and reputation of persons".

Article 2 states: "Personal data, irrespective of their origin or form, must be processed in the context of respect for human dignity, private life and public freedoms and must not prejudice the rights, honour and reputation of persons."

With regard to the term "personal data", every information, regardless of its corollary, relates to an identifiable or identifiable person... directly or indirectly, in particular by reference to the identification number, element or several elements of his physical, physiological, genetic, biometric, psychological, economic, cultural or social identity,"

This definition refers to the existence of two characteristics: first, that data of a personal nature relate to the natural person and not to the legal person, and secondly, that such data enables the identification and identification of the person with respect to him, and the doctrine has differed in the definition of a concept of personal data, which some consider to be "Those relating to an individual's private life such as his or her own health, financial and family condition" and the other considers that "there are different types of data on the inviolability of the private life of the human person and data that allow a picture to be drawn of his political trends, tendencies, religious beliefs and financial dealings,"

¹ Osama Abdullah Gaid, op. cit., p. 77-78.

² Law N^o 18/07 of 10 June 2018 on the Protection of Natural Persons in the Processing of Personal Data, OJ No. 34 of 2018.

However, under article 3 of the Personal Data Protection Act, the above-mentioned Act No. 18-07, Algerian legislation affirms that personal data is not required to be relevant only to individuals' private lives, but also to their professional life, political affiliation or even public life.

For the second term, "processing", it is intended according to the same article. "Every operation or set of operations carried out with or without the assistance of automated methods and applied to personal data such as assembly, registration, organization, preservation, convenience, alteration, extraction, access, use, delivery through transmission, publication or any other form of availability, approximation, interconnection, such as closure, encryption, surveying or destruction;"

2.2.2.2 Scope of application

Any treatment of a personal nature entails the formation of a file of such data, which may be an information file or a manual file, article 4 of which is confirmed in its first paragraph. "This Law applies to the automated or partial processing of personal data as well as to non-automated processing of a personal nature that is received or can be contained in handmade fabrications".

The scope of application of Act No. 18-07 remains restricted. The legislature excludes certain types of treatments from legal protection, such as the processing of personal data by a subjective person with the aim of engaging exclusively in personal or domestic activities.

Processing of personal data obtained and processing in the interest of national defence and internal or external security of the State and those relating to the prevention and punishment of crimes and offences, and then the data obtained in accordance with a special legislative provision.

3. Offence of breach of the obligation to obtain prior consent of the person concerned

The Algerian legislator dealing with personal data is obliged to comply with a set of procedural provisions and obligations, which are criminalized. In all, they include rules relating to their obligation to take a set of formalities prior to the processing process. They should also inform the person concerned of the treatment of his personal data in order to obtain his or her explicit consent.

In addition, the legislator has made provisions for measures to preserve the integrity and confidentiality of the data. Given that the effectiveness of the application of personal data protection laws is only with an independent body that ensures that they are respected The Algerian legislature has enacted rules aimed at facilitating

cooperation with the national authority in the performance of its work and at respecting its decisions; Violation of these rules of procedure is a legally punishable offence and we will be satisfied with the obligation to inform the person concerned of the processing of his personal data in order to obtain his or her express consent. in order to attach great importance to the will of the individuals involved in the treatment, the handler was obliged to obtain prior consent of the person concerned before the treatment is carried out and to override this obligation is a punishable offence under article 55 of Act No. 18-07.

3.1 meaning of the person's will

Article 7 of the Personal Data Protection Act, Act No. 18-07, states: "Processing of personal data can only be done with the express consent of the person concerned.

If the person concerned is incapacitated or incapacitated, consent shall be subject to the rules of common law.

The person concerned may refrain from consent at any time" ¹.

The "person in question" is defined in article 03 of the Act as "any natural person in respect of whom the personal data relating thereto are addressed" and thus excludes the moral person from the context of the person concerned in accordance with the law of the 18-07.

If the person concerned is a child, article 8 of the Act affirms that the processing of personal data relating to a child can only be done after the consent of his or her legitimate representative or where necessary by the competent judge, but that the judge may order the processing even without the consent of his or her legitimate representative if the best interest is invoked The child may at any time renounce his or her licence².

Article 2/(j) of European Recommendation No. 95/46 on the protection of personal data defines a person's consent as "any expression of will, free, private, certain, whereby the person concerned accepts that the personal data relating to him or her should be a place of treatment."

