

Digital Personal Data of the E-Consumer under Algerian Legislation: A Comparative Study

Cheddani Nassima¹

Criminal Business Law

University of Colonel Akli Mohand Oulhadj, Bouira

n.cheddani@univ-bouira.dz

Abbes Rima²

PhD Specialization: Law

University of Colonel Akli Mohand Oulhadj, Bouira

r.abbes@univ-bouira.dz

Soumission: 21/03/2026 Acceptation: 25/07/2026 Publication: 09/10/2026

Abstract:

This research paper addresses the issue of digital personal data of the e-consumer under Algerian legislation, considering such data as one of the most important elements related to the protection of consumer privacy in the digital environment. The study aims to clarify the concept of personal data and identify its main forms, particularly data relating to identity, address, banking information, biometric data, and other information that may enable the direct or indirect identification of the consumer.

The study also examines the position of the Algerian legislator regarding the protection of such data, particularly in light of Law No. 18-07 on the Protection of Natural Persons in the Processing of Personal Data, while drawing on certain comparative legal frameworks. The paper further explores the electronic signature as one of the most important forms of digital data and means associated with electronic transactions, as well as the legal issues it raises concerning the verification of the consumer's identity and the protection of their privacy.

Furthermore, the study highlights the main risks threatening personal data, particularly cyberattacks, unauthorized access to files, and the exploitation of data without consent. This underscores the need to establish effective legal safeguards to protect e-consumers and their personal data in light of the continuous development of digital transactions.

Keywords: Personal Data; E-Consumer; Privacy Protection; Electronic Signature; Legal Protection.

Introduction

Over the past decades, the world has witnessed rapid developments in the field of information and communication technologies, which have had a significant impact on various aspects of life, particularly the economic and commercial spheres. The widespread use of the Internet has led to the emergence of new forms of electronic transactions, and consumers have become increasingly engaged with websites and digital platforms to conclude contracts, purchase goods and services, and benefit from various electronic services. This digital transformation has resulted in a growing volume of activities involving the collection, processing, and

storage of information relating to consumers, making personal data one of the most important elements associated with electronic transactions.

Digital personal data is of particular importance due to its nature and the information it contains, which may allow an individual to be identified directly or indirectly, such as identification data, addresses, contact details, and banking information, in addition to biometric data and other information related to an individual's private life. Consequently, the circulation of such data in the electronic environment may constitute a threat to consumer privacy, particularly given the possibility of accessing, exploiting, altering, or transferring such data through unlawful means.

To address these risks, modern legislation has increasingly established legal rules aimed at protecting personal data and ensuring respect for individuals' private lives. The Algerian legislator has followed this approach by establishing a legal framework governing the processing of personal data, particularly through Law No. 18-07 on the Protection of Natural Persons with Regard to the Processing of Personal Data. The legislator has also regulated certain technical and legal mechanisms associated with electronic transactions, including electronic signatures, which have come to play an important role in verifying the identity of the contracting party and establishing their acceptance of electronic documents.

The importance of this issue has increased in light of the growing technological risks threatening the personal data of electronic consumers, particularly cyberattacks, unauthorized access to databases, interception of electronic communications, as well as technical mechanisms that enable the collection of users' data and the tracking of their activities on the Internet. This makes the protection of personal data not merely a technical matter, but rather a legal issue closely connected with protecting consumer privacy and ensuring the security of electronic transactions.

The significance of this study lies in the fact that it sheds light on one of the emerging legal issues arising from digital development. It seeks to define the concept of personal data relating to electronic consumers and identify its main forms, while examining the extent of the protection afforded to such data by the Algerian legislator, with reference to certain comparative legal systems relevant to the subject. The study is also significant in highlighting the risks to which consumers may be exposed as a result of the misuse of their data and in assessing the need to strengthen the legal safeguards capable of protecting their privacy in the digital environment.

Accordingly, the study raises the following main research question:

To what extent has the Algerian legislator succeeded in providing effective legal protection for the digital personal data of electronic consumers in light of the rapid development of electronic transactions?

This main question gives rise to several subsidiary questions, the most important of which are: What is meant by the personal data of electronic consumers? What are its main forms? What legal mechanisms has the Algerian legislator adopted to protect such data? And to what extent is this protection effective in addressing the risks threatening consumer privacy in the digital environment?

To address this research question and the subsidiary questions arising from it, the study adopts the descriptive-analytical approach by defining the relevant legal concepts and

analyzing the legal provisions governing personal data. It also employs the comparative approach in order to draw upon certain comparative legislative experiences and highlight the similarities and differences between those legal systems and Algerian legislation.

Accordingly, this study has been divided into two main sections. The first examines the nature of the consumer's digital personal data, while the second is devoted to examining the legal protection afforded to such data under Algerian legislation, with particular emphasis on the main risks threatening them and the legal and technical means associated with their protection.

