

Legal Security of the Electronic Consumer in Algeria: Between Technical Challenges and the Protection of Digital Rights

الأمن القانوني للمستهلك الإلكتروني في الجزائر: بين التحديات التقنية وحماية الحقوق الرقمية

Guedouari Fatma Zohra¹, Ahmed Noui²

¹University of Biskra (Algeria), fatmazohra.guedouari@univ-biskra.dz

²University Center of Barika (Algeria), ahmed.noui@cu-barika.dz

Received: 16/10 /2025

Accepted: 09/09 /2026

Published: September /2026

الملخص:

تسلط هذه الدراسة الضوء على التحديات التي تواجه المستهلك الإلكتروني في الجزائر في ظل البيئة الرقمية، لا سيما فيما يتعلق بالدفع الإلكتروني وحماية المعطيات الشخصية، باعتبارهما من أبرز نقاط ضعف المركز القانوني للمستهلك. وتهدف الدراسة إلى تقييم مدى نجاعة الإطار التشريعي الجزائري، ممثلا في القانون رقم 05-18 المتعلق بالتجارة الإلكترونية والقانون رقم 07-18 الخاص بحماية المعطيات الشخصية، وقد أظهرت النتائج أنّ التدابير التشريعية تشكل خطوة إيجابية نحو تعزيز الثقة الرقمية، إلا أنها تبقى محدودة التأثير بسبب غياب آليات رقابية فعّالة وصعوبة تحديد المسؤولية القانونية في حالات الاحتيال أو خرق البيانات. كما تبين أنّ الدفع الإلكتروني أصبح ضرورة لإنجاح التجارة الإلكترونية، لكنه يظل محفوفًا بمخاطر تقنية وقانونية تستدعي تطوير المنظومة التشريعية وتعزيز التعاون الدولي والإقليمي لمواجهة الجرائم المعلوماتية ذات الطابع العابر للحدود، بما يحقق التوازن بين حماية المستهلك وتشجيع الاستثمار في الاقتصاد الرقمي.

الكلمات المفتاحية: المستهلك الإلكتروني، الدفع الإلكتروني، حماية المعطيات الشخصية، القانون 05-18، القانون 07-18.

Abstract:

This study highlights the challenges faced by electronic consumers in Algeria within the digital environment, particularly concerning electronic payment systems and the protection of personal data, as these constitute some of the most significant vulnerabilities in the consumer's legal position. The study aims to assess the effectiveness of the Algerian legislative framework, represented by Law No. 18-05 on electronic commerce and Law No. 18-07 on the protection of personal data.

The findings indicate that the legislative measures represent a positive step toward enhancing

digital trust; however, their impact remains limited due to the absence of effective oversight mechanisms and the difficulty of establishing legal liability in cases of fraud or data breaches. Furthermore, electronic payment has become indispensable for the success of e-commerce. However, it remains fraught with technical and legal risks that necessitate the development of the legislative framework and the strengthening of international and regional cooperation to combat cross-border cybercrime, thereby achieving a balance between consumer protection and the promotion of investment in the digital economy.

Key words: Electronic Consumer; Electronic Payment; Personal Data Protection; Law 18-05; Law 18-07.

Introduction:

The rapid advance of digital transformation and the growing reliance on electronic commerce and services have rendered the digital sphere an inseparable component of contemporary life. It now constitutes a vast arena for information exchange and the execution of commercial and financial transactions. Within this environment, the electronic consumer is no longer adequately shielded by traditional means of protection, but is instead exposed to a wide spectrum of technological risks that endanger financial security, compromise privacy, and infringe upon the fundamental rights of access to and control over personal data. Empirical evidence indicates that such risks extend beyond financial fraud and cyber intrusions to encompass potential violations of privacy, the misuse of data, and the manipulation of information. Consequently, the protection of the electronic consumer emerges as both urgent and complex, requiring a convergence of technological safeguards and legal guarantees. Digital consumer security has become a cornerstone for fostering trust in the online environment, safeguarding both financial and personal rights, and ensuring the integrity of electronic transactions.

The digital era thus represents a distinctive intersection of technology, law, economics, and human behavior, necessitating coordinated efforts among legislators, regulatory authorities, and consumers themselves. Reliance on technical measures alone—such as encryption or multi-factor authentication—is insufficient, just as legal provisions, detached from effective enforcement and continuous oversight, prove inadequate. Rather, what is required is a coherent legal framework, preventive technical mechanisms, and heightened consumer awareness of rights and responsibilities in order to achieve comprehensive and effective protection.

The aim of the study:

The primary aim of this study is to examine the adequacy and effectiveness of the Algerian legislative framework in protecting electronic consumers within the digital environment, particularly in the areas of electronic payment and personal data protection. It seeks to identify the extent to which existing laws—namely Law No. 18-05 on electronic commerce and Law No. 18-07 on the protection of personal data—succeed in ensuring consumer security, fostering digital trust, and addressing the technological and legal risks inherent in online transactions. Furthermore, the study aims to propose practical recommendations to strengthen legal mechanisms, enhance institutional oversight, and promote a balanced approach that reconciles consumer protection with the encouragement of

digital economic growth.