The "article 29" group referred to earlier clarified this definition by advisory opinion No. 15/2011 of 13 July 2011, stating that consent must be free, while emphasizing that the lack of fraud, fear and consent risks should be investigated³.

¹ See article 07 of Law N^o 18-07.

² See article 08 of the Law N^o 18-07

³ Article 29 Working Group, Opinion 15/2011 on the definition of consent, adopted on 13 July 2011, wp 187, p (12 – 18).

This requirement is raised in particular in the area of labour relations; An employee's consent to the processing of his personal data may be under pressure or coercion by the employer and the employee's consent may not be considered free in all cases¹.

The expression of will must also be special and specific, so that the handler must determine the exact place of consent by referring to the area of processing and its consequences.

It follows that the subject accepts only the authorized purpose when collecting such data and if the handler wants to use such data to another end he has to obtain a new satisfaction from the person concerned, that information is not the responsibility of the handler acting freely².

In addition, satisfaction must be assured, as the person concerned must be accurately and clearly aware of accurate and complete information, such as the nature of the data processed, the purpose of the processing and the consequences of the refusal to approve the processing³.

3.2 Elements of crime

Article 55 of the Personal Data Protection Act criminalizes Law No. 18-07 for the offender to process personal data without obtaining the consent of those concerned.

It stipulates that: "Anyone who handles personal data in violation of article 7 of this Act shall be liable to a penalty of 1 to 3 years' imprisonment and a fine of 100,000DA to 300,000 DA.

The same penalty shall be imposed on anyone who, despite the objection of the person concerned, handles data of a personal nature when such treatment is aimed at, in particular, commercial publicity or when the objection is based on legitimate grounds of."

The physical element of the offence is the external manifestation of the offender's activity, that is, criminal conduct that is foreseeable to criminalization and punishable, that is, external physical activity constituting the offence and the cause of the damage.

¹ Anne Debet, Measurement of diversity and protection of personal data, Report presented to the plenary session, CNIL, 15 May 2007, p. (13-14). Available on <https://www.cnil.fr>

² Article 29 Working Group, Opinion 15/2011, op. cit., p. 19.

³ Cynthia Chassigneux, Legal Framework for the Processing of Personal Data on Online Business Sites, doctoral thesis, University of Montreal, Faculty of Law, Private Law, Paris, 2003, p150.

It is clear from the text of the above-mentioned article 55 that there are two images of the criminal offence: the processing of personal data without the express consent of the meaning and the processing of personal data despite his objection.

3.2.1 Processing personal data without explicit consent

The offence specified in article 55 referred to above is the handler's handling of personal data without the prior consent of the person concerned.

In accordance with Article III of the Act, the handler or handler is any natural or moral person, public or private, or any other entity that, individually or in association with others, determines the purposes and means of processing the data¹.

The processing of data is whether it is complete, partial or non-automatic processing received or can be contained in manual files.²

The automated processing of the data is completed in whole or in part by means of automated methods such as recording the data, applying logical and/or computational processes to these data, altering, surveying, extracting or publishing them³.

The processing of a person's fortunate data can be carried out by public or private bodies and is a place of protection:

- When it takes place by a natural or moral person, the person responsible shall reside on the national territory or on the territory of a State which has a procurement equivalent to the national legislation in the field of the automation of personal data.

He is a resident of Algeria who is responsible for processing and is active in Algerian territory under the establishment of whatever its legal form.

- When the person responsible is not resident on the national territory and for the purpose of processing personal data resorts to automated or non-automated means located on the national territory, except for treatments used for the purposes of crossing the national territory.

In this case, the processing officer must, without prejudice to his personal responsibility, inform the national authority of the identity of his resident representative in Algeria, who replaces him in all his rights and obligations arising from the provisions of this Act and its implementing provisions⁴.

- Article (7) of the same Act requires not only satisfaction in order to remove

¹ See article 03, paragraph 12, of Act No. 18-07.

² See article 04 of Law 18-07

³ See article 03, paragraph 05, of the Act 18-07.

⁴ See article 04, paragraph 04, of the Act 18-07

treatment from the field of criminalization but also explicit consent. The legislator did not clarify what was meant by explicit consent, and the French Conseil d'Etat's jurisprudence stated that express consent was meant by an express agreement written in a special document.

- Some States' legislation in that regard explicitly stipulated the need for written consent, such as Tunisian legislation¹.

