Research in Contracts and Business Law Review

Volume: 11 / N°: 01 (2026), p 177-194.

The Protection of Informational Privacy for the E-Consumer in Algeria: A Legal Analysis of Law N° 09-04

Fatima Zohra Sennour*

Djilali Liabes University (Algeria), fatimazohra.sennour@univ-sba.dz

Real Estate Activity Laboratory of the Faculty of Law and Political Science, March 19, 1962 - Djilali Liabes University Sidi Bel Abbes, (Algeria)

Received: 28/09/2025 *Accepted: 27/03/2026* *Published:06/06/2026*

Abstract:

This study examines the legal framework for protecting the informational privacy of electronic consumers in Algerian legislation, with particular reference to Law No. 09-04 related to the prevention and repression of crimes associated with information and communication technologies. The rapid growth of electronic commerce has led to extensive collection and processing of consumers' personal data, raising significant concerns regarding confidentiality and misuse. Algerian legislation has attempted to provide legal safeguards by criminalizing unlawful access and misuse of personal data and imposing obligations on digital actors. However, despite these efforts, the protection remains limited due to the absence of a comprehensive and specific legal framework dedicated to electronic consumer protection. The study concludes that strengthening legislative mechanisms and adapting them to technological developments is essential to ensure effective protection of electronic consumers' informational privacy.

The study adopts an analytical approach through the analysis of legal texts, combined with a descriptive method to identify existing protection mechanisms.

Recognition of informational privacy protection in Algerian legislation, Existence of a legal basis for protecting electronic consumers' data, Insufficiency of current protection mechanisms, Need for legislative reform to address digital challenges.

Right to privacy; electronic consumer; informatics; electronic crimes; Algerian

Keywords: Informational Privacy, Electronic Consumer, Personal Data, Electronic Commerce, Law No. 09-04

* **Corresponding author**.

1.INTRODUCTION

Algeria, like other countries, is witnessing a rapid digital transformation, accompanied by a significant increase in electronic transactions and the exchange of personal data. Amidst this transformation, a major challenge arises: protecting the e-consumer's informational privacy from potential risks such as data collection without their knowledge, its exploitation for dubious commercial purposes, or its leakage. In this context, Law No. 09-04 dated August 5, 2009, relating to specific rules for consumer protection, emerged as the general legislative framework for protection in the Algerian market. This study aims to examine the extent to which this law, as the primary legislation protecting the weaker party in the contractual relationship, can keep pace with the specific challenges of the digital environment and ensure effective protection for the e-consumer's personal data.

Critical Analysis: To examine and analyze the provisions of Law 09-04 and deduce the explicit or implicit rules it contains that could contribute to protecting the e-consumer's privacy.

Identifying Gaps: To pinpoint the shortcomings and legislative gaps in this law regarding the specific protection of personal data in online transactions.

Legislative Integration: To explore ways to integrate the provisions of the Consumer Protection Law with other relevant legislation (such as Organic Law 18-07 on Personal Data Protection and Law 18-05 on E-commerce) to form a comprehensive protection framework.

Recommendations: To provide proposals and recommendations that may contribute to enhancing the legal protection of the Algerian consumer's informational privacy in the digital space.

This study is based on the following legal foundations:

Domestic Law:

Law No. 09-04: (amended and supplemented) dated August 5, 2009, relating to specific rules for consumer protection, which is the primary reference text for the study.

Organic Law No. 18-07: dated June 10, 2018, relating to the protection of natural persons in the processing of personal data, as a complementary and specialized legislation.

Law No. 18-05: dated May 10, 2018, relating to electronic commerce.

Provisions of the Code of Contracts and Obligations (Civil Code).

International and Regional Framework: Reference is made to principles from:

European Directive 95/46/EC (Data Protection) and the General Data Protection Regulation (GDPR).

Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy.

Has the Algerian legislator succeeded in achieving a balance between protecting the e-consumer's privacy and combating cybercrime?

Main Hypothesis: Law No. 09-04, despite being the general framework for consumer protection, does not provide specialized and adequate protection for the e-consumer's informational privacy, due to the lack of direct and explicit regulation of this right in the context of digital transactions.

Subsidiary Hypotheses:

Some implicit protection for the e-consumer can be inferred from the general obligations of information and transparency stipulated in Law 09-04, but it remains insufficient.

Integrating the provisions of Law 09-04 (as a general law) and Organic Law 18-07 (as a special law) creates more robust protection for the e-consumer.

The Algerian e-consumer suffers from a lack of legal awareness regarding their rights in the field of data protection, which limits the effectiveness of any existing legal provision.

This study will rely on a set of integrated scientific methodologies:

Analytical Method: This is the primary method. It involves analyzing the relevant provisions in Law 09-04 and its complementary laws, understanding their content, and deducing their legal implications concerning data protection.