Research Issue:

This study, therefore, addresses the central research question:

How can electronic consumer security be ensured against technological risks while maintaining an effective balance between technical safeguards and the enforceable legal framework?

Study Hypotheses:

The following hypotheses guide this research:

- 1-The current Algerian legislative framework, although progressive in intent, remains insufficient to fully ensure the protection of electronic consumers against technological and cyber risks due to the lack of effective enforcement mechanisms and specialized digital oversight bodies.
- 2- Strengthening the integration between legal regulation and technical security measures would significantly enhance consumer protection and digital trust within Algeria's e-commerce landscape.
- 3- A coherent strategy combining legal reform, institutional capacity-building, and international cooperation is essential to address cross-border cyber threats and to achieve a sustainable equilibrium between consumer security and digital innovation.

Methodology Adopted for the Study:

To this end, the study adopts a descriptive-analytical methodology, examining the technological risks confronting electronic consumers, analyzing the legal instruments regulating electronic payments and the protection of personal data, and assessing the effectiveness of existing legal and technical measures. It further highlights the responsibility and legal accountability of electronic providers in cases of non-compliance, thereby presenting a comprehensive perspective on the level of consumer protection and reinforcing trust in digital transactions. This was done to address the problem.

Study Framework:

There are two main parts to this research. The first part addresses the protection of electronic consumers against risks arising from electronic payment systems. The second part focuses on ensuring the security of consumers' personal data in the digital environment.

1- The Protection of the Electronic Consumer Against the Risks of Electronic Payment

Electronic payment has become one of the fundamental pillars for conducting transactions within the sphere of e-commerce. It constitutes an innovative and effective instrument for discharging financial obligations in the digital environment. Electronic payment systems have been specifically designed to meet the requirements of commercial transactions conducted through digital platforms, thereby ensuring speed of execution, efficiency of performance, and a reduction in reliance on traditional means of payment, while simultaneously reinforcing trust and security in digital transactions.¹

Nevertheless, this modern mechanism is not devoid of risks that may undermine the interests of the electronic consumer, particularly given the consumer's limited technical

expertise or the lack of clarity surrounding certain aspects of transactions. Such circumstances may expose consumers to fraud or financial deception.

On this basis, the present axis seeks to examine the concept of electronic payment instruments, followed by an analysis of the mechanisms for protecting the electronic consumer against the risks associated with electronic payment, with a focus on both the technical and legal dimensions in order to ensure effective consumer protection.

1.1-The Concept of Electronic Payment Instruments

With the accelerated development of e-commerce, electronic payment instruments have become indispensable tools for the completion of financial transactions at a distance. They enable consumers and suppliers alike to fulfill their financial commitments efficiently and swiftly, while reducing dependence on traditional methods of payment.

Accordingly, we shall first seek to define the concept of electronic payment instruments from both a legal and technical perspective (first section), before proceeding to present their types, while highlighting their characteristics and advantages in the context of modern digital transactions (second section).

First Section: Definition of Electronic Payment Instruments

Electronic payment instruments are defined as the various technologically-based tools and mechanisms issued by banks and duly licensed financial institutions, which allow consumers to carry out payment operations or transfer funds remotely without the need for the direct circulation of cash. They thus represent one of the most significant manifestations of digital transformation in the financial and banking sectors.²

Certain national legislations have attached particular importance to this concept. Law No. 23-09 on Monetary and Banking Law³Article 74 stipulates that: "Payment instruments are considered to be all tools that enable any person to transfer funds, regardless of the instrument or technical method employed, including electronic currency."

From this provision, it is evident that the Algerian legislator has adopted a broad conception of payment instruments, one that encompasses all tools employed, irrespective of their nature or the technology upon which they operate. This approach enhances confidence in electronic transactions, mitigates potential technical risks, and provides a basis for holding suppliers accountable in electronic environments should they breach their legal obligations. Furthermore, it lays the foundation for the development of future regulatory frameworks. Accordingly, this definition constitutes a cornerstone for understanding the role of law in safeguarding the digital consumer and in ensuring the stability of electronic transactions in a landscape fraught with technological risks.

This orientation was reaffirmed by Law No. 18-05 on Electronic Commerce⁴, which expands the concept of electronic payment instruments to include all legally authorized tools, whether for proximity or remote payments, provided they operate within a secure digital framework, as expressly set forth in Article 6 of the law. This legal determination underscores

the legislator's primary objective of ensuring the reliability of digital financial operations and the effectiveness of consumer protection, while establishing a clear basis for holding suppliers accountable in cases of non-compliance with their legal obligations.