- As long as the Algerian legislature has failed to determine its position in this regard, there is nothing to prevent the consent of the subject from being oral and then legally valid. and, more precisely, that the lack of writing does not firmly confirm the perpetration of the offence punishable under article 55 of the Act and in any event, The availability of the written requirement is of the utmost importance in the issue of proof that lies with the handler.

- In view of the importance of prior consent to the treatment process, certain legislation, such as Tunisian legislation, under a special provision, criminalized the use of deception, violence or threats for the purpose of obtaining the treatment's consent.

- As defined in the same article, article III above, "Consent of the person concerned", "Any expression of distinctive will whereby the person concerned or his or her legitimate representative accepts the manual or electronic processing of personal data relating to him or her."

- Article 7 of the Act affirms and limited cases that do not require the consent of the person concerned or are not required if the treatment is necessary, i.e. through which the legislator has been removed from the Criminalization Service in certain cases where the treatment is carried out without the consent of the person concerned. These cases are:

- Respect for a legal obligation to which the person concerned is subject or is responsible for processing, which is particularly the tax and social obligations imposed on the employer²;
- To protect the person's life, which is one such case in natural disasters when treatment is necessary to assist victims³;

¹ Otherwise, the Council of Europe's Group of 29 interpreted the text of article II. (2) of European Recommendation No. 95/46 on the protection of personal data indicates that writing is not a requirement for the consent of the person concerned, i.e. that the consent of the person concerned may be oral, noting that the wording of article II (2) There is no assertion that there should be a particular form of expression of will.

² Sameh Abdul Wahid Elhami, Legal Protection of Personal Data, Study in French Law, Section II, Law Journal, Kuwait University, No. 4, 2011, p. 252.

- To perform a contract to which the person concerned is a party or to carry out pre-contract actions taken at the person's request;
- To safeguard the person's vital interests if he or she is physically or legally unable to express his or her consent-;
- To carry out a task which is part of the public interest or the exercise of the functions of the public authority which is handled by the processing officer or other person who is informed of the data;
- To achieve a legitimate interest on the part of the addressee or addressee, taking into account the person's fundamental interest and/or rights and freedoms. The legitimate interest adheres to the principle of proportionality so that the interest, however legitimate, cannot ignore the fundamental rights and freedoms of the individuals concerned.

Article 09 of the Act provides that the relevant personal data shall be processed:

- Addressed in an impartial and legitimate manner,
- grouped for specific, stated, clear and legitimate purposes and not subsequently addressed in a manner incompatible with these ends,
- appropriate, appropriate, not excessive and not exaggerated in view of the objectives for which they were collected or addressed,
- True, complete and honest if necessary,
- Preserved in a way that enables the identification of the persons concerned for the period specified and necessary to accomplish the objectives for which they have been collected and processed¹.

It should be noted that several entities have become forming personal data files either in the public sector by public administrations and institutions or in the private sector in banks, borrowing institutions and others.

In order to protect individuals' right to confidentiality of their private lives, the legislature has established objective and procedural rules to regulate the collection and processing of personal data, consisting, on the one hand, of restricting the collection, storage and processing of individuals' data by certain controls set out in article 09 of Act No. 18-07, so that the handler must legitimately collect such data. The State party is

³ Gérard Haas, Yael Cohen-Hadria, Legal guide computer and freedoms, ENI editions, France, October 2012 , p 89.

¹ See article 09 of Law N° 18-07.

also required to comply with the authorized purpose of requesting a licence or authorization of treatment, as well as to respect the deadlines for these ends.¹

On the other hand, the legislator has developed special rules governing certain types of data; As a general rule, certain types of personal data are prohibited from being processed in article 03, which is sensitive², and data of a personal nature relating to a child cannot be processed only after obtaining the approval of his or her legitimate representative or the authorization of the competent judge.³

In others, under article 11 of the Code, the competent authorities to deal with them shall be restricted to information relating to case law;

Article 10 of the Act affirms that "personal data relating to crimes, penalties and security measures can only be processed by the judiciary, public authorities, legal persons in a public interest and justice assistants within their legal competence.

The processing must identify who is responsible for the processing, the purpose, the persons concerned and those not entitled to access this information, its source and the procedures to be taken to ensure the proper processing.

Article 11 of the same Act states that judicial decisions requiring an assessment of a person's conduct cannot be based on the automated processing of personal data that includes an assessment of certain aspects of his or her personality.⁴

Articles 32 to 36 of the same Act also set out provisions relating to the rights of persons concerned with data, so that the individual has the right to have access to his or her personal information and to seek correction from possible errors, and the right to challenge the processing process on the basis⁵.