Under Algerian legislation, the expression "personal data" appears in Article 5 of Law No. 15-04 and in Article 46 of the 1996 Constitution ¹The same terminology was also used in European Directive 95/46 concerning the protection of individuals with regard to the processing of personal data and the free movement of such data ²By contrast, the French legislature used the term "personal data" pursuant to Law No. 2004-801, amending and supplementing Law No. 78-17 ³thereby following the approach adopted by Council of Europe Convention No. 108 on the protection of individuals ⁴which used the expression "personal data" ⁵

The consumer's digital personal data may be classified into two categories according to the stages of the contractual process: digital personal data disclosed by the electronic consumer before and during the conclusion of the contract (Section One), and the electronic signature, which constitutes a form of digital personal data. However, it has been addressed separately in a distinct section due to the serious consequences that may result from its infringement, given that a signature constitutes an expression of its holder's consent to be bound by the terms of the contract. Interference with or misuse of this personal data not only constitutes an

¹ Presidential Decree No. 96-438 of 7 December 1996, concerning the promulgation of the constitutional amendment approved by referendum on 28 November 1996, Official Gazette No. 76, issued on 8 December 1996, as amended and supplemented. The Algerian legislature has used several terms to designate data relating to individuals. Thus, Law No. 18-07 refers to such data as "personal data," while the expression "personal information" is used in the legislation relating to the placement of workers and employment control. See: Law No. 04-19 of 25 December 2004, concerning the placement of workers and employment control, Official Gazette No. 83, issued on 26 December 2004.

² Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal No. L 281, 23 November 1995, available at: <https://eur-lex.europa.eu/legal-content/FR>.

³ Law No. 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties, available on the website of Légifrance, accessed on 23 November 2020: <http://www.legifrance.gouv.fr>.

⁴ Council of Europe Convention No. 108, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, translated by the European Union in March 2014.

⁵ The French legislature, having previously used the expression "nominal data" in Law No. 78-17, replaced it with the expression "personal data" in accordance with the terminology adopted by Council of Europe Convention No. 108 on the protection of individuals. This represents an expansion of the concept, while also making it more abstract and clearer. The expression "personal data" encompasses all data relating to individuals, rather than merely data concerning their names, and is also sufficiently broad to accommodate future means of identifying individuals. See: Rabia Nassira, "Legal Protection of the Automated Processing of Personal Data: A Comparative Study," *Al-Mouhallil Al-Qanouni Journal*, University of Bouira, Vol. 3, No. 2, December 2021, p. 3.

infringement of the electronic consumer's privacy, but may also, when exploited by third parties, result in the consumer being bound by contracts and subjected to obligations in transactions of which they have no knowledge (Section Two).

Section One: Digital Personal Data Disclosed by the Electronic Consumer Before and During Contracting

Subsection One: Definition of Digital Personal Data in Comparative Legislation

Numerous national and international legal instruments have addressed the definition of personal data. Most legislation has confined the definition of such data to personal information relating to natural persons, rather than legal persons, owing to the particular importance attached to the privacy and protection of natural persons as recognized by national legislation.

Council of Europe Convention No. 108 defined personal data in Article 2(1) as any information relating to an identified or identifiable natural person. This is also the meaning adopted by Article 2(1) of European Directive 95/46, which defines personal data as any information relating to an identified or identifiable natural person (the "data subject"), who may be identified directly or indirectly, in particular by reference to an identification number or to one or more specific elements relating to their physical, physiological, economic, cultural, or social identity.

Article 2 of the Directive on Electronic Signatures, issued on 13 December 1999, also referred to the concept of personal data and defined it as: "any information relating to an identified or identifiable natural person"¹ This is also the same definition adopted by the first Guidelines of the Organisation for Economic Co-operation and Development (OECD) in 1980²

The above-mentioned definitions generally limited the means of identifying a person to "information." Accordingly, anything that does not constitute information cannot serve as a means of identifying a person, such as physical means used by an individual, including a telephone number, vehicle registration number, or any other means used by the person that may serve to identify them³

Conversely, Article 40 of the General Data Protection Regulation (GDPR), applicable to users in the European Union, defined personal information as information relating to an individual whose identity has been established, directly or indirectly, particularly by reference to an identifier such as a name, social security number, location data, or an online identifier, or to one or more factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity⁴

This definition broadened the means by which a person may be identified and did not restrict them to information alone. Furthermore, it referred to certain personal identifiers by way of example and not limitation, as indicated by the expressions "in particular" and "such as." This

¹ Directive on Electronic Signatures, issued on 13 December 1999.

² First Guidelines of the Organisation for Economic Co-operation and Development (OECD), 1980.

³ Mona Al-Ashqar Jabbour and Mohammad Haidar, *Personal Data and Arab Laws: The Security Concern and Individual Rights*, 1st ed., Arab Center for Legal and Judicial Research and the Council of Arab Ministers of Justice, League of Arab States, Beirut, Lebanon, n.d., pp. 75–76.

⁴ Arab Technical News Portal, available at: <https://atnews.com>, accessed on 22 January 2022 at 11:06.

is a commendable expansion, as it leaves room for any information or means that may lead to the identification of an individual.

In the same vein, Article 2 of Moroccan Law No. 08-09 on the Protection of Individuals with Regard to the Processing of Personal Data ¹provides that personal data means any information, regardless of its nature or the means used to obtain it, whether in written form or through audio or visual means, relating to an identified or identifiable natural person.

The Tunisian legislator, for its part, defined personal data in Article 4 of Organic Law No. 63 of 2004as data, regardless of its source or form, that makes a natural person identified or ² identifiable, directly or indirectly, with the exception of information relating to public life or considered as such.

