Kurdish Studies
March 2025
Volume: 13, No: 1, pp 103-112
ISSN: 2051-4883 (Print) | ISSN 2051-4891 (Online)
www.KurdishStudies.net

DOI: 10.53555/ks.v13i1.3764

Protection Of Personal Data Of E-Consumers In Algerian Legislation

Benrejdal Amel[1*], Kasmi Belkacem[2]

[1*]University of Algiers 1, Email: a.benrejdal@univ-alger.dz
[2]ENSJSI, Email: belkacemkasmi@gmail.com

Abstract :
This study examines the protection of e-consumers' personal data in Algerian legislation, given the increasing importance of e-commerce and its associated risks. The article focuses on the legal framework governing consumer data protection, highlighting key laws such as Law 18-05 on e-commerce and Law 18-07 on personal data protection.
It also discusses the role of cybersecurity, encryption, and electronic signatures as technical measures to safeguard personal data. Despite legislative efforts, challenges remain in enforcement and technological adaptation. The article concludes by emphasizing the need for stronger legal oversight, improved digital protection tools, and increased consumer awareness to ensure a secure and fair electronic environment.

Key Words : Personal Data, E-Consumers, Degital Protection, Electronic Certification, Technical protection, Cybersecutrity.

I.Introduction

E-commerce has experienced significant growth since 1999, the year when the *Organisation for Economic Co-operation and Development* (OECD) adopted its first international instrument for consumer protection in e-commerce, later known as the 1999 Recommendation. On March 24, 2016, the OECD Council revised this instrument and adopted a new recommendation on consumer protection in e-commerce, addressing emerging trends and challenges faced by consumers in the dynamic digital marketplace.
This development resulted from efforts made during the 1998 OECD Ministerial Conference, held under the theme *"A Borderless World: Realizing the Potential of Global Electronic Commerce."* The conference led to the adoption of the 1999 Recommendation on the Core Principles of Consumer Protection in E-Commerce, which include:

- Fairness and transparency in commercial and advertising practices
- Providing information about businesses, products, services, and transactions
- Effective dispute resolution and compensation mechanisms,
- Payment Security
- Privacy protection and consumer awareness

In response to the ministers' call during the 2008 Ministerial Meeting on the Future of the Internet Economy, the Organisation for Economic Co-operation and Development (OECD) reassessed the 1999 Recommendation to explore ways to enhance consumer benefits from the opportunities provided by e-commerce.
In this context, during the "*Empowered and Protected Consumers in the Internet Economy*" conference held in Washington in 2009, the OECD *Consumer Policy Committee* (CPC) conducted studies and analyses on policy trends and challenges related to: Mobile and online payments, The purchase of intangible digital content, and Collaborative e-commerce.
Given the rapid development of e-commerce, privacy protection has become a critical issue for many online businesses. With the increasing number of data breaches, rising consumer awareness, and the imposition of fines for non-compliance, safeguarding customer data, and respecting privacy have become new market standards.[1]
According to *The Economist*, customer data is now considered the most valuable business asset in the world. This is unsurprising, as properly utilized data can help businesses better understand their customers and develop effective digital marketing strategies that enable them to promote products and services in a more targeted manner.[2]
Privacy protection remains a fundamental issue in e-commerce worldwide. Numerous studies and reports in the United States, for example, highlight its importance. A study conducted by *PricewaterhouseCoopers* (PwC) found that approximately two-thirds of surveyed consumers stated they would engage more in online transactions if they trusted that commercial websites would not use their personal information for other purposes.

[1] A study conducted by Cisco in 2021 showed that 79% of consumers consider privacy respect as a factor influencing their purchase. See CISCO SCURE, Building Consumer Confidence Through Transparency and Control, available at: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf?CCID=cc000742&DTID=esootr000875&OID=rptsc027438

[2] See Sara Jabbari (2022), The Protection of Customers' Privacy in Digital Marketing: Everything You Need to Know!, WIDEA, available at: https://www.wedia-group.com/fr/blog/respect-de-la-vie-privee-du-consommateur-dans-le-marketing-digital-tout-ce-quil-faut-savoir-fr

In the same year, a study by the U.S. *Federal Trade Commission* (FTC) reported that 67% of consumers were highly concerned about the protection of their personal data transmitted online.[3] Similarly, a 2005 *CBS News survey* revealed that most Americans viewed their privacy as being seriously threatened.[4]

In a more recent study conducted by Turow et al., findings showed that most Americans reject targeted advertising due to privacy concerns.[5]

The significance of this issue is evident in the economic, technological, and regulatory context in which businesses operate today, as well as in the lack of well-established knowledge on the subject. There remains ambiguity regarding what individuals consider personal information and in what circumstances data processing is perceived as a violation of their privacy.

Additionally, there is a lack of information on how individuals make decisions regarding sharing their personal data, whether they consent to its collection, use, or transfer to third parties.

As consumer concerns about privacy continue to grow, as confirmed by several recent surveys,[6] and businesses increasingly strive to gain deeper insights into their customers, it has become essential—within the era of the "privacy economy"[7]—to establish clear conditions for a balanced approach between these two interests.

II.Privacy and Personal Data of the E-Consumer: What is the Concept?

It is important to note that consumers' personal data falls under what is known as "informational privacy,"[8] referring to private data stored on electronic devices or the internet. This data goes by various names, such as "private data," "informational privacy," or "nominal information," all of which refer to the concept of an individual's right over their personal information.

This includes data related to their personal identity, such as name, personal photo, date and place of birth, gender, and place of residence, as well as health-related information stored in medical files prepared by hospitals. These files contain various personal details about the patient, such as name, gender, date and place of birth, symptoms, treatment history, etc., all of which are considered personal.