In addition, under articles 44 and 45 of the same law, the legislature has established rules on the transfer and circulation of data to a foreign State⁶.

3.2.2 Processing personal data despite the subject's objection

The second paragraph of article 55 mentioned above penalizes the failure to respect the right of objection recognized to the subject. The basis of this right is article 36, which provides that "the person concerned shall have the right to object, for legitimate

¹ See article 09 of the Law N° 18-07.

² Sensitive data as stipulated in article 03, paragraph 06, of Law N° 18-07 "Personal data showing racial or ethnic origin, political opinions, religious or philosophical convictions or trade union affiliation of the person concerned or related to his or her health, including his or her genetic content."

³ See article 08 of the Law N° 18-07 .

⁴ See article 11 of Law N° 18-07.

⁵ See articles 32 to 36 of the Law N° 18-07.

⁶ See articles 44 and 45 of the Law N° 18-07.

reasons, to the treatment of his personal gifts". For example, the worker shall object to the collection and processing of his data relating to his or her family and private life, without having any relevance to the work .¹

Article 36 of the same Act does not specify the nature of the data to which individuals are entitled to object. The text is general and the jurisprudence considers that the objection is not in relation to ordinary data such as name and address and is often in cases involving infringement of private life and individual freedoms.

The handler's disregard for the interception of the subject only falls into the offence, if it is based on legitimate grounds. It is illogical for an order to store individuals' information completely and completely to depend on their consent, as this would impede the information development that has become indispensable in our time².

Therefore, individuals must prove that there are legitimate grounds for objection that M-N - logical to invoke during the refusal of the processing process³

Consequently, the offence defined in article 55, paragraph 2, of the 18-07 Code remains to be determined by the judge's discretion, who must balance the right of the person concerned to intercept with the treatment required by the handler and assess whether or not the offence is committed⁴.

The subject need not demonstrate the availability of the legitimate grounds for objection if the processing is for propaganda purposes, particularly commercial, in other words, that the right to object to the processing of personal data in the event of its transmission to another for the purpose of propaganda is not conditional s personal data and their use for propaganda unless the stakeholder so agrees, It would therefore be logical to exempt the stakeholder from establishing the legitimate grounds for objecting to the transfer of his personal goods to others until publicity .⁵

In both photographs, the offence punishable under article 55 of the Act is a deliberate offence requiring the tendency of the offender's will to process the personal data of individuals without prior or express consent of the person concerned, notwithstanding his objection, knowing that this is prohibited by law.

¹ Aupele Nadine, Computer-aided Criminal Offences, doctoral thesis, Criminal Law, Faculty of Law and Economics, Montpellier, 1984, p 188.

² Hussam al-Din Kamel al-Ahwani, op. cit, p. 39- 40.

³ Nader Amran, Protection of Personal Data in the Light of Organic Law No. 63 of 2004 of 27 July 2004, Journal of the Judiciary and Legislation, published by the Centre for Legal and Judicial Studies, Tunisia, No. 8, 46th year, October 2004, p. 177.

⁴ Jerrari Said, Computer Fraud, doctoral thesis, Legal Informatics and Computer Law, University of Montpellier 1, 1986, p. 266 - 267

⁵ Nader Amran, op. cit., p. 179.

The offender who commits this offence shall be liable to an estimated penalty of one to three years' imprisonment and a fine of 100,000 DA to 300,000 DA.

4- Conclusion

From what has been detailed in this research, which we have devoted to studying irregularities in violation of the procedural provisions for handling personal data, we can draw a set of important findings and recommendations:

- Algerian legislation provides for preventive protection of individuals' right to private life against the dangers of informatics. This is reflected in its criminalization of the act of processing personal data without taking prior formalities. The legislator criminalized this for fear of the dangers of clandestine treatment and the resulting serious damage to individuals' private lives. and that penal protection not only extends to automated treatment but also to non-automated treatment, which demonstrates the legislator's interest in protecting the data of individuals from all attacks, whether caused by automated treatment, which is more serious or by manual processing, albeit less harmful than its predecessor.
- The legislator also attached importance to the will of the person concerned to deal with his personal data that the offence of the handler proceeding with the processing process without obtaining prior consent or resorting to subsequent processing despite their objection. However, ignoring the right to challenge is only a punishable offence if it is based on legitimate grounds and the lawmaker's purpose is to strike a balance between the needs of treatment and the requirements for the protection of the rights of individuals.
- Moreover, the legislator dealing with the need to take the necessary measures to ensure the integrity of the data and its failure to comply with this obligation is a crime. However, the legislator's remuneration is that he commuted the penalty for this offence and only imposed financial penalties, which may cause the processors to tolerate such an obligation .