What may be observed regarding the Moroccan and Tunisian legislations is their use of terms that are similar in meaning, although different in wording. The Moroccan legislator refers to them as “data,” whereas the Tunisian legislator refers to them as “information.” However, both legislations have adopted the same approach by providing a broad definition of such data or information rather than limiting it to information that merely identifies a person. Instead, they encompass all data related to an individual across the various aspects of their life ³

The issue of expanding the means of identifying an individual plays a significant role in protecting that person against infringements upon their privacy. This is in contrast to restricting such means, which facilitates the processing of data without effective oversight, due to the inability to apply the relevant legal provision, thereby indirectly excluding such data from its scope.

Subsection Two: Definition of Digital Personal Data in Algerian Legislation

Although Law No. 18-05 on Electronic Commerce regulates the obligation to protect personal data in several provisions, it does not provide a definition of such data, thereby referring the matter to the legislation in force. Likewise, the Penal Code, which addresses crimes involving interference with automated data-processing systems in its seventh bis section, does not define such data. This situation constituted a legislative gap ⁴that remained unaddressed until the enactment of Law No. 18-07 on the Protection of Natural Persons in the Processing of Personal Data. Article 3, paragraph 1, of this law expressly defines personal data as any information, regardless of its medium, relating to an identified or identifiable person, who is referred to therein as the “data subject.”

Such identification may be carried out directly or indirectly, particularly by reference to an identification number or to one or more elements relating to the identity of that person,

¹ Law No. 08-09 on the Protection of Individuals with Regard to the Processing of Personal Data, Official Gazette, No. 5711, issued on 23 February 2009, p. 52.

² Law No. 63 of 2004, dated 27 July, on the Protection of Personal Data, Official Gazette of the Republic of Tunisia, No. 61, issued on 30 July 2004.

³ Nesrine Ghazal, “Protection of Natural Persons in the Field of Personal Data,” Algerian Journal of Legal and Political Sciences, University Center of Tipaza, Vol. 56, No. 1, 2019, p. 114.

⁴ We describe this situation as a legislative gap in light of recent trends in legislation, as the majority of modern legal systems tend to include definitions of numerous legal terms within their legislative provisions.

including their physical, physiological, genetic, biometric, psychological, economic, cultural, or social identity ¹

An analysis of the provisions of this text leads to the following observations:

1- The provision is formulated in general terms, as evidenced by the expression “any information.” The term “in particular,” on the other hand, is used by way of example rather than limitation. Accordingly, the Algerian legislator has followed the approach adopted by legislations that provide an extensive definition of personal data ²Pursuant to this provision, the protection of personal data encompasses all data relating to the electronic consumer, as a natural person, which is provided to the electronic supplier within the framework of an electronic commerce contract. Such data may consist of identifying information relating to the person, including their first and last name, postal or electronic address, personal photograph, place of residence, and place of employment; or other information that does not constitute identifying data in itself but is nevertheless associated with the consumer, such as banking information, including a bank account number, biometric data, and other data relating to the consumer ³This broad approach is commendable, since, as previously indicated, a restrictive definition of data may allow numerous entities to infringe upon such data.

1- It is clear from the wording of the article that the data subject to legal protection concern natural persons rather than legal persons. This is evident from the expressions used in the article: “... through certain elements that distinguish them and relate to their physical, physiological, genetic, biometric, psychological, cultural, or social identity...”. These elements concern natural persons rather than legal persons. Furthermore, Law No. 18-07 on the protection of personal data was enacted under the title “Law on the Protection of Natural Persons in the Processing of Personal Data.”

This implies that the protection of public or private legal persons does not fall within the scope of this law. However, it should be noted in this regard by reference to Article 3, Paragraph 4 of the same law that it provides that the consent of the data subject to the processing of his or her personal data may be given either directly by that person or by his or her legal representative. Since the law allows a natural person to have a legal representative in certain circumstances, such as when the data subject lacks legal capacity or has limited capacity, a legal person may likewise express its will through its legal representative. Accordingly, legal protection may also extend to its personal data relating to its commercial and economic activities, as such data merits protection of its confidentiality.

Section Two: Electronic Signature as Digital Data Relating to the Electronic Consumer

An electronic contract, like a traditional contract, needs to bear the signatures of the parties in order to be binding upon them. However, the specific nature of such a contract, resulting from the digital environment in which it is concluded, has rendered the traditional forms of signature (handwritten signature, seal, and fingerprint) unsuitable for this purpose. This has

¹ The same article, in its second paragraph, defines the “data subject” as: “Any natural person whose personal data is the subject of processing.”

² Mofid Mabroukia, “Criminal Protection of Digital Privacy under Algerian Law,” Journal of Sharia and Economics, Faculty of Sharia and Economics, University of Constantine, No. 13, June 2019, p. 463.

³ See Article 3, paragraphs 1 and 6, of Law No. 18-07.

led to the emergence of an electronic alternative to the traditional signature, namely the electronic signature.

Subsection One: Definition of the Electronic Signature

The purpose of introducing the electronic signature is to perform the functions of the traditional signature within the digital environment. The latter has characteristics that distinguish it from the physical environment, and these specificities have also influenced the electronic signature, which has acquired its own definition (first) and specific forms (second).

First: Definition of the Electronic Signature between the Functional and Technical Approaches

Both legal scholarship (1) and legislation (2) have defined the electronic signature, and the definitions have varied according to the perspective from which this signature is considered.