It is agreed that the first article on privacy was published in the American *Harvard* magazine in 1890 by *Samuel Warren and Louis Brandeis*, where they defined the right to privacy as *"the right to be let alone."* Since then, other definitions have emerged to complement this concept, yet no real consensus has been reached on its precise meaning. Some definitions focus on the concept of confidentiality, while others highlight privacy as being in contrast with public and/or professional life.

Notably, privacy issues have remained fundamentally similar over time.[9] This is evident in the fact that the legal discussions surrounding privacy in 1890 and today share a common thread—the publication of personal information continues to pose both legal and ethical dilemmas.[10] However, the key difference lies in modern technology's ability to collect, store, and analyze vast amounts of data in ways that may threaten privacy—even when the information appears to be publicly available.[11]

What *Samuel Warren* and *Louis Brandeis* pointed out in 1890 remains profoundly relevant today—every technological advancement brings new challenges to privacy. With technology evolving at an unprecedented pace, it has become essential to continuously rethink how the law can adapt to these transformations with flexibility while maintaining its core purpose of protecting individuals from potential violations.

Their insights at the time revealed the shortcomings of American laws[12]—similar to those in the rest of the world—in providing comprehensive privacy protection. This led them to suggest the need for an expanded right to privacy, a necessity that has become even more apparent in the face of challenges businesses encounter in the era of digital and technological transformation.

From this, the philosophical and legal question remains: How can the law keep pace with the ongoing digital revolution while balancing innovation and the protection of individual rights?

---

[3] The FTC reported that 67% of consumers were "very concerned" about the protection of personal data transmitted online, and This report is submitted by the United States Delegation to the Competition Law and Policy Committee FOR CONSIDERATION at its forthcoming meeting on 5-6 June 2000, (DAFFE/CLP(2000)6/07) , available at: https://www.ftc.gov/sites/default/files/documents/reports_annual/2000-report/2000-annrpt-competition-policy-developments.pdf

[4] CBS News et The New York Times. CBS News/New York Times Monthly Poll #1, mars 2005. Consortium interuniversitaire pour la recherche politique et sociale [distributeur], 2006-03-06. https://doi.org/10.3886/ICPSR04321.v1

[5] Turow, J., King, J., Hoofnatle, C.J., et al. (2009) Americans Reject Tailored Advertising and Three Activities That Enable It. Departmental Papers (ASC), 137

[6] See: Acquisti, A., MBo'o Ida, M., & Rochelandet, F. (2011). Privacy behaviors in e-commerce: An economy of immediate gratification. Réseaux, No. 167(3), 105-130. Available at:https://doi.org/10.3917/res.167.0105

[7] See Posner R.A (1981), "The economics of privacy"», American Economic Review, vol. 71(2), pp. 405-409.

[8] Maâzouz, D. (2021). Protection of personal data in the virtual environment in Algerian legislation (reality and challenges). Al-Ijtihad Journal for Legal and Economic Studies, 10(1), 126-144. Available at: https://asjp.cerist.dz/en/article/146015

[9] See Anthony G. Volini, (2023), *The Right t The Right to Data Priv o Data Privacy: Re acy: Revisiting W visiting Warren & Br en & Brandeis*, Norrthwestern Journal of Technology And Intellectual Property, vol 21 (1), p, 1, available at: https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1372&context=njtip.

[10] Ibid, pp, 8-10.

[11]According to Gartner, it was estimated that 75% of consumers worldwide benefited from the protection of their personal data under privacy protection laws by the end of 2023, representing a significant increase compared to 10% in 2020.

[12] See David Alan Sklansky,(2014), Too Much Information: How Not to Think About Privacy and the Fourth Amendment, 102 CAL. L. REV. 1069, 1121

The significance lies in the growing concerns of consumers regarding their privacy, in contrast to companies' increasing desire to gain deeper insights into their customers day by day. This issue now falls under the category of "personal risks of electronic transactions"[13]—a dilemma where "either you consume and your right to privacy is compromised, or you refrain from consuming and your right to privacy is still affected." This reality necessitates the establishment of clearer conditions, standards, and rules to balance the interests of all parties involved.[14]

The primary safeguard that the law provides to protect a vulnerable party like the consumer in this digital space is ensuring compliance in e-commerce. Compliance refers to adhering to the regulations governing e-commerce activities in the markets where businesses operate. This includes, but is not limited to, laws regulating e-commerce itself, data privacy regulations, electronic payment standards, accessibility requirements, and measures to prevent deceptive interfaces[15] or digital discrimination.[16]

This protection is based on the idea of the right to ownership of personal information by the individual concerned. The issue of ownership rights is frequently discussed today, particularly through the concept of "personal data ownership." This concept refers to granting any citizen the right to be the "owner of the commercial exploitation rights of their own data."[17] This presents another challenge regarding the scope of protection.

This raises the question: What types of data and information qualify as private in the context of electronic consumption?

Article 10 of *Law No. 18-05*[18] specifies the information that must be included in an electronic commercial offer provided by the electronic supplier within the framework of an electronic commercial transaction. This includes the general terms of sale, particularly the provisions related to the protection of personal data.[19]

The protection of personal data is an obligation that falls on the electronic supplier, who collects this data and creates customer files for both existing and potential clients. The supplier is strictly required to collect only the essential and necessary data for concluding commercial transactions. Additionally, they must obtain the explicit consent of e-consumers before collecting any data.[20] Moreover, they are obligated to ensure the security of information systems and maintain the confidentiality of this data.[21]

It is worth noting that e-commerce is subject to a legal framework, including provisions regulating the methods and mechanisms for protecting the personal data of e-consumers.