Second Section: Types of Electronic Payment Methods

Electronic payment methods have witnessed considerable diversification as a result of the continuous development of digital technologies employed in conducting remote financial transactions. They have become versatile tools that enable individuals and institutions alike to fulfill their financial obligations within the digital environment. The most prominent of these methods include:

A- Bank Cards:

Bank cards are among the most widely used electronic payment methods. Although definitions may vary, their essence lies in being plastic or paper-based instruments that are difficult to counterfeit due to the incorporation of technological security elements⁵ Such as electronic chips or magnetic strips. These features allow cardholders to withdraw money from automated teller machines (ATMs) or pay for goods and services without carrying large amounts of cash, which may otherwise be lost or stolen.⁶ Bank cards essentially combine two core functions: payment and credit. A financial institution issues them to a natural or legal person under specific contractual conditions.⁷ This indicates that bank cards constitute a technically and legally reliable electronic payment instrument that contributes to consumer protection and ensures the integrity of digital transactions. Bank cards are generally classified into two categories:

- **Credit Cards:**

These are instruments issued by a financial institution in the form of a consumer loan, based on a contract binding the institution to the cardholder. They allow the holder to obtain goods or services from contracted merchants without immediate payment, and even to withdraw money in cases of insufficient funds. The cardholder is subsequently required to repay the amount used, together with interest, often through periodic installments.⁸

Accordingly, credit cards are an electronic payment method that grants consumers flexibility in fulfilling their obligations while establishing clear legal responsibility for repayment of both the principal and accrued interest. This enhances the protection of parties' rights and regulates digital financial transactions.⁹

- **Non-Credit Cards (Debit Cards):**

These function as a direct payment tool, whereby the amount is immediately deducted from the current account maintained with the issuing bank upon use of the card for purchasing goods, services, or withdrawing cash, without waiting for the issuance of a periodic statement.

B- Electronic Commercial Papers:

These represent the digital counterpart of traditional commercial papers, performing the same functions through electronic processing. Their main forms include:

- **Electronic Bills of Exchange:**

An electronic instrument of a tripartite nature, processed wholly or partially by electronic means, containing an order from the drawer to the drawee to pay a specified sum to the beneficiary either on demand or at a predetermined date.¹⁰

- **Electronic Checks:**

These constitute the digital equivalent of paper checks. They are issued electronically through dedicated tools, used to settle specific sums payable to a designated person or entity on a certain date. They are usually authenticated with an electronic signature to ensure validity and legal reliability.¹¹

C- Electronic Bank Transfers:

These are financial operations executed through banks or legally authorized financial institutions under a set of secure technical procedures. Transfer orders are issued via computers or specialized electronic platforms. Such transfers are distinguished by their speed, efficiency, and provision of a high degree of security and credibility in transactions, thereby strengthening consumer confidence in the digital environment.¹²

D- Electronic Money:

Electronic money represents a modern form of digital payment instruments. It constitutes a monetary value stored electronically, used as an autonomous means of payment not directly linked to a bank account, thus rendering it compatible with the requirements of e-commerce.¹³ Its types vary depending on the adopted classification criteria. However, their common feature lies in being issued in exchange for deposited sums at the issuing entity, then stored electronically either on central servers or on embedded microchips, allowing for flexible and secure use in digital transactions.¹⁴

1.2-Mechanisms of Consumer Protection Against Risks of Electronic Payment:

Given the multiplicity of risks associated with electronic payment methods—and the ensuing threats to transaction confidentiality, consumer security, and trust—it has become essential to adopt effective and comprehensive protective mechanisms. These must ensure the safe use of such methods. The forms of protection encompass both technical measures aimed at safeguarding transactions through encryption, electronic authentication, and advanced security systems that prevent intrusion or manipulation, and legal safeguards that establish the legislative and regulatory framework necessary to protect consumer rights, define the obligations of electronic suppliers and financial intermediaries, and enforce liability in cases of breach. Hence, protecting the electronic consumer against the risks of electronic payment requires combining both technical and legal approaches in a manner that guarantees security and trust within the digital environment.

First Section: Technical Protection of the Electronic Consumer Against Risks of Electronic Payment

Technical protection refers to the set of preventive measures and procedures adopted to secure electronic systems dedicated to executing payment operations, and to ensure the integrity of the platforms and websites through which such transactions are conducted. This protection rests on two interdependent aspects: first, techniques aimed at identifying and verifying user identity, thereby ensuring the legitimacy of transactions and preventing identity theft or unauthorized use; and second, techniques designed to secure electronic communications and websites through encryption protocols and information security systems that preserve data confidentiality and integrity against intrusion or tampering. Technical protection thus forms the first line of defense, enabling consumers to carry out their financial transactions with confidence and safety.

A- Identity Verification and Authentication Technologies:

With the growing risks of personal data breaches, banking institutions have adopted advanced technical standards to protect client accounts and reduce the likelihood of unauthorized withdrawals or cyberattacks. Among the most prominent of these technologies are:

- **User ID and Password Systems:**

These constitute the initial stage of technical protection, allowing clients to access and manage their personal accounts while providing valuable data used to detect hacking attempts and trace their sources.