1- The Doctrinal Definition of the Electronic Signature:

Legal scholarship has adopted two approaches to defining the electronic signature. The first defines the electronic signature on the basis of its functional aspect, considering it to be a set of letters, numbers, symbols, or signs possessing a distinctive character, which makes it possible to identify the person who owns the signature and distinguish that person from others. It constitutes an essential means of electronic transactions in the processes of conclusion and performance, as well as in maintaining the confidentiality of information and messages.¹ This definition approaches the electronic signature in terms of the function it performs, which is the same function as that of the traditional signature, although it relates specifically to electronic transactions.²

The second approach, on the other hand, defined the electronic signature in terms of the means through which such a signature is created, considering it as a set of procedures and means whereby symbols and numbers are used to generate an electronic message containing a distinctive mark identifying the sender of the electronically transmitted message. Unlike the first definition, this definition therefore focuses on the procedures through which the signature is created.

Based on the foregoing, it is clear that an electronic signature consists of two aspects: the means used to create the signature and the function performed through it. Accordingly, an accurate definition of the electronic signature requires combining these two aspects.

From this perspective, the electronic signature has been defined as a set of information inserted into, added to, or logically associated with a data message in electronic form, which is used to identify the signatory, demonstrate the signatory's consent to the contents of the message, and confirm its integrity.³ In other words, for a signature to be considered electronic,

¹ SAMBATH Hel, *Le formalisme du contrat électronique dans L'ASEAN: Définition et interprétation des notions d'écrit et de signature*, Thesis submitted to the Faculty of Graduate Studies in partial fulfillment of the requirements for the degree of Doctor of Law, Faculty of Law, University of Montreal, May 2013, p. 20.

² In the same vein, the electronic signature has been defined as a set of technical procedures that make it possible to identify the person who carried out such procedures and to establish his or her acceptance of the content of the legal act in connection with which the signature was made.

³ Sharaf al-Din Ahmed, *Electronic Signature, Rules of Evidence, and Security Requirements in Electronic Commerce*, paper presented at the Conference on Electronic Commerce held at the League of Arab States, Egypt, 2000, p. 3.

the relevant data must necessarily be incorporated in electronic form, while the functions that the electronic signature must perform are also specified. This definition is distinguished by combining both the functional and technical aspects of the electronic signature.

2. Legislative Definition of the Electronic Signature

International organizations, as well as domestic legislation, have addressed the definition of the electronic signature, considering it a mechanism used to conclude legal transactions in the electronic environment.

At the international legislative level, the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Signatures ¹defines an electronic signature in Article 2 as follows: “Data in electronic form in, affixed to, or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory’s approval of the information contained in the data message.”

It can be inferred from this provision that the Model Law does not prescribe a specific method for creating an electronic signature. It may therefore take any form, allowing it to accommodate any new form or method of electronic signature that may emerge in the future. However, it requires the method used to perform the functions of a signature, namely identifying the signatory and indicating the signatory’s approval of the information contained in the contract. This is further confirmed by Article 3 of the Model Law ²

The European Regulation No. 910/2014, issued by the European Parliament on 23 July 2014 concerning electronic identification and trust services for electronic transactions within the internal market ³defined the electronic signature in Article 3(10) as: “data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.” The same Article, in paragraph 11, introduced a new type of signature, namely the advanced electronic signature, with reference to Article 26 of the same Regulation, defining it as a signature that meets the requirements set forth in Article 26. The latter provision establishes a number of conditions that an electronic signature must satisfy in order to qualify as an advanced electronic signature. These conditions clearly appear to have been established with the aim of enhancing the security of electronic signatures⁴

With regard to domestic legislation, the Tunisian legislator, although being among the first Arab legislators to enact legislation regulating electronic signatures and electronic commerce in 2000, did not provide a definition of the electronic signature and merely regulated its legal

¹ Tawakkal Fadi Imad al-Din, *The Legal Regulation of Certification Authorities*, cited in: Alaa Ahmed Mohammed Haj Ali, op. cit., p. 36.

² This Model Law was adopted in 2001 and consists of twelve articles addressing various aspects of electronic signatures, including their definition and validity requirements, with the aim of serving as a model for different states when enacting their own legislation on electronic signatures. Available at: www.uncitral.org.

³ Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

⁴ Article 26 sets forth a number of requirements for a signature to qualify as an advanced electronic signature, namely: that it be uniquely linked to the signatory and capable of identifying the signatory; that it be created using electronic signature creation data that the signatory can use with a high level of confidence under his or her sole control; and that it be linked to the data associated with the signature in such a way that any subsequent change to the data can be detected.

framework. In contrast, the Egyptian legislator defined the electronic signature in Article 1 of the Egyptian Electronic Signature Law¹ as: “that which is placed on an electronic document and takes the form of letters, numbers, symbols, signs, or otherwise, and which has a unique character allowing the identification of the signatory and distinguishing him or her from others.” It may be noted that the Egyptian legislator’s definition combines both the technical and functional aspects of the electronic signature. However, this definition may be criticized for referring to only one of the functions of the electronic signature, namely identifying the signatory and distinguishing him or her from others, while overlooking another function that is no less important.

This shortcoming was addressed by the UAE legislator in Article 1 of Federal Decree-Law No. 46 of 2021 on Electronic Transactions and Trust Services, which defined an electronic signature as a signature consisting of letters, numbers, symbols, sounds, fingerprints, or a processing system in electronic form, attached to or logically associated with an electronic document, and capable of verifying the identity of the signatory and his or her acceptance of the content of the associated data.