In the context of developing its legal framework to keep pace with the new transformations imposed by modern economies and to align with other countries[22] in regulating electronic transactions—under the necessities and requirements of ensuring legal and technical security for consumers[23]—the Algerian legislator enacted *Law No. 18-05* on e-commerce, alongside other legal texts related to e-consumers. Among these are *Law No. 18-07* on the protection of natural persons in the processing of personal data,[24] *Law No. 18-04* establishing general rules on postal and electronic communications,[25] and *Law No. 15-04* setting general rules on electronic signatures and certification.[26]

This raises the question of the effectiveness of the legal framework in protecting the personal data of e-consumers.

III.Legal Protection of E-Consumers' Personal Data

1.Defining the Scope of Protected Personal Data

Law No. 18-07, in *Article 3*, defines personal data as:

---

[13] See Weinstein N.D (1989), "Optimistic biases about personal risks", Science, vol. 24, pp. 1232-1233

[14]See Dumoulin, Caroline Lancelot Miltgen (2012). Enterprise and Consumer Privacy Protection. Revue Française de Gestion, 38(224), pp. 95-109. Hall-01115987. Acquisti, A., R. Dingledine, and P. Syverson (2003). "On the Economics of Anonymity," in Financial Cryptography - FC '03, pp. 84-102, Springer Verlag.

[15] See Community Banker Association of Indiana (2001), Identity fraud expected to triple by 2005, http://www.cbai.org/Newsletter/December2001/identity_fraud_ de2001.htm, Federal Trade Commission (2002), Identity theft heads the ftc's top 10 consumer fraud complaints of 2001, http://www.ftc.gov/opa/2002/01/idtheft.htm.

[16] See Odlyzko A. (2003), "Privacy, economics, and price discrimination on the Internet", in Fifth International Conference on Electronic Commerce, pp. 355-366, ACM.

[17] See in this regard: Arnaud Anciaux, Joëlle Farchy, and Cécile Méadel (2017), "The Establishment of Property Rights on Personal Data: A Questionable Economic Legitimacy," Revue d'économie industrielle [Online], 158 | 2. Saint-Aubin, T. (2012), "Design Your Privacy: For a Personal Data Sharing License," InternetACTU.net.

[18] Issued on May 10, 2018, concerning electronic commerce, O.G. No. 28.

[19] As stated in Article 11, Paragraph 6 of Law No. 18-05.

[20] As stated in Article 26, Paragraph 1 of Law No. 18-05.

[21] As stated in Article 26, Paragraph 2 of Law No. 18-05.

[22] See Drexl, J. (2002). E-commerce and consumer protection. Revue internationale de droit économique, Vol. XVI(2), 405-444. https://doi.org/10.3917/ride.162.0405

[23] See Allal, Naziha. (2022). Legal protection of personal data in e-commerce transactions. Journal of Research and Studies in Legal and Political Sciences, 6(2), 178-199. https://asjp.cerist.dz/en/article/198023

[24] Dated June 10, 2018, OG 34.

[25] Dated May 10, 2018, OG 27.

[26] Dated February 1, 2015, OG 6.4.

"Any information, regardless of its medium, related to an identified or identifiable person, referred to below (...) 'the data subject', either directly or indirectly, particularly by reference to an identification number or one or more elements specific to their physical, physiological, genetic, biometric, psychological, economic, cultural, or social identity."[27]

This concept, as introduced in *Article 3* of the aforementioned law, applies to the personal data of e-consumers in the field of e-commerce. *Article 26* of the same law does not specify the cases and scope of such data but merely obligates the electronic supplier to collect only the necessary data for concluding commercial transactions, provided that prior consent is obtained from e-consumers. It also requires the supplier to ensure the security and confidentiality of the information.

In this context, *Article 26, Paragraph 4* emphasizes the obligation to *"comply with the applicable legal and regulatory provisions in this field."*

Information regarding the political or religious inclinations of the e-consumer is not necessary for electronic commercial transactions, as it constitutes purely personal data. Therefore, the consumer cannot be required to disclose personal information unrelated to the transaction being conducted. Additionally, the conclusion of an electronic transaction must not be conditional upon obtaining such information.

In cases where personal data is collected, the electronic supplier is obligated to store it securely and not disclose it, as it falls under confidential data protection. Any unauthorized disclosure would constitute a violation of confidentiality, which is a responsibility placed on the electronic supplier.

The electronic supplier who has collected information and data concerning the e-consumer is not permitted to transfer this data record—whether for a fee or free of charge—to another company. This applies, for example, to mobile phone companies that provide specialized competition firms with customers' phone numbers and names.[28]

Therefore, such data may be used for purposes other than those for which they were originally intended, such as the political or religious profiling of individuals or for commercial purposes like direct marketing—for instance, displaying ads related to the word or topic a user searches for or contacting an internet and email subscriber for marketing purposes. This can lead to significant costs for consumers in addition to infringing on their freedom and privacy.[29]

For this reason, some legal opinions advocate for protecting e-consumers in this regard by using technical and technological measures to prevent such misuse, granting consumers the right to object and seek compensation, and, in some cases, even criminalizing such actions.[30] Accordingly, some legal scholars argue that information technology should serve humanity and must not lead to violations of human identity, rights, freedoms, or privacy.[31]

2. E-Consumer Rights in Personal Data Processing Under Law 18-07

Initially, it is important to emphasize that, according to *Article 26*, *paragraph 4* of *Law No. 18-05*, which stipulates the necessity of complying with the *"applicable legal and regulatory provisions in this field,"*[32] we can conclude that the legal framework governing e-consumers is not limited to Law *No. 18*-05 alone. Instead, it is also regulated by the provisions of *Law No. 18-07*, which serves as the general law concerning personal data protection in a broader sense.