- **Electronic Signatures:**

The electronic signature is one of the most significant means of expressing consent in the digital environment. It carries the same evidentiary weight as a traditional signature, though in electronic form, and serves as an effective tool to verify the signatory's identity and guarantee transaction authenticity.¹⁵

In this regard, the Algerian legislator explicitly provided in Article 323 bis 1 of the Civil Code that electronic signatures are legally admissible as evidence whenever they can reliably establish the signatory's identity and authenticity, provided that certified technical means are employed, chief among them electronic certification systems issued by officially authorized entities. Consequently, the legislator did not merely recognize the legality of electronic signatures but conditioned their validity upon objective and technical standards ensuring their integrity and precluding challenges to their authenticity. This reflects a legislative commitment to balancing technological development with legal security guarantees in the realm of evidence.¹⁶

B- Technologies Ensuring the Security of Transactions and Websites:

Alongside identity verification mechanisms, financial institutions employ advanced tools to secure transactions and guarantee their integrity, including:

- **Encryption:**

A technical mechanism that transforms client data into complex secret codes that are extremely difficult to decipher, thereby protecting them against intrusion or manipulation. Encryption enhances the privacy of banking transactions and boosts consumer trust in the digital environment.¹⁷ A widely adopted model is the SSL/TLS protocol (Secure Sockets Layer/Transport Layer Security), extensively used in banking websites to ensure the confidentiality of communications and transactions.

- **Firewalls:**

These function as digital barriers that regulate data flow within banking networks, connecting branches within a private internal network, and ensuring information security at a centralized monitoring point.¹⁸ Many financial institutions apply advanced firewalls integrated with Intrusion Detection Systems (IDS) to detect hacking attempts in real time.

- **Blockchain Technology:**

One of the most innovative modern digital tools, blockchain is based on a distributed system that stores transactions across a decentralized network of computers, rendering data breaches or manipulation nearly impossible. It provides a high degree of security and reliability.¹⁹ Some global banks have begun adopting blockchain to secure cross-border financial transfers, notably through the Ripple project, which enables safe and instantaneous transfers between international financial institutions.

Second Section: Legal Protection of the Electronic Consumer Against Risks of Electronic Payment

The Algerian legislator has devoted specific provisions to regulating electronic payment under Chapter VI of Law No. 18-05 on E-Commerce, particularly Articles 27 to 29, by establishing a set of rules and mechanisms aimed at strengthening consumer trust and securing financial transactions via digital platforms.

Article 27 stipulates that payment in electronic commercial transactions may be effected either remotely or upon delivery of the product, provided that licensed and legally recognized payment methods are used. Regarding cross-border electronic commercial transactions, the same article imposes mandatory remote payment through electronic platforms established by the Bank of Algeria or Algeria Post, requiring their connection to the national payment network.²⁰ This demonstrates the legislator's intent to establish a strict legal framework that ensures the security and reliability of digital transactions, balances freedom of contract with consumer protection, and constitutes an effective mechanism to mitigate technical and

financial risks while enhancing confidence in the national digital system. It thereby serves as a solid legal foundation for the stability and security of e-commerce.

Furthermore, Article 28 requires that the electronic supplier's website be linked to the payment platform through a secure electronic certification system, thus fostering trust and security among contracting parties and ensuring user authentication and transaction validity.²¹

Article 29 subjects electronic payment platforms to the supervision of the Bank of Algeria, with the aim of ensuring compliance with interoperability requirements, preserving data confidentiality, and safeguarding its integrity and security. The Bank of Algeria is thereby recognized as the sole legally authorized regulatory authority for overseeing payment systems, vested with the power to examine various banking operations both domestically and in dealings with clients.²²

Accordingly, the Algerian legislator has adopted a balanced approach combining the regulation of technical means used in electronic payment with the establishment of institutional legal safeguards, by entrusting the supervisory role to the Bank of Algeria as guarantor of financial system integrity and protector of the electronic consumer against risks associated with digital transactions.

2-Ensuring the Security of Consumers' Personal Data in the Digital Sphere

The right to the protection of privacy and personal data is among the fundamental rights recognized by various national and international legal systems, and equally enshrined in the principles of Islamic law, as it constitutes an integral component of human dignity and essential rights. With the rapid advancement of communication technologies and the expansion of electronic contracting, consumers' personal data has become increasingly exposed to exploitation and unlawful violations, thereby necessitating legislative intervention to establish a comprehensive legal framework that balances the encouragement of digital commerce with the safeguarding of individual privacy.

Within this context, this section addresses the scope of obligations incumbent upon electronic suppliers with regard to consumers' personal data, followed by the sanctions resulting from a supplier's breach of these obligations.

2.1-The Scope of the Electronic Supplier's Obligations Concerning Consumers' Personal Data

The notion of personal data has emerged in the context of electronic transactions as the information provided by the consumer to the supplier through digital media for the purpose of verifying contractual identity and ensuring the validity of commercial operations. Such data reflect an individual's private life, often encompassing sensitive information that merits special protection.²³

The significance of these data in the digital environment is heightened by their considerable economic and strategic value for online enterprises, as they are utilized to construct detailed intelligence databases that help identify consumer preferences and build

consumer profiles. However, when such use is not subject to strict legal and technical safeguards, it may evolve into a direct threat to the consumer's right to privacy.