As for the Algerian legislator, the electronic signature was defined in Executive Decree No. 07-162, amending and supplementing Executive Decree No. 01-123 concerning the operating regime applicable to each type of network. Article 3 bis 1 defines the electronic signature as: “...data resulting from the use of a method that meets the conditions laid down in Articles 323 bis and 323 bis 1 of Ordinance No. 75-58 of 20 Ramadan 1395, corresponding to 26 September 1975, referred to above.” This definition may be regarded as ambiguous, since it defines the electronic signature by reference to the conditions that it must satisfy, thereby referring to the requirements established under the Civil Code²

With the enactment of Law No. 15-04 on electronic signatures and electronic certification, the Algerian legislator clarified the matter by defining an electronic signature in Article 2, Paragraph 1 thereof as data in electronic form that is attached to, or logically associated with, other electronic data and is used for authentication purposes. Article 6 of the same Law further provides that an electronic signature is used to authenticate the identity of the signatory and to demonstrate his or her acceptance of the content of the document in electronic form.

Accordingly, the Algerian legislator has also combined the technical and functional approaches in defining the electronic signature. However, it did not provide detailed specifications concerning its technical aspect, thereby leaving the field open to any newly developed means of electronic signature. This approach adopted by the legislator is appropriate, as it is necessary to adopt a broad definition of the electronic signature. It cannot

¹ This was provided for in point (c) of Article 1 of Law No. 15 of 2004 regulating electronic signatures and establishing the Information Technology Industry Development Authority, dated 21 April 2004, Official Gazette No. 17 (Supplement D), issued on 22 April 2004.

² The first recognition by the Algerian legislator of the electronic signature was through Article 327(2) of the Civil Code, which provides that: “...an electronic signature shall be recognized in accordance with the conditions referred to in Article 323 bis 1 above.” Article 323 bis 1 further provides that: “Evidence in writing in electronic form shall have the same evidentiary value as evidence in writing on paper, provided that it is possible to verify the identity of the person who issued it and that it is created and retained under conditions ensuring its integrity.”

be confined to a specific form, particularly in light of the remarkable technological developments taking place in the field of technology. Therefore, the definition must be sufficiently comprehensive to encompass any new form that may emerge, provided that it is capable of fulfilling the functions of an electronic signature.

It can be inferred from the aforementioned legislative definitions that they are relatively similar, which may be attributed to their reliance on the same legislative source, namely the UNCITRAL Model Law.

These legislations are noteworthy for having emphasized the importance of recognizing electronic signatures, as well as broadening their concept, in order to keep pace with all the new types and forms of electronic signatures generated by scientific and technological advancement.

B – Forms of Electronic Signatures:

Based on the foregoing discussion concerning the definition of the electronic signature, it appears that neither national nor international legislation has specified particular forms that an electronic signature must take. Rather, they have left the matter open to the technological and scientific developments that may arise in this field.

In light of technological developments, it can be observed that an electronic signature does not take a single form. Rather, its forms vary according to the technology used to create it. Each technology has its own operating system, which differs from the others. Nevertheless, what they have in common is that they rely on electronic media and employ technologies capable of transforming the distinctive characteristics of an individual, as well as numbers and letters, into data that can be uniquely used by its holder for the purpose of signing documents and carrying out electronic transactions ¹

1 – Biometric Signature

In a biometric signature system, the identity of the person carrying out the transaction is verified through physical characteristics, such as an eye scan (iris or eye biometric), a fingerprint, a lip print, voice characteristics, hand movements, and so forth. One of these characteristics is stored in encrypted form in the computer's memory, enabling the computer to perform a matching process when the signature is made.

What distinguishes this type of signature is its reliance on the intrinsic characteristics of an individual, which cannot be identical to those of another person. This makes it a reliable means of distinguishing and identifying an individual. In addition, it does not rely on secret keys, thereby avoiding the loss or theft of passwords or confidential identification numbers.

However, these considerations do not prevent such a signature from being subject to forgery, particularly where the voiceprint of a specific person is recorded and subsequently replayed on a file other than the one on which the person originally signed. Furthermore, this type of electronic signature is vulnerable to changes in the intrinsic characteristics of the individual over time, such as changes in the tone of the voice, for example.

¹ Zakaria Massoudi and Djegrief Zahra, "Electronic Signature and Its Protection of Electronic Payment," International Journal of Legal and Political Research, El Oued University, Vol. 1, No. 03, December 2017, p. 161.

With regard to Algerian legislation, it appears that the legislator implicitly referred to this type of signature in Article 543 of the Commercial Code, which provides: “Payment cards are considered to be any card issued by banks and ... allowing its holder to withdraw or transfer funds. Withdrawal cards are considered to be any card issued by banks and ... allowing its holder only to withdraw funds.” Thus, the provision distinguishes between two types of cards: a payment card, which its holder may use to withdraw or transfer funds, and a withdrawal card, whose function is limited to withdrawing funds. Both cards incorporate an electronic signature and are issued by banks and duly authorized financial institutions ¹

2. Digital Signature (Signature numérique) ²

A digital signature consists of a set of data, symbols, and mathematical algorithms that are encrypted and attached to an electronic message or document by means of specialized software. This software converts the electronic message or document into an unintelligible form.