Additionally, *Article 26, paragraph 5* of *Law No. 18-05* states that *"the methods of storing and securing personal data shall be determined in accordance with the applicable legislation and regulations."*

By analyzing this article, we observe that the storage of personal data falls under what is referred to as "processing". Consequently, the e-consumer benefits from the rights related to the processing and protection of personal data under *Law No. 18-07*, which serves as a legal tool for safeguarding both the e-consumer specifically and the "data subject"[33] in general.

The rights of the e-consumer[34] in the field of personal data processing include:

a. Right to Information:

The data controller is required to inform in advance every individual contacted for the purpose of collecting their personal data about the following elements:

- Identity of the data controller
- Purposes of data processing
- Any additional useful information
- Transfer of data to a foreign country

---

[27] Comp Brunk B.D. (2002), "Understanding the privacy space", First Monday, 7, http://firstmonday.org/issues/issue7_10/brunk/index.html

[28] See in this context Chaum D. (1981), "Untraceable electronic mail, return addresses, and digital pseudonyms", Communications of the ACM, vol. 24, n° 2, pp. 84-88. Cf Chellappa R.K. et R. Sin. (2002), "Personalization versus privacy: An empirical examination of the online consumer's dilemma", in 2002 Informs Meeting.

[29] See Council Recommendation on Consumer Protection in E-Commerce, March 24, 2016 – C(2016)13, available at:https://www.oecd.org/content/dam/oecd/fr/publications/reports/2016/05/oecd-recommendation-of-the-council-on-consumer-protection-in-e-commerce_g1g66e4e/9789264255272-fr.pdf

See Mohamed Hussein Mansour, Electronic Liability, Al-Maaref Establishment, Alexandria, 2006, p. 115.

[30] Ibid., p. 115.

[31] See Faqih Dandash, Studies in Private Law, Rin Legal Publications, Beirut, 1st ed., 2019, p. 113.

[32] See Karoun, S. (2020). The E-Supplier's Obligation to Protect Consumers' Personal Data in Law No. 18-05 on E-Commerce. Al-Bahith Journal for Academic Studies, 7(2), 1013-1031. https://asjp.cerist.dz/en/article/124442

[33] Article 3/2 of Law 18-17 states: "The data subject" refers to any natural person whose personal data is subject to processing.

[34] Ministry of Posts and Communications, (2024), Guide on E-Commerce, available at: https://www.mpt.gov.dz/wp-content/uploads/2024/01/guide_FR2.pdf

Additionally, when data is collected through open networks, the e-consumer must be informed, as they may not be aware that their personal data is being exchanged within networks without security guarantees. This means their data could be accessed and used without authorization by third parties.[35]

b. Right to Access

The e-consumer has the right to obtain from the data controller the following:

- Confirmation of whether their personal data has been processed, for what purposes, etc.
- Access to their processed personal data, along with any available information regarding the source of the data.[36]

c. Right to Rectification

The e-consumer can obtain for free from the data controller:

- The updating, correcting, deleting, or blocking of personal data that is being processed in violation of this law due to its incomplete or incorrect nature. The data controller is required to make the necessary corrections within ten (10) days of being notified. If the request is denied or no response is received within the specified period, the e-consumer has the right to submit a correction request to the *National Authority for Electronic Certification* to enforce the correction.[37]
- Notifying third parties to whom the personal data has been transmitted of any updates, corrections, deletions, or blocking of personal data.[38]

d. Right to Object

The e-consumer may object to the processing of their personal data whenever there is a legitimate reason. This objection may relate to the use of their data for advertising purposes, particularly for commercial use, by the data controller.[39]

3. Prohibition of Direct Prospecting

Direct solicitation through any communication mechanism, email, or any technology-based means using the personal data of a natural person is prohibited unless they have given prior consent. However, authorization for direct solicitation via email may be granted if the data was directly requested from the recipient (the e-consumer in the context of e-commerce) during the sale or provision of services. This is permitted only if the direct solicitation concerns similar products or services offered by the same natural or legal person, and if the recipient (or e-consumer) is explicitly informed of their right to object.

4. Parties Involved in the Protection of E-Consumers' Personal Data

The Algerian legislature is moving towards adopting a comprehensive framework to protect the e-consumer in their electronic transactions. Given that the concept of privacy and personal data protection in the open digital world remains challenging to define and regulate, violations can take multiple forms. The difficulty increases as electronic practices are linked to an open network. Therefore, any offer or distribution requires the prior consent of the concerned party, and any offer made without such consent could infringe on privacy. This highlights the role of various parties, whether directly or indirectly involved, in safeguarding the personal data of the e-consumer.

Among the entities involved in protecting the personal data of the e-consumer, we can mention the following:

a. The Role of Certification Service Providers in Protecting Personal Data

i.Introduction to Electronic Certification Service Providers

Article 02, paragraph 12 of *Law No. 15-04* defines the electronic certification service provider as *"a natural or legal person who grants qualified electronic certification certificates and may provide other services in the field of electronic certification."* The activity of providing electronic certification services is subject to a license granted by the National Authority for Electronic Certification.[40]

The legislator has set several conditions that must be met for licensing and practicing electronic certification services, which include:[41]

- Being subject to Algerian law if a legal entity or holding Algerian nationality if a natural person.
- Having sufficient financial capacity.
- Possessing proven qualifications and experience in the field of information and communication technologies, whether as a natural person or a manager of a legal entity.
- Having no prior conviction for a felony or misdemeanor that is incompatible with the activity of providing certification services.