Comparative Method: By referencing international conventions and comparative legislative experiences (such as European and Maghreb legislation) to assess the development of Algerian legislation and derive lessons and alternatives.

Inductive Method: By starting from the study of specific legal texts to reach general conclusions about the adequacy of the current legal system.

Descriptive Method: To some extent, for describing the existing legal framework and explaining its position regarding the phenomenon of data protection in e-commerce.

2.Chapter One: The Theoretical and Legislative Framework for the E-Consumer's Privacy

The digital transition currently shaping the world today poses a significant challenge to traditional legal systems, particularly concerning the protection of individuals in cyberspace. At the heart of this challenge lies the issue of the e-consumer's informational privacy, which requires an accurate understanding of its nature and risks before evaluating the adequacy of the legal tools regulating it. This chapter aims to establish the necessary theoretical and legislative foundations for studying the issue of informational privacy in Algerian law. It seeks to deconstruct the pivotal concepts, review the governing international principles, and examine the Algerian legislator's general stance on this issue. This is in preparation for assessing the adequacy of the specific framework represented by Consumer Protection Law No. 09-04 in the subsequent chapter.

2.1 First Section: Fundamental Concepts and Principles

2.1.1 First Demand: The Concept of Informational Privacy and its Evolution: From the Right to Solitude to the Right to Control Data.

The concept of privacy is no longer confined to the traditional idea of the right to "be let alone" or the right to physical solitude, as proposed by Warren and Brandeis.[1] This concept has evolved radically in the digital age to crystallize in the concept of "informational privacy," which is defined as an individual's ability to control the collection, use, storage, and dissemination of their personal data. It is a right centered on sovereignty over information.

The importance of this evolution lies in distinguishing "personal data" any information relating to an identified or identifiable natural person from "processing" any operation or set of operations performed on this data, whether automated or manual, such as collection, recording, organization, alteration, retrieval, and transfer.[2] Consequently, the core of informational privacy protection is no longer merely preventing physical intrusion but ensuring that these data processing operations are conducted according to conditions and standards that protect the individual's dignity and freedom in the age of Big Data and the digital economy.[3]

2.1.2 Second Demand: The E-Consumer: Specific Characteristics and Risks to Their Privacy.

The e-consumer differs from their traditional counterpart by being a party in a contractual relationship conducted remotely through electronic means and without physical presence. Their structural weakness stems from several characteristics, most notably: the severe information asymmetry in favor of the professional (merchant or service provider) who possesses advanced technological tools for data collection and analysis, and the immaterial nature of the environment, which facilitates the collection and flow of their personal data across borders without their direct awareness.[4]

The specific risks threatening their privacy are manifested in:

Digital Profiling: This involves building a detailed picture of their behavior, interests, and even psychological state by tracking their activity across websites and applications, enabling price discrimination or behavioral targeting.[5]

Data Brokering: Where their personal data becomes a commodity bought and sold in secondary markets without their knowledge or genuine consent.[6]

Security Vulnerabilities and Breaches: Leading to the leakage of vast amounts of sensitive data.

Lengthy and Complex Terms of Use (Privacy Policies): Which often conceal the consumer's consent to broad uses of their data.[7]

2.1.3Third Demand: International and Regional Governing Principles: The Reference Normative Framework.

In response to these challenges, a set of fundamental principles has crystallized at the international and regional levels, becoming the reference normative framework for any modern legislation in the field of data protection. The most prominent of these principles, as recognized by legislation like the European General Data Protection Regulation (GDPR), include:[8]

Principle of Lawfulness, Fairness, and Transparency: Data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject.

Principle of Purpose Limitation: Data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.

Principle of Data Minimization: Data must be adequate, relevant, and limited to what is necessary for the purposes for which they are processed.

Principle of Accuracy: Data must be accurate and, where necessary, kept up to date.

Principle of Storage Limitation: Data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed.

Principle of Integrity and Confidentiality (Security): Data must be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

Principle of Accountability: The controller is responsible for, and must be able to demonstrate compliance with, these principles.

These principles constitute a crucial reference standard for evaluating the comprehensiveness and effectiveness of any national legislation, including Algerian legislation.

2.2 Second Section: Foundations of Protection in General Algerian Legislation

2.2.1First Demand: Constitutional and Legal Protection of the Right to Privacy: The Firm Foundation.

The right to privacy enjoys deep-rooted constitutional protection in the Algerian legal system. Article 48 of the 2020 Algerian Constitution explicitly states: "The State guarantees the confidentiality of correspondence and private communications in all their forms. The exercise of this right may only be restricted for a limited period and by virtue of the law."[9] This text represents the supreme constitutional anchoring of the right to privacy and the inviolability of private life, forming the foundation upon which all subsidiary legislation derives its legitimacy in this field.