The International Organization for Standardization (ISO), in its standard concerning security architecture for Open Systems, ISO 7498-2:1989, defined a digital signature as data appended to a data unit, or a cryptographic transformation of a data unit, enabling the recipient to prove the source and integrity of the data unit and protecting it against forgery or alteration ³

The United Nations Commission on International Trade Law (UNCITRAL), in a document dated 31 December 1996 ⁴ defined it as follows: “A numerical value affixed to a data message which, by means of a mathematical procedure associated with the private cryptographic key of the message originator, enables the recipient to determine that such numerical value was obtained using the private cryptographic key of the message originator and no other key. The mathematical procedures used to generate digital signatures under these rules are based on public-key cryptography. When such mathematical procedures are applied to a data message, they produce a transformation of the message enabling a person who possesses the original message and the originator’s public cryptographic key to determine with certainty:

(a) Whether the transformation was performed using the private cryptographic key corresponding to the originator’s public key; and

¹ The Algerian legislator has also employed this type of signature in the issuance of biometric passports and biometric national identity cards, pursuant to the Order dated 19 July 2010 concerning the application file for biometric electronic national identity cards and passports and the procedures for processing such applications, Official Gazette No. 45, issued on 8 August 2010.

The same applies to biometric driving licences, pursuant to Law No. 17-05 of 16 February 2017, amending and supplementing Law No. 01-14 concerning the organization, safety, and security of road traffic, Official Gazette No. 22, issued on 22 February 2017.

² The term “digital signature” derives from the fact that the message, after the application of encryption techniques, appears in the form of numbers; hence, it is referred to as a cryptographic-based digital signature.

³ “3.3.26 Digital signature: Data appended to a data unit, or cryptographic transformation (see cryptography) of a data unit, allowing a recipient to prove the source and integrity of the data unit and protecting against forgery (by the recipient, for example).” ISO 7498-2:1989 (fr).

Available at: <https://www.iso.org/obp/ui/#iso:std:iso:7498:-2:ed-1:v1:fr>. Accessed on 22 July 2023 at 1:03.

⁴ Document No. 7/CN.9/WG.IV/WP.71, dated 31 December 1996, v.55. Available in Arabic on the following website: <http://document-dd.snv.org/undoc/ltd/v96/885/25pdf/v9688525.pdf/openElement>.

(b) Whether the original message has been altered after the transformation was performed”¹

Based on the foregoing definitions, it may be stated that a digital signature is a form of signature based on mathematical algorithms. These algorithms are characterized by their technical complexity and generate what is known as an electronic fingerprint, which is unique and distinguishable from other fingerprints. This enables the digital signature to provide a high level of security and confidentiality sought by contracting parties when conducting electronic transactions², particularly in sensitive fields such as the banking sector. Nevertheless, the digital signature remains vulnerable to the risk of impersonation, whereby another person may assume the identity of the sender after obtaining the relevant cryptographic keys, using them, and subsequently attributing the resulting signature to the legitimate holder.

3. Code-Based Signature

This type of signature is also referred to as a signature using electronic payment cards³ It is based on the use of either letters, numbers, or a combination of both, selected by the signatory for the purpose of identifying his or her identity and personality. These take the form of a specific code⁴ known only to the signatory or to the person to whom it has been communicated. It operates by matching the number obtained by the signatory with a secret number previously stored in the memory of the computer used for the service or stored in the electronic banking system. If the two numbers correspond, the signature is considered completely valid.

There are several types of magnetic cards. For example, there are cash withdrawal cards, which are used to withdraw cash from a person's account⁵ and payment cards, through which the cardholder pays for purchases or services by means of specially designed payment terminals.

There is also another type of card known as a credit card. The latter grants its holder the right to obtain a credit facility from the bank that issued it. The bank pays for the goods and services obtained by the cardholder and subsequently grants the cardholder a period within

¹The confidentiality of information is ensured by preventing anyone other than the intended recipient from reading the electronic document, since the recipient is the only person possessing the mathematical keys used for encryption. Security, on the other hand, means that the signatory cannot deny having signed the message in question, as it is attributable to the signatory.

² Also known as magnetic cards associated with a secret number, they are also referred to as payment or bank cards. They are rectangular in shape, made of plastic, and bear the name and logo of the issuing institution, as well as the cardholder's signature prominently displayed on the front of the card, together with its number, the cardholder's name and account number, and the expiry date. They are issued by banks. Their use does not require any particular expertise, nor does it require the user to own a computer or have access to the Internet. See: Abbas Al-Aboudi, Challenges of Proof by Electronic Documents and the Requirements of the Legal System to Overcome Them, Al-Halabi Legal Publications, Beirut, Lebanon, 1st ed., 2010, p. 153.

³ It is abbreviated as PIN, which stands for Personal Identification Number.

⁴ Aisha Qassar Al-Layl, The Evidentiary Value of Electronic Documents and Electronic Signatures in Proof: An Analytical Comparative Study, PhD Dissertation in Legal Sciences, Faculty of Law and Political Science, University of Hadj Lakhdar, Batna, 2016–2017, p. 103.