[35] Article 32 of Law No. 18-07.
[36] Article 34 of Law No. 18-07.
[37] Article 35 of Law No. 18-07.
[38] The same article.
[39] However, Article 36/2 of Law 18-07 provides an exception, stating that the provisions of the first paragraph of this article do not apply "if the processing complies with a legal obligation or if the application of these provisions has been excluded by an explicit provision in the document authorizing the processing."
[40] Article 33 of Law No. 15-04.
[41] Article 34 of Law No. 15-04.

The electronic certification service provider is granted a qualification certificate for a period of one year, renewable once.[42] After that, a license[43] is issued for a period of five (05) years. The license is accompanied by a terms and conditions document,[44] which specifies the conditions and procedures for providing electronic certification services. Additionally, the certification authority signs the service provider's electronic certification certificate.[45]

ii. Their Role in Data Protection

The electronic certification service provider plays a significant role in protecting personal data, as they are involved in the certification process, including registration, issuance, granting, revocation, publication, and storage of the electronic certification certificate. This is done in accordance with the electronic certification policy, which is approved by the certification authority.[46]

The law also obligates the electronic certification service provider to maintain the confidentiality of the data and information related to the granted electronic certification certificate.[47]

The electronic certification service provider is prohibited from collecting the personal data of the concerned party (the e-consumer) without their explicit consent.[48] The provider is also obligated to collect only the necessary personal data and is not allowed to use it for other purposes.[49] Additionally, the provider must transfer information related to electronic certification certificates to the *Economic Certification Authority* for safekeeping after their expiration.[50]

In cases of service termination and license withdrawal, the provider must inform the *Economic Certification Authority*, which will then be responsible for preserving the information related to electronic certification.[51]

Regarding the processing of personal data linked to certification and electronic signatures, the law requires that data collected by the provider must be used solely for issuing and storing electronic signature certificates. However, it cannot be processed for purposes other than those for which it was originally collected.[52]

iii. Economic Authority Oversight of Electronic Certification Service Providers in Consumer Personal Data Protection

The *Economic Certification Authority* is appointed by the *Ministry of Post and Telecommunications.*[53]

Since the role of the *Electronic Certification Service Provider* is to offer electronic signature and certification services to the public, the *Economic Certification Authority* oversees and monitors its activities. This is because the service provider possesses all the information and data related to electronic certification activities. The *Economic Certification Authority* ensures the confidentiality of these data.[54] When an electronic certification certificate expires, the service provider is required to transfer it, along with the related data and information, to the *Economic Certification Authority*, which, in turn, may provide it to the judicial authorities when necessary.[55]

In conclusion, the Economic Certification Authority plays a crucial role in upholding the principle of confidentiality and protecting personal data, as the electronic certification certificate issued by the Electronic Certification Service Provider is closely linked to the e-consumer's personal data.

It is worth noting that among the electronic certification authorities is the *National Certification Authority*, which operates under the *Prime Minister*. It is an independent administrative authority responsible for promoting, developing, and ensuring the reliability of electronic signatures and certification *(Article 18 of Law 15-04)*. Additionally, it approves the electronic certification policies issued by both the *Governmental and Economic Certification Authorities (Article 18/2 of Law 15-04)*.

In the second part of this discussion, we will discuss the role of the *National Certification Authority* in ensuring vigilance over system and network security.

---

[42] Article 35 of Law No. 15-04.

[43] Article 10, paragraph 1 of Executive Decree No. 16-134: "The Legal Affairs Department is responsible for providing a legal opinion on proposals issued by the economic authority regarding the granting of a license to electronic certification service providers." See Executive Decree No. 16-134, dated April 25, 2016, which defines the organization, operation, and functions of the technical and administrative departments of the National Electronic Certification Authority (published in Official Gazette No. 26).

[44] Article 10, paragraph 3 of Executive Decree No. 16-134 states that the Legal Affairs Department is responsible for providing a legal opinion on the specifications document that defines the terms of electronic certification services before its approval by the Authority's Council.

[45] Article 38 of Law No. 15-04.

[46] Article 41 of Law No. 15-04.

[47] Article 42 of Law No. 15-04.

[48] Article 43, paragraph 1, of Law No. 15-04.

[49] Article 43, paragraph 2, of Law No. 15-04.

[50] Article 47 of Law No. 15-04.

[51] Article 59 of Law No. 15-04.

[52] For a detailed review of the automated data processing system and the crime of data manipulation in automated processing systems, see the article by Professor Boumaïza Jaber, "Attacks on Automated Data in E-Government," published in the Journal of Legal and Political Research and Studies, Faculty of Law and Political Science, Blida 2 University, Issue 12, June 2017, Part 1, p. 123 and following.

[53] Article 29 of Law No. 15-04

[54] Article 30, paragraph 14 of Law No. 15-04.

[55] Article 30, paragraph 4 of Law No. 15-04.

b. The Role of the Trusted Third Party in Protecting Personal Data

i.Introduction to the Trusted Third Party

A trusted third party is *"a legal entity that issues qualified electronic certification certificates and may provide other electronic certification services for stakeholders within the government sector."*[56]

Accordingly, a qualified electronic certification certificate is issued by a trusted third party, which ensures the authenticity and security of the electronic signature.

ii.Its Role in Data Protection

The trusted third party plays a role similar to that of the electronic certification service provider in ensuring the confidentiality of the data entrusted to it.