Protecting private life is one of the foremost legal challenges generated by the digital environment, particularly in light of individuals' limited awareness of the sensitivity of their data and the mechanisms of its use, as well as the difficulty of determining legal liability in the event of a breach or leak. In this regard, international privacy guidelines have underscored the necessity of establishing effective mechanisms enabling consumers to exercise control over their data through rules grounded in transparency, informed consent, and the assurance of security and confidentiality in data collection and processing.²⁴

Personal data is defined as any information relating to a human being in his or her physical, moral, health-related, professional, or social condition, making their protection part of the fundamental rights tied to human dignity. Although the notion of data protection is not new, the accelerated pace of technological development has imparted it with ever-growing significance, prompting many national legislatures to enact specialized laws designed to prevent misuse and ensure the confidentiality of data circulation.²⁵

In electronic commercial transactions, consumer data acquires particular sensitivity, as it relates to consumers' requests, preferences, and consumption patterns. Comparative legal systems have afforded such data special protection, recognizing it as one of the essential digital rights of consumers.²⁶

Accordingly, Algerian law imposes on electronic suppliers an explicit duty to protect consumer data within the framework of their responsibility for processing it, by requiring them to comply with legal principles of data processing and to enable consumers to exercise authority over their own personal information.

First section: Supplier Liability in the Processing of Personal Data:

As a general principle, the storage or exploitation of personal data infringing on the consumer's private life is prohibited, as such rights are legally protected. However, to serve the public interest and ensure the smooth functioning of electronic commercial transactions, legislators have allowed, in certain cases, the collection and processing of such data, provided that the statutory and regulatory safeguards governing such processing are strictly observed.

Key manifestations of this obligation concern adherence to the principles of lawful data processing and specific commitments relating to the use of data for electronic advertising.

A- The Obligation to Respect the Principles of Lawful Data Processing:

The rule of directing data processing towards clearly defined purposes constitutes one of the foundational pillars of protecting consumer privacy, whereby the collection of personal data is restricted to what is strictly necessary for concluding the transaction, without excess or arbitrariness.²⁷ Article 26 of Law No. 18-05 on Electronic Commerce explicitly stipulates that: "The electronic supplier who collects personal data and compiles files of prospective

customers shall collect only such data as are necessary for the conclusion of commercial transactions...”

This provision obliges the supplier to limit data collection to what is essential, thereby prohibiting requests for information unrelated to the transaction. Moreover, consumer consent to provide data does not grant the supplier unlimited authority to disclose or transfer such data to third parties, as the supplier remains legally bound to ensure their confidentiality and security. This obligation represents one of the cornerstones of trust in the digital environment.²⁸

Nonetheless, the legislator’s phrasing of “the supplier shall” and “necessary data” raises the issue of leaving the supplier broad discretion in determining the nature of required data. This may be used positively to achieve balance in transactions, or negatively to infringe on consumer rights. In addition, the law does not contain explicit provisions on methods of storing such data, merely referring to existing legislative and regulatory rules intended to safeguard their integrity during processing or storage.

B- Obligations Relating to the Use of Data for Electronic Advertising:

Companies increasingly rely on consumers’ personal data to establish more precise marketing relationships, through what is termed targeted advertising (*la publicité ciblée*). To reconcile supplier interests with consumer rights, Article 32 of Law No. 18-05 obliges suppliers to enable consumers to refuse receipt of any electronic advertising via a specific electronic system that records their preference and provides a receipt confirming their choice.²⁹

This principle enshrines the “opt-in” system, which requires the supplier to obtain the consumer’s explicit prior consent before sending any marketing messages. This system, a form of permission-based marketing, prohibits suppliers from transmitting advertising without such consent, while simultaneously granting consumers the right to withdraw consent later under the “opt-out” mechanism.³⁰

The opt-in system is more consistent with the principle of balancing freedom of expression on the one hand, and the consumer’s right to privacy on the other. It also strengthens trust in direct marketing mechanisms in the digital environment.³¹

Furthermore, Law No. 18-05 explicitly prohibits suppliers from using personal data of natural persons for direct surveys without their prior consent, thereby requiring suppliers to specify the purpose when collecting a consumer’s email address and granting the consumer the choice to accept or refuse such surveys.³²

Second section: Enabling the Consumer to Exercise Control Over Personal Data:

The right of electronic consumers to control their personal data is among the key guarantees established by Algerian law under Law No. 18-05 on Electronic Commerce. The supplier is obliged to inform consumers clearly and in advance before processing their data, and must obtain their explicit prior consent before any collection or processing.³³ Implicit or presumed consent is insufficient; consent must be expressed directly, typically in written form

through electronic means such as clicking an “Agree” or “Accept” button on a clear message notifying the user of the intended purposes of data use.

In this regard, websites are usually required to publish a transparent privacy policy detailing methods of data collection, the purposes of use, and whether such data will be shared with third parties—thereby strengthening contractual transparency and consumer trust.³⁴

The legislator reinforced this obligation through Article 32 of Law No. 18-07³⁵, which requires informing any person, in advance, clearly and unambiguously, when contacted for the purpose of collecting personal data. This enshrines transparency as a cornerstone of privacy protection in the digital environment. Article 26 of Law No. 18-05 reiterates the same principle by requiring the consumer’s explicit consent before data collection, a principle also confirmed by Article 7 of Law No. 18-07 on Personal Data Protection, which expressly states: “No processing of personal data may be carried out without the explicit consent of the person concerned.”