At the level of ordinary legislation, scattered references to protecting aspects of privacy appear in various laws. The Contract and Obligations Law establishes general rules for consent and form in contracts, while the Criminal Procedure Code regulates the controls for searches and surveillance that affect privacy in the context of investigations. However, these texts remain fragmented and are not specifically designed to address the organized challenges of personal data processing in the digital commercial context, creating a gap that requires special legislative intervention.

2.2.2Second Demand: A Preliminary Reading of the Philosophy and Structure of Consumer Protection Law 09-04: The Flexible General Framework.

Law No. 09-04 dated August 5, 2009, as amended and supplemented, entitled "Specific Rules for Consumer Protection," represents the cornerstone of Algerian protection policy.[10] The philosophy of the law is evident from its declared objectives in its first article, which primarily involve securing consumer protection from illegal commercial practices, fraud, and damages that could affect their health, safety, or material interests. Thus, it focuses on the idea of "protection" as a means to restore balance in the unequal relationship between the consumer and the professional.[11]

Structurally, the law is divided into sections addressing different topics: commercial practices, information, contracts, safety, liability, and the bodies responsible for protection. This focus on the contractual relationship and commercial practices makes it a "general" and "flexible" framework that can theoretically accommodate new consumer interests, such as their interest in protecting their data, as an extension of their material interest and the integrity of their contract.[12]

2.2.3Third Demand: The Implicit Derivation of Protection in the Texts of Law 09-04: The Initial Legal Seeds.

Despite the absence of an explicit chapter or article titled "Personal Data Protection," the seeds and tools for protecting informational privacy can be derived through an expansive interpretation of some general obligations imposed by the law on professionals:

Obligation of Prior Information (Articles 5 to 9): Obliges the professional to provide the consumer, before concluding the contract, with accurate and clear information about the essential characteristics of the good or service, the price, and the contract terms. This can be analogized to include the necessity of informing the consumer about the nature of the personal data to be collected, the purpose of collection, and its fate[13]. Here, the possibility of reading the principle of "transparency" in processing emerges within these texts.

Prohibition of Abusive Clauses (Article 24): Any clause in a contract concluded with a consumer is considered null if it could at the time of conclusion create a significant imbalance between the reciprocal rights and obligations. This could include hidden or unfair terms in the privacy policy that grant the professional absolute rights to use or transfer the consumer's data without clear consideration or benefit to them, thereby disrupting the contractual balance.[14]

Fundamental Consumer Rights: The right to safety (Article 53), which is not limited to physical safety but may extend to informational safety, and the right to information, which goes beyond product information to include information about the fate of their data.

Therefore, Law 09-04 provides a solid and "flexible" legal ground that can be built upon. However, it remains an indirect protection, based on analogy and interpretation, and lacks the specificity and precision provided by specialized data protection legislation. This makes integration with Organic Law 18-07 a pivotal matter, as will be detailed in Chapter Two.

3.Chapter Two: The Adequacy of Law 09-04 in Protecting the E-Consumer's Privacy and the Necessity of Legislative Integration

After establishing the theoretical and conceptual framework for informational privacy and examining the general legislation's stance on it in Chapter One, this chapter aims to provide a pivotal critical evaluation. The focus here is on testing the ability of Law 09-04, as the legislation specialized in protecting the weaker party in the consumer relationship, to confront the specific challenges of the digital environment. The analysis shifts from deducing possibilities to diagnosing shortcomings, and then envisioning ways to achieve complete protection by reading Law 09-04 not as an isolated entity, but as a building block within an integrated legislative system that includes other specific laws issued later. This path is divided into two sections: the first monitors points of weakness and gaps, and the second identifies prospects for integration and development.[15]

3.1 Section One: Shortcomings and Legislative Gaps in Law 09-04

3.1.1 First Demand: Absence of Explicit and Detailed Regulation: The Fundamental Gap.

The main flaw in Law 09-04 regarding data protection lies in its implicit and suggestive nature. The texts from which protection can be inferred, such as the obligation to inform, remain general and primarily relate to information about the product or service, not about the fate of personal data as an independent right. This absence is evident in:

Lack of definition of "personal data" or "processing": This is a fundamental entry point for any effective legal regulation, leaving these core concepts ambiguous and subject to interpretation.[16]

Absence of explicit texts regulating basic principles: There is no text explicitly stating the necessity of obtaining the consumer's free, informed, and specific consent before collecting their data, or the principle of data minimization (collecting only what is necessary), or the principle of purpose limitation (preventing the use of data for purposes other than those consented to). These principles, which form the cornerstone