Additionally, e-commerce law emphasizes the protection of the e-consumer's confidential data, particularly when using electronic signatures.[57] It also mandates the security of personal data and information in electronic communications, prohibiting unauthorized access by third parties.[58]

c. Government Authority Oversight of the Trusted Third Party in Consumer Personal Data Protection

The Governmental Electronic Certification Authority operates under the Minister in charge of Postal Services and Information and Communication Technologies. It possesses legal personality and financial independence[59] and is responsible for overseeing the implementation of the electronic certification policy[60] specific to the trusted third party.

As part of its supervisory role, the governmental authority monitors and regulates the electronic certification activities carried out by the trusted third party.[61] It also retains expired electronic certification certificates, particularly those linked to the issuance process by the trusted third party, ensuring they can be handed over to the judicial authority when necessary.[62]

Overall, the Governmental Electronic Certification Authority is responsible for supervising the trusted third party, particularly in issuing electronic certification certificates and handling personal data associated with them. In addition, it plays a key role in the preservation process, which involves a set of technical measures that enable the electronic storage of documents on a secure preservation medium.[63]

IV. Technical Protection of Personal Data in E-Commerce

Law No. 18-05 on electronic commerce, in *Article 26, Paragraph 3*, establishes the principle of ensuring information system security and data confidentiality, commonly referred to in the information society as "information security,"[64] "cybersecurity,"[65] or "technological vigilance."[66]

Moreover, the amendment of the *Penal Code* under *Law No. 04-15*, dated November 10, 2004, which supplements *Ordinance No. 66-156* on the *Penal Code,* dedicates an additional section *(Section VII bis)* to this matter under the title *"Offenses Against Automated Data Processing Systems."*[67]

It is worth recalling the importance of this idea, which was previously addressed at the *World Summit* on the *Information Society* held in Tunis in 2005. The summit emphasized the need to *"enhance trust and security in the use of information and communication technologies, raise ethical awareness in technology usage, protect personal data, and adopt preventive measures to prevent the misuse of technology."*[68]

---

[56] Article 2, paragraph 11 of Law No. 15-04.

[57] See: Abdel Fattah Bayoumi Higazy, Consumer Protection on the Internet, Dar Al-Kutub Al-Qanuniya, Cairo, 2008, p. 134.

[58] Same reference, p. 135.

[59] Article 26 of Law No. 15-04.

[60] The electronic certification policy is the set of regulatory and technical rules and procedures related to electronic signature and certification (Article 2/15 of Law 15-04).

[61] Article 28 of Law No. 15-04.

[62] Article 28 of Law No. 15-04, as well as Article 14 of Executive Decree 16-135, states that the Director General of the governmental authority is responsible for ensuring the preservation of expired electronic certification certificates and the data related to their issuance by the trusted third party. (Executive Decree No. 16-135 dated April 25, 2016, defining the nature, composition, organization, and functioning of the governmental electronic certification authority, published in Official Gazette No. 26 dated April 28, 2016).

[63] In this context, Article 26/5 of Law No. 18-05 on e-commerce stipulates that the methods for storing and securing personal data shall be determined in accordance with the applicable legislation and regulations.

[64] Reda Methnani, Information Society and Development: What Relationship?, University Publishing Center, 2006, p. 446.

[65] Same reference, p. 547.

[66] This term was used in the aforementioned Executive Decree No. 16-134.

[67] Reda Metnani, previous reference, p. 404.

[68] It included eight articles from Article 394 bis to Article 394 bis 7 and specified several crimes, some of which are mentioned below:

- Fraudulent input, removal, or modification of data in an automated processing system (Article 394 bis 1).
- Possession, disclosure, publication, or use of data obtained from any of the crimes mentioned in this section, for any purpose (Article 394 bis 2).
- Designing, searching, collecting, providing, altering, or directing stored, processed, or transmitted data through an information system (Article 394 bis 2).

For further details on this matter, refer to: Aisha Ben Qara Mustafa, "The Evidentiary Value of Electronic Evidence in Criminal Proof" in Algerian and Comparative Law, New University House, Alexandria, 2010, pp. 27-28.

In this context, some believe[69] that the most significant achievement after recognizing electronic documents and electronic signatures is the possibility of contracting electronically. However, the legislator was not only aiming to promote e-commerce but also sought to develop electronic exchanges in general, enhance information networks, finalize the project of providing efficient remote services, and establish modern archiving methods, commonly referred to as *'electronic archiving.'* This, however, must be safeguarded with the necessary protection and preventive measures against all risks that may affect the contracting parties, their security, and their safety.

On the other hand, information security is particularly evident in the field of electronic payment methods. The Algerian legislature has developed this by establishing an electronic payment platform linked to the electronic certification system, along with ensuring a set of technical mechanisms, such as the implementation of an electronic transaction security system, an encryption system (public key and private key), as well as a cybersecurity system.

1.Cybersecurity and Information Security as a Mechanism for Personal Data Protection

The Geneva Summit on the Information Society in 2003, held under the theme *"Building the Information Society: A Global Challenge in the New Millennium,"* stated that *"strengthening a framework of confidence, which includes information security, network security, authentication, privacy protection, and consumer protection, is an essential and indispensable condition for the development of the Information Society and for building trust among users of information and communication technology. This necessitates the promotion of a global cybersecurity culture (...) The key content of this culture is enhancing security and ensuring data protection."*[70]

In the same context, *Article 4, Paragraph 2* of *Law No. 18-04*[71], which defines the general rules related to postal services and electronic communications, states that: *"The state, within the framework of its powers and responsibilities, shall ensure the security and integrity of electronic communications networks."*

Article 9, Paragraph 1[72] of *Executive Decree No. 16-134* states that the *Infrastructure Security Division*, managed by the division head, is responsible for providing an opinion on security-related aspects concerning electronic certification policies issued by the governmental and economic certification authorities for approval.