It follows that consumer consent is the cornerstone of lawful data processing. However, such consent never equates to granting suppliers unrestricted authority over that data; disclosure or transfer to third parties is only permitted within the limits expressly authorized.³⁶

It should be noted that legislators did not restrict themselves to requiring prior consent, but also granted consumers the right to withdraw such consent at any time. Paragraph 2 of Article 7 of Law No. 18-07 recognizes the right to revoke previously granted consent for data processing. While this provides additional protection for consumers’ interests and privacy, it raises a practical challenge by potentially destabilizing electronic transactions.³⁷ Sudden revocation could disrupt contractual obligations. The legislator thus sought to balance the individual’s interest in protecting personal data with the supplier’s interest in transaction stability, but ultimately prioritized privacy as a fundamental human right in the digital era.

2.2-Sanctions Resulting from the Supplier’s Breach of Personal Data Protection:

The Algerian legislator has accorded significant importance to protecting electronic consumers and ensuring the security and confidentiality of their personal data. Title III of Law No. 18-05 on Electronic Commerce is dedicated to regulating offenses and sanctions applicable to suppliers who violate or neglect their legal obligations. These sanctions include both administrative and criminal penalties, designed to achieve general and specific deterrence while ensuring stability of electronic transactions in a high-risk digital environment.

First section: Administrative Sanctions

Electronic commercial activity in Algeria is strictly regulated. Suppliers must register in the Commercial Register or the Register of Traditional Industries and Crafts and obtain a special card from the National Center for the Commercial Register containing their official information. They must also deposit their electronic domain name with the relevant authority prior to commencing operations.³⁸

Chapter II of Title III of Law No. 18-05, particularly Articles 42 and 43, provides for administrative sanctions in two primary cases:

- **First case:** If a natural or legal person offers goods or services online without prior registration in the Commercial Register, the authority responsible for domain names in Algeria—based on a decree issued by the Ministry of Commerce—shall immediately suspend the supplier’s domain registration until their legal status is regularized.³⁹ This measure reflects the legislator’s intent to formally organize the digital space, ensure legal transparency in online transactions, and prevent unlawful exploitation of digital tools prior to supplier registration—thereby strengthening consumer protection and reducing risks linked to dealings with unregulated entities.

- **Second case:** If, during the course of activity, the supplier commits an offense warranting closure of their business premises under commercial legislation, the competent authority prohibits the supplier from benefiting from a domain name for a precautionary period not exceeding 30 days.⁴⁰ This preventive measure curtails unlawful exploitation of digital activities.⁴¹ It demonstrates the legislator’s emphasis on prevention and graduated sanctions, allowing the supplier an opportunity to remedy the violation while simultaneously shielding the digital environment from harmful or fraudulent practices.

In addition, Articles 45 and 46 of Law No. 18-05 empower the consumer protection authority to impose settlement fines on non-compliant suppliers. These fines constitute the legal minimum penalty, with the possibility of a 10% reduction if the supplier accepts payment. This approach reflects the legislator’s preference for conciliatory solutions, alleviating judicial burdens while retaining the deterrent effect of administrative sanctions.

Second section: Criminal Sanctions

On the criminal level, Law No. 18-05 contains explicit provisions in Chapter II of Title III imposing criminal penalties on electronic suppliers who violate the legal rules governing online transactions, particularly those concerning consumer rights and data protection. These penalties primarily take the form of monetary fines, the amount of which varies according to the violation. Suppliers who breach obligations set forth in Articles 11 and 12 of the law are liable to fines ranging from 50,000 to 500,000 Algerian dinars. This reflects the legislator’s determination to enshrine financial deterrence as a means of curbing unlawful practices and ensuring supplier compliance with legal standards for consumer and data protection.

The competent judiciary may also, as a preventive measure, suspend a supplier’s access to electronic payment platforms for up to six months, thereby protecting the integrity of electronic transactions and shielding consumers from harm resulting from legal non-compliance.⁴² This measure embodies the principle of prevention in Algerian law, striking a balance between safeguarding consumer rights, preventing potential violations, and maintaining the stability of electronic commerce.

Moreover, the legislator devoted particular attention to regulating electronic advertising in Chapter VII of Title II of Law No. 18-05, setting conditions and restrictions on product promotion via digital media.⁴³ Violations of Articles 30, 31, 32, and 34 of this law are likewise punishable by fines ranging from 50,000 to 500,000 Algerian dinars.⁴⁴ This regulation underscores the legislator’s concern with ensuring the integrity of digital

advertising, preventing unauthorized use of consumer data in marketing, and reinforcing the principles of transparency and supplier accountability.

Through this integrated system of administrative and criminal sanctions, it becomes evident that the Algerian legislator has sought to establish effective protection of personal data in the digital environment, ensure electronic suppliers' compliance with their legal obligations, strengthen trust in e-commerce, and achieve equilibrium between consumer protection and the stability of economic transactions in the digital sphere.

Conclusion:

The study reveals that protecting the electronic consumer from risks associated with payment methods and personal data constitutes one of the most pressing challenges posed by the digital economy and electronic commerce. The digital consumer is now in confrontation with complex technological and legal risks concerning the security of transactions and the protection of privacy. The Algerian legislator has responded to these transformations by establishing a relatively advanced legislative framework through Laws 18-05 and 18-07.