⁵ Iman Mamoun Ahmed Suleiman, Conclusion and Proof of Electronic Contracts, Dar Al-Jamia Al-Jadida for Publishing, Alexandria, 2008, p. 202.

which to repay the amount. If repayment is not made within the specified period, high interest rates are imposed. Hence, these cards are known as credit cards ¹

The secret number contained in the code-based signature is regarded as an alternative to the handwritten signature ²It provides a high degree of security and reliability, since its use is associated with a secret number that can only be provided to the customer. In the event that the card is lost or stolen, or the secret number is forgotten, the cardholder may deactivate its validity simply by notifying the bank, thereby preventing third parties from using the card or benefiting from it.

4. Electronic Pen Signature (Pen-Op)

In an electronic pen signature, the handwritten signature is transferred to a computer by means of an electronic pen. The signature is then stored inside the computer on an electronic medium. An image of this signature can subsequently be transferred to a file in order to sign it and use it in connection with a commercial contract concluded over the Internet.

This type of signature is widely used by security and intelligence agencies for the purpose of identifying individuals ³particularly because the validity of the signature is verified each time through a dedicated electronic software program It also provides a high degree of security, since, even if the cards and secret numbers are stolen, it is difficult for the thief to imitate the movements involved in producing the signature ⁴

However, this type of signature faces several difficulties. It requires a high-quality computer equipped with specialized software capable of reading the electronic pen signature and comparing it with the signature previously stored. Moreover, it is relatively easy to transfer a person's signature using a scanner and place it on another document, without being able to verify whether the actual holder of the signature was the person who affixed it to that document.

The aforementioned forms of electronic signature give rise to the following observations:

Electronic signatures, in all their forms, demonstrate that the fundamental difference between electronic and traditional signatures lies in the medium or support on which the signature is affixed. A traditional signature is made on a paper-based medium, whereas an electronic signature is created through an automated medium using computer systems over the Internet. This gives rise to multiple forms of electronic signatures, which may be incorporated electronically in optical or digital form, whereas the traditional signature generally appears in a single form, namely the handwritten signature.

Although all the aforementioned forms of electronic signature are carried out through electronic media, the technologies used in each form differ. Consequently, each technology has a particular level of security and reliability, which in turn affects the legal value attributed to each form of electronic signature.

¹ Ayman Abdullah Fikri, *Cybercrimes: A Comparative Study of Arab and Foreign Legislation*, Law and Economics Library, Riyadh, Saudi Arabia, 1st ed., 2015, p. 373.

² Najwa Abu Haiba, *Electronic Signature*, Dar Al-Nahda Al-Arabiya, Egypt, 2002, p. 42.

³ Suhaila Tamine, *Formal Requirements in Electronic Commerce Contracts*, Master's Thesis, International Business Law, Faculty of Law and Political Science, Mouloud Mammeri University, Tizi Ouzou, 2011, p. 53.

⁴ Lawrence Mohammed Obeidat, *Proof of Electronic Documents*, 1st ed., Dar Al-Thaqafa for Publishing and Distribution, Amman, 2009, p. 95.

Conclusion

In conclusion, this study has demonstrated that consumers' personal digital data have become one of the most significant elements shaping the digital environment, given their direct connection to consumers' identities, private lives, and electronic transactions. The study has concluded that the concept of personal data is no longer limited to traditional information relating to names, addresses, and means of communication; rather, it has come to encompass various types of information that may enable a person to be identified or recognized, either directly or indirectly, including banking and biometric data, as well as other data associated with the individual's online activities. The study has also shown that the Algerian legislator has sought to establish a legal framework for the protection of such data, particularly through Law No. 18-07 on the Protection of Natural Persons in the Processing of Personal Data, in addition to regulating electronic signatures as one of the important means used in electronic transactions, given their role in verifying the identity of the signatory and establishing their acceptance of the electronic document.

The study further revealed that technological development, despite the considerable facilities it has provided to consumers and electronic transacting parties, has simultaneously created a range of risks that may compromise consumers' privacy and the security of their data. These risks include, most notably, cyberattacks, unauthorized access to databases, interception of electronic communications, and the exploitation of personal data without the knowledge or consent of the data subject, in addition to technical means that enable the collection and tracking of users' information. The seriousness of these practices is further increased by the difficulty of recovering stolen data or correcting it once it has been disseminated, as well as by the material and moral harm that may consequently be suffered by consumers. Therefore, the protection of personal data should not be limited merely to the existence of legal provisions; rather, it requires effective and enforceable safeguards capable of keeping pace with the rapid developments in technology and electronic transactions.

In light of these findings, the study recommends the continued development of the Algerian legal framework governing the protection of personal data in a manner consistent with the ongoing evolution of digital technologies. It also recommends strengthening mechanisms for monitoring the collection, processing, and storage of consumers' data, while imposing stricter liability and sanctions for the unlawful use of such data. Furthermore, it is necessary to strengthen the technical and security measures adopted by institutions and entities responsible for processing data in order to reduce the risks of breaches and unauthorized access, and to enhance the security of electronic transactions. On the other hand, the importance of promoting legal and digital literacy among electronic consumers should be emphasized by informing them of their rights concerning their personal data and the means of protecting such data, as well as raising their awareness of the risks associated with sharing their information through electronic platforms and websites. It is also advisable to strengthen cooperation among the various competent authorities and facilitate the exchange of expertise in the fields of data protection and digital security. Such measures would contribute to achieving a balance between promoting electronic commerce and benefiting from technological development, on the one hand, and ensuring the protection of consumers' privacy and data security, on the

other, thereby contributing to a safer, more trustworthy, and more stable electronic environment.