Meanwhile, *Paragraph 3* of the same article emphasizes the implementation of organizational, technical, and physical security measures and ensuring their application as outlined in the security policy.

As for *Paragraph 4*, it highlights the importance of *"ensuring vigilance regarding organizational, technical, and physical security."*

2. Securing the E-Payment Platform with an Electronic Certification System

Article 27, Paragraph 2 of *Law No. 18-05* states that electronic payment must be made through dedicated payment platforms. These platforms are established and operated exclusively by banks accredited by the *Bank of Algeria* and *Algeria Post*. These platforms must be connected to any type of electronic payment terminal (EPT) via the public telecommunications network.

Article 28 of the same law emphasizes that any e-commerce website must be linked to an electronic payment platform that is secured through an electronic certification system. Additionally, these platforms are subject to monitoring by the *Bank of Algeria* to uphold the principles of data confidentiality, transaction security, and integrity in electronic exchanges.[73]

Article 6, paragraph 5, of the same law, defines a payment method as any authorized means of payment under applicable legislation that allows its holder to make payments either in person or remotely through an electronic system. This definition highlights that electronic payment is a subset of electronic fund transfers, which encompass a broader range of digital transactions.[74]

In alignment with this, *Law No. 18-05* on E-Commerce reinforces the technical framework of electronic payments. *Article 27, paragraph 1*, states that payments in electronic commercial transactions can be made either remotely or upon product delivery using authorized payment methods, in accordance with applicable legislation.[75]

Given the technical and technological foundations of electronic payment, simply using a card number is not sufficient for a consumer to fulfill their obligation. In other words, providing the card number alone—whether through web pages or email—does not create a binding obligation on the consumer.

---

[69] Ali Kahloun, The General Theory of Obligations (Domestic and International Contracts), Publications of Al-Atrash Society for Books, 2012, p. 598.

See for comparison: Nathalie Mallet-Poujol, (2024), Law of Electronic Communications. Légipresse: The News of Media, Communication, and Social Networks Law, 424, pp. 257.

[70] The Geneva document also stated the need to "strengthen the framework of trust and security by taking measures to enhance mutual security in the use of information and communication technology, initiating guidelines on the right to privacy, data protection, and consumer protection."

See also Professor Reda Methnani, previous reference, pp. 453 and 491, where he defines information security as follows: "This principle concerns the responsibilities of entities tasked with data collection, namely service providers, in adhering to security standards necessary to ensure data confidentiality, safe usage, and the prevention of unauthorized access. These measures include passwords, encryption codes, and other tools ensuring information integrity."

[71] Dated May 10, 2018, Official Gazette No. 27.

[72] Executive Decree No. 16-134 dated April 25, 2016, defining the organization, operation, and functions of the technical and administrative departments of the National Electronic Certification Authority (published in Official Gazette No. 26).

[73] Article 29 of Law No. 18-05.

[74] Ali Kahloun, previous reference, p. 568.

[75] Article 46/4 of Law 18-4 on Postal and Electronic Communications states: "Every transfer of funds shall be made through all written or electronic payment methods."

Instead, electronic identity verification is required, which is ensured by electronic certification services. This means that the card number must be linked to the identity of its owner, as verified by an electronic certification certificate.[76] As a result, some describe this type of payment as "trusted electronic payment."[77]

It is also observed that in electronic payments made through electronic communication networks,[78] the electronic consumer is often unaware of who is behind the computer system or to whom the public encryption systems belong. This necessitates the intervention of a trusted third party or an electronic certification service provider to identify the parties involved and ensure the consumer's connection to their digital signature by issuing a secure electronic certification certificate, which is itself authenticated by an electronic signature.

The role of both the trusted third party and the certification service provider is to authenticate the parties and ensure security in an open digital environment. Upon verifying the electronic certification certificate, the counterpart can confidently identify the other party and trust the authenticity of their signature.[79]

Electronic certification serves as a digital mechanism that guarantees the link between the public encryption system and its owner, assuring the counterpart that the electronic signature belongs to a specific individual and no one else, thereby ensuring the required level of security.[80]

Thus, the introduction of electronic authentication signifies the intervention of a third party capable of monitoring identities, verifying them, and confirming that the signature originates from its rightful owner alone.

3. Mechanisms for Ensuring the Security of Electronic Transactions

Within the *National Electronic Certification Authority*, there is a department known as the *Information Security Department*. This department is responsible for implementing and overseeing the authority's information security policy. Additionally, it ensures continuous vigilance regarding the security of systems and information networks.[81]

The *Governmental Electronic Certification Authority* is legally required[82] to ensure technological vigilance regarding electronic signatures and certification, as well as security monitoring of systems and information networks. From these provisions, it can be inferred that the legislature has established structures aimed at reinforcing information security,[83] both in terms of electronic signatures and certification and in protecting the personal data of electronic consumers benefiting from this security framework.

a. In the Field of Auditing

The audit process serves as a mechanism for enforcing security policies, whether in electronic certification practices or data security. It involves conducting a field analysis based on an investigation of organizational and structural security aspects, assessing security measures and their implementation, evaluating the availability and effectiveness of information system security mechanisms, and performing a technical analysis of all system components. Additionally, it includes testing system resilience against various risks and analyzing potential threats by identifying vulnerabilities discovered during the audit process.[84]

The audit process is carried out by an audit unit operating under the supervision of the Director-General of the *National Electronic Certification Authority*.[85] This unit is responsible for developing audit references and internal audit procedures for the governmental authority in accordance with electronic certification policies and security policies.[86] In addition, it analyzes audit reports related to the trusted third party, which are conducted by the government entity responsible for auditing.