However, practical implementation has demonstrated the limited effectiveness of this framework in addressing the rapidly evolving technological landscape, thereby necessitating an integrated vision that combines legal, technological, and institutional dimensions.

Citations:

- 1- Fatouma Boudlal, **Electronic Payment in Algerian Legislation**, Tabnah Journal of Academic Scientific Studies, Vol. 06, No. 01, 2023, University Center of Barika (Algeria), p. 1428.
- 2- Hicham Lebza, Mohamed El Hadi Deifallah, **The Reality and Challenges of Electronic Means of Payment in Algeria**, Journal of Social Studies and Research, No. 24, December 2017, Martyr Hamma Lakhdar University, El Oued (Algeria), p. 280.
- 3- Law No. 23-09 of 21 June 2023, **containing the Monetary and Banking Law**, Official Journal, No. 43, dated 27 June 2023.
- 4- Law No. 18-05 of 10 May 2018, **concerning Electronic Commerce**, Official Journal, No. 28, dated 16 May 2018.
- 5- Wafaa Abdli, **Electronic Payment as a Means between the Inevitability of Banking Globalization and the Reality of the Monetary Function in Algeria**, Journal of Legal Studies and Research, No. 04, 2017, University of M'sila (Algeria), p. 149.
- 6- Ammar Lousif, **Strategies of the Payment System for the Twenty-First Century with Reference to the Algerian Experience**, Master's Thesis in Economic Sciences, Mentouri University, Constantine 1 (Algeria), 2009, p. 11.
- 7- Karima Shaib Bacha, **Mechanisms of Protection from the Risks of Electronic Payment in Algerian Legislation**, Algerian Journal of Public Policies, Vol. 07, No. 02, December 2018, University of Algiers 3, p. 34.
- 8 -Djamel Oujani, **The Legal System of the Credit Card**, Master's Thesis, Business Law specialization, Department of Legal and Administrative Sciences, Faculty of Law and Political Sciences, University of 8 May 1945, Guelma (Algeria), 2015/2016, pp. 28–29.
- 9- Naima Abdli, **Means of Electronic Payment in Law**, Journal of Legal and Political Thought, Vol. 05, No. 01, 2021, Ammar Thelidji University, Laghouat (Algeria), p. 227.
- 10 -Nabila Kourdi, **The Electronic Bill of Exchange**, Nebras Journal of Legal Studies, Vol. 02, No. 02, March 2017, Faculty of Law and Political Sciences, Larbi Tebessi University, Tebessa (Algeria), p. 93.

- 11- Hamid Soultani, **The Concept of Electronic Payment and Prospects for its Development in Algeria**, Journal of Legal and Political Studies and Research, Vol. 11, No. 02, 2022, Blida 2 University (Algeria), p. 215.
- 12- Imad Eddine Berkate, Houria Taybi, **Electronic Payment Methods and Their Role in Promoting Electronic Commerce**, Journal of Law and Local Development, Vol. 01, No. 02, June 2019, Ahmed Draia University, Adrar (Algeria), p. 129.
- 13- Amna Zarbout, **The Role of Electronic Payment Means in Promoting Electronic Commerce with Reference to the Algerian Experience**, Araa Journal of Economic and Administrative Studies, Vol. 01, No. 01, 2019, Institute of Economic, Commercial, and Management Sciences, University Center of Aflou (Algeria), p. 56.
- 14-Asriati, **Legal Protection for Consumers Who Use Electronic Wallets (E-Wallets) as a Means of Payment**, Alauddin Law Development Journal (ALDEV), Universitas Muslim Indonesia, Volume 6, No 1, 2024, p.46.
- 15- Saif Eddine Rahali, **Legal Guarantees for the Protection of the Electronic Consumer**, Doctoral Thesis (LMD), Law Division, Private Law specialization, Faculty of Law and Political Sciences, M'Hamed Bougara University, Boumerdes (Algeria), 2024, pp. 254–268. See also: Nour El Houda Kadri, Kamal Dahmani, **The Role of the Electronic Signature as a Technical Mechanism in Ensuring the Information Security of Electronic Payment Transactions**, Journal of Law and Human Sciences, Vol. 16, No. 02, 2023, Ziane Achour University, Djelfa (Algeria), p. 497.
- 16 -Fazia Waamer, Samia Khouthra, **The Electronic Signature as a Guarantee for Protecting the Electronic Consumer**, Journal of Research in Law and Development, Vol. 01, No. 01, June 2021, Faculty of Law and Political Sciences, Boumerdes University (Algeria), p. 36.
- 17 -Hamza Mourabit, Mansour Daoudi, **Encryption as a Mechanism to Protect Digital Works from Electronic Piracy**, Journal of Law and Political Sciences, Vol. 10, No. 01, 2023, Abbas Laghrour University, Khenchela (Algeria), p. 42.
- 18- Fatiha Hezzam, **Protection of Digital Systems between Technical Mechanisms and Security Devices: A Reading of Presidential Decree 05-20**, Journal of Law and Human Sciences, No. 03, October 2020, Ziane Achour University, Djelfa (Algeria), p. 175.
- 19 -Oussat Taklit, **Blockchain Technology: A Study of the Concept and Elements**, Journal of Legal and Social Sciences, Vol. 07, No. 02, June 2022, Ziane Achour University, Djelfa (Algeria), p. 945.
- 20 -See: Article 27 of Law No. 18-05 cited above.
- 21 -See: Article 28 of Law No. 18-05 cited above.