List of Sources and References

Books

Iman Mamoun Ahmed Suleiman, *Conclusion and Proof of the Electronic Contract*, Dar Al-Jamiaa Al-Jadida for Publishing, Alexandria, 2008.

Ayman Abdullah Fikri, *Cybercrimes: A Comparative Study of Arab and Foreign Legislation*, Law and Economics Library, Riyadh, Saudi Arabia, 1st ed., 2015.

Abbas Al-Aboudi, *Challenges of Proving Evidence through Electronic Documents and the Requirements of the Legal System to Overcome Them*, Al-Halabi Legal Publications, Beirut, Lebanon, 1st ed., 2010.

Lawrence Mohammad Obeidat, *Proof of the Electronic Document*, 1st ed., Dar Al-Thaqafa for Publishing and Distribution, Amman, 2009.

Mohammad Hussein Mansour, *Electronic Liability*, Mansha'at Al-Maaref, Alexandria, Egypt, 2006.

Mona Al-Ashqar Jabbour and Mohammad Haidar, *Personal Data and Arab Laws: Security Concerns and Individual Rights*, 1st ed., Arab Center for Legal and Judicial Research and the Council of Arab Ministers of Justice, League of Arab States, Beirut, Lebanon, 1st ed., n.d.

Najwa Abu Haiba, *Electronic Signature*, Dar Al-Nahda Al-Arabiya, Egypt, 2002, p. 42.

Theses and University Dissertations

A. Doctoral Theses

Aisha Qassar Al-Lail, *The Evidentiary Value of the Electronic Document and Electronic Signature: An Analytical Comparative Study*, Doctoral Dissertation in Legal Sciences, Faculty of Law and Political Sciences, University of Batna, Batna, 2016–2017.

B. Master's Theses and Dissertations

Souheila Tamine, *Formal Requirements in Electronic Commerce Contracts*, Master's Dissertation, International Business Law Branch, Faculty of Law and Political Sciences, Mouloud Mammeri University, Tizi Ouzou, 2011.

Scientific Articles

Rabia Nassira, "Legal Protection of the Automated Processing of Personal Data: A Comparative Study," *Al-Muhallil Al-Qanouni Journal*, University of Bouira, Vol. 3, No. 2, December 2021.

Zakaria Massoudi and Djegrief Zahra, "Electronic Signature and Its Protection of Electronic Payment," *International Journal of Legal and Political Research*, University of El Oued, Vol. 1, No. 3, December 2017.

Ghazal Nesrine, "Protection of Natural Persons in the Field of Personal Data," *Algerian Journal of Legal and Political Sciences*, University Center of Tipaza, Vol. 56, No. 1, 2019.

Mofid Mabroukia, "Criminal Protection of Digital Privacy under Algerian Law," *Journal of Sharia and Economics*, Faculty of Sharia and Economics, University of Constantine, No. 13, June 2019.

Legal Texts

A. National Legal Texts

Presidential Decree No. 96-438 of 7 December 1996, concerning the promulgation of the constitutional amendment approved by referendum on 28 November 1996, Official Gazette, No. 76, issued on 8 December 1996, as amended and supplemented.

Law No. 04-19 of 25 December 2004, concerning the placement of workers and employment control, Official Gazette, No. 83, issued on 26 December 2004.

Law No. 17-05 of 16 February 2017, amending and supplementing Law No. 01-14 concerning the organization, safety, and security of road traffic, Official Gazette, No. 22, issued on 22 February 2017.

Law No. 08-09 concerning the protection of natural persons with regard to the processing of personal data, Official Gazette, No. 11, issued on 23 February.

Decision of 19 July 2010, concerning the application file for the national identity card and electronic biometric passport and the procedures for processing such applications, Official Gazette, No. 45, issued on 8 August 2010.

B. Foreign Legal Texts

European Union Directive, European Treaty Series No. 108, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, translated by the European Union in March 2014.

Law No. 63 of 2004, dated 27 July 2004, concerning the protection of personal data, Official Gazette of the Tunisian Republic, No. 61, issued on 30 July 2004.

Law No. 15 of 2004 regulating electronic signatures and establishing the Technology Industry Development Authority, dated 21 April 2004, Official Gazette, No. 17 (Supplement D), issued on 22 April 2004.

SAMBATH Hel, The Formalities of Electronic Contracts in ASEAN: Definition and Interpretation of the Concepts of Writing and Signature, PhD Thesis submitted to the Faculty of Graduate Studies in fulfillment of the requirements for the degree of Doctor of Law, Faculty of Law, University of Montreal, May 2013.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal No. L 281, 23 November 1995, available at: <https://eur-lex.europa.eu/legal-content/FR>.

Law No. 78-17 of 6 January 1978, relating to information technology, files and freedoms, consulted on 23 November 2020, available at: <http://www.legifrance.gouv.fr>.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal No. L 281, 23 November 1995, available at: <https://eur-lex.europa.eu/legal-content/FR>.

Law No. 78-17 of 6 January 1978, relating to information technology, files and freedoms, consulted on 23 November 2020, available at: <http://www.legifrance.gouv.fr>.

Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Electronic Websites:

<http://www.cert.gov.om/library/information-glossary-arabi> www.unictr.org