The audit process plays a crucial role in establishing the overall strategy for information system security, ensuring network safety, and maintaining technological vigilance.

b. In the Field of Encryption

The encryption system is a mechanism for securing and protecting information and data. It is a process of *"converting information into incomprehensible coded text to prevent unauthorized individuals from accessing or understanding it. So, it involves transforming plain text into*

---

[76] According to Article 02/7 of Law 15-04, an electronic certification certificate is defined as: a document in electronic form that establishes the link between electronic signature verification data and the signer.

[77] Ali Kahloun, previous reference.

[78] It is any establishment or group of establishments that ensures either the transmission, sending, or delivery of electronic signals, as well as the exchange of control and management information related to them between the terminal points of this network. If necessary, it also includes other means that ensure the delivery of electronic communication, as well as transmission and routing. (Article 10/21 of Law No. 18/04, dated May 10, 2018, defining the general rules related to postal and electronic communications).

[79] See Ali Kahloun, previous reference, pp. 589-590.

[80] Ali Kahloun, same reference, p. 591.

[81] See Article 9/4 of Executive Decree No. 16-134.

[82] See Executive Decree No. 16-135, dated April 25, 2016, which defines the nature, composition, organization, and functioning of the governmental electronic certification authority (published in Official Gazette No. 26).

[83] For more details, see Laurent Bloch et al. (2016), Sécurité informatique pour les DSI, RSSI et administrateurs, 5th ed., Eyrolles.

[84] Ali Kahloun, previous reference, p. 573.

[85] Articles 4 and 5 of Executive Decree No. 16-134.

[86] Article 16 of Executive Decree No. 16-134.

encrypted text."[87] It serves as a crucial method for preserving data in a form different from its original content using an algorithmic system.[88] Encryption is one of the key factors in protecting privacy and is particularly employed in cases such as commercial transactions and related data.[89]

Encryption is classified into two types: symmetric encryption,[90] which relies on a single key for both encryption and decryption and asymmetric encryption,[91] which uses two interrelated keys. The first key is a private key, known only to its owner, while the second is a public key, accessible to all users. In asymmetric encryption, data is encrypted using the private key, making it unreadable, and then transmitted over the network. When the recipient decrypts it using the public key, they can verify that the message originated from the sender (i.e., the electronic provider) and not from another source.[92]

The Algerian legislature has established encryption regulations in *Law No. 15-04* on *Electronic Signature and Certification*, defining two key components: the private encryption key and the public encryption key. The private key is a unique sequence of numbers exclusively held by the signer and is used to generate an electronic signature.[93] The second one is the public key, which is another numerical sequence made publicly available to allow verification of the electronic signature. The public key is also included in the electronic certification certificate.[94]

c. In the Field of Cybersecurity

Cybersecurity is addressed in *Article 10, Paragraph 3* of *Law No. 18-04*, which establishes the general rules related to postal and electronic communications. It encompasses a set of tools, policies, security concepts, mechanisms, guidelines, risk management strategies, best practices, safeguards, and technologies aimed at protecting electronic communications from any event that could compromise the availability, integrity, or confidentiality of stored, processed, or transmitted data.

The Algerian legislature has reinforced information security and data protection by adopting various mechanisms and guarantees to safeguard the personal data of electronic consumers, whether stored, processed, or transmitted.

V. Conclusion

In the midst of the rapid digital revolution, protecting consumers' personal data has become a fundamental pillar in ensuring a balance between freedom in electronic commerce and individual privacy rights. With the growing risks of data breaches and cyberattacks, there is an urgent need to strengthen the legal framework and develop effective monitoring mechanisms to safeguard consumers in the digital environment. The Algerian legislator has established a specialized legal corpus consisting of various tools and mechanisms to enforce this protection, aiming to keep pace with technological advancements in business and the emerging digital market. This is particularly crucial since the electronic consumer remains the weaker party in contractual relationships with economic operators who provide them with goods and services to meet their needs.

Despite the efforts made by the Algerian legislature in this field, challenges remain, particularly in the strict enforcement of laws and keeping up with rapid technological advancements. Therefore, it is essential to enhance public awareness, improve the digital infrastructure, and promote collaboration between the public and private sectors to ensure safer and more transparent electronic transactions.

---

[87] Shams El-Din Ibrahim Ahmed, Means of Combating Attacks on Privacy in the Field of Information Technology: A Comparative Study, 1st ed., Dar Al-Nahda Al-Arabiya, Cairo, 2005, p. 157

[88] See Mohamed Louadi, Introduction to Information and Communication Technologies, Centre de Publications Universitaires, 2005, p. 392: "Encryption is based on mathematical algorithms that allow an original message to be encrypted so that it remains secure throughout its transmission and is decrypted upon arrival."

[89] See Shams El-Din Ibrahim Ahmed, previous reference, p. 157.

[90] Symmetric Cryptography

[91] Asymmetric Cryptography

[92] Ali Kahloun, previous reference, pp. 581 and 582.

[93] Article 2, paragraph 8 of Law No. 15-04.

[94] Article 2, paragraph 9 of Law No. 15-04.