22- See: Article 29 of Law No. 18-05 cited above.

23 -Sabrine Hansali, **Protection of Personal Data of the Electronic Contractor: Towards Achieving Cybersecurity**, *Algerian Journal of Legal and Political Sciences*, Vol. 59, No. 02, 2020, University of Algiers 1, p. 271.

24- United Nations Conference on Trade and Development (UNCTAD), **Note by the UNCTAD Secretariat: Consumer Protection in Electronic Commerce**, Item 3(e), 24 April 2017, United Nations, p. 11.

25 -Yehia Ibrahim Dahshan, **Criminal Protection of Data in the Context of Digital Transformation**, *Journal of Legal and Economic Studies*, Vol. 9, No. 3, September 2023, Faculty of Law, Zagazig University (Egypt), 2022, pp. 18–19.

26- Mahassen Ibtissam Zeghm, **Protection of the Electronic Consumer in the Contractual Phase (A Comparative Study)**, Doctoral Thesis, Business Law specialization, Department of Law, Faculty of Law, University of Ain Témouchent – Belhadj Bouchaib (Algeria), Academic Year 2023/2024, p. 194.

27- Siham Qaroun, **The Obligation of the Electronic Supplier to Protect the Consumer's Personal Data under Law No. 18-05 on Electronic Commerce**, *Journal of Academic Studies "Al-Bahith"*, Vol. 07, No. 02, 2020, University of Batna 1 – Hadj Lakhdar (Algeria), p. 1019.

28- Mohamed Reda Temimi, **Mechanisms of Protecting the Electronic Consumer during the Contract Formation Phase in Accordance with Law No. 18-05 on Electronic Commerce**, *Journal of Human Sciences*, Vol. 09, No. 02, June 2022, Larbi Ben M'hidi University, Oum El Bouaghi (Algeria), p. 1274.

29 -Naziha Allal, Fatima Achour, **The Legal Protection of Personal Data in Electronic Commerce Transactions**, *Journal of Research and Studies in Legal and Political Sciences*, Vol. 06, No. 02, 2022, University Center Morsli Abdallah, Tipaza (Algeria), p. 184.

30- Fatima Srir, **Protection of the Consumer's Personal Data from Unsolicited Advertising via Email in the Context of Electronic Commerce Law No. 18-05**, *Journal of Rights and Freedoms*, Vol. 13, No. 01, 2025, Faculty of Law, Hassiba Ben Bouali University, Chlef (Algeria), p. 428.

31- Fatima Srir, *ibid*, p. 430.

32- *Ibid.*, p. 185.

33- Amira Ghababcha, **The Legal Protection of the Consumer in the Electronic Contract Concluded via the Internet**, Doctoral Thesis (LMD, Third Cycle in Law), Business Law specialization, Department of Law, Faculty of Law and Political Sciences, Batna 1 University – Hadj Lakhdar (Algeria), 2021–2022, p. 286.

34- Nouwara Hamlil, **Protection of Personal Data in Confronting E-Government Administration**, Critical Journal of Law and Political Sciences, Vol. 15, No. 02, 2020, Faculty of Law and Political Sciences, Mouloud Mammeri University, Tizi Ouzou (Algeria), p. 41.

35- Law No. 18-07 of 10 June 2018, **concerning the Protection of Natural Persons in the Processing of Personal Data**, Official Journal, No. 34, dated 10 June 2018.

36- Zakaria Moulay, Karim Khadim, **Protection of Consumers in E-Commerce – A Comparative Study between Algerian and European Legislations**, The Algerian and Comparative Public Law Journal, Vol. 06, No. 02, December 2020, University of Algiers 1, p. 2626.

37 -Amina Messaid, **Mechanisms for Protecting Personal Data under Law No. 18-07**, Al-Bahith Journal of Legal and Political Sciences, No. 05, June 2021, Mohamed Cherif Messaadia University, Souk Ahras (Algeria), pp. 105–106.

38- Kamal Fathi Driss, Hizoum Badr Eddine Marghni, **The Liability of the Electronic Supplier – An Economic and Legal Study**, Journal of Economic Reforms and Integration into the Global Economy, Vol. 13, No. 03, 2019, Higher School of Commerce, Algiers, p. 9.

39 -See: Article 42 of Law No. 18-05 cited above.

40 -Kamal Fathi Driss, *ibid.*, p. 10.

41- See: Article 43 of Law No. 18-05 cited above.

42- See: Article 39 of Law No. 18-05 cited above.

43 -Kamal Fathi Driss, Hizoum Badr Eddine Marghni, *ibid.*, p. 10.

44- See: Article 40 of Law No. 18-05 cited above.