Recommendations

- Algerian legislation should intensify the punishment for the offence of failure to take safety measures to protect personal data punishable under article 65 of the Algerian Code of Criminal Procedure, by adding penalties for deprivation of liberty as well as financial penalties, in view of the importance of this obligation for the effective protection of personal data.
- The wording of article 56 of the Algerian Code of Criminal Procedure (HMG)

must be adjusted to make it clearer by defining the moral element of the offence of failure to take prior formality and whether criminal intent is required in the offence of failure to take prior formality or whether the offence is based on mere error, which is the best option .

Bibliography List:

Books:

- Osama Abdallah Gaid, *Criminal Protection of Private Life and Information Banks, Comparative Study*, Arab Renaissance House, Cairo, 3rd Edition, 1994, p. 81.
- Vincent Fauchoux, Pierre Deprez, Jean-Michel Bruguière, *Internet Law (laws – contract and usages)*, 2 ed, Lexisnexis, Paris, 2013, p314.
- Alain Bensoussen, *Computer legal guide and freedoms*, François Lefebvre, France, ed 2008, p 15, n° 5.
- Celine Castets Renard, *Internet law*, Montchrestien, Lextenso, France, 2010, p 14.

Journal article:

- Moufida Mibarkia, *Criminal Protection of the Right to Digital Privacy in Algerian Legislation*, *Journal of Shari' a and Economics*, published by the Faculty of Shari' a and Economics, Prince Abdelkader University of Islamic Sciences, Constantine, vol. VII, 1st Edition, 2018, p. p.(481 - 469) .
- Nader Amran, *Protection of Personal Data in the Light of Organic Law No. 63 of 2004 of 27 July 2004*, *Journal of the Judiciary and Legislation*, published by the Centre for Legal and Judicial Studies, Tunisia, No. 8, 46th year, October 2004, p. 177.
- Gérard Haas, Yael Cohen-Hadria, *Legal guide computer and freedoms*, ENI editions, France, October 2012 , p 89.
- Sameh Abdul Wahid Elhami, *Legal Protection of Personal Data, Study in French Law, Section II*, *Law Journal*, Kuwait University, No. 4, 2011, p. 252.

These:

- Jerrari Said, *Computer Fraud*, doctoral thesis, *Legal Informatics and Computer Law*, University of Montpellier 1, 1986, p. 266 – 267
- Aupele Nadine, *Computer-aided Criminal Offences*, doctoral thesis, *Criminal Law*, Faculty of Law and Economics, Montpellier, 1984, p 188.
- Cynthia Chassigneux, *Legal Framework for the Processing of Personal Data on Online Business Sites*, doctoral thesis, *University of Montreal*, Faculty of Law, Private Law, Paris, 2003, p150.

Internet websites:

- Anne Debet, Measurement of diversity and protection of personal data, Report presented to the plenary session, CNIL, 15 May 2007, p. (13-14). Available on the website <https://www.cnil.fr> On 21/08/2024 at 22.00
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EU. Available on the website, <https://eur-lex.europa.eu> , On 16/08/2024 at 23.50.

Legal Texts :

- Law N^o 18/07 of 10 June 2018 on the Protection of Natural Persons in the Processing of Personal Data, OJ No. 34 of 2018.
- Law N^o 16/01 of 6 March 2016 amending the Constitution, No. 14 of 2016.
- Law N^o. 86-09 of 29 July 1986 on the General Population and Housing Statistics, No. 31 of 1986.
- Legislative Decree N^o. 94-01 of 15 January 1994 on the Statistical System, No. 3 of 1994.
- Council of Europe, convention for the protection of individuals with regard to the automated processing of personal data, European Treaties Series n^o 108, Strasbourg, 28 January 1981.
- Council of Europe, Directive 95/46, 24 October 1995 on the protection of individuals and the processing of personal data and the free movement of such data, OJ 1995 L 281, p 31.
- Article 29 Working Group, Opinion 15/2011 on the definition of consent, adopted on 13 July 2011, wp 187, p (12 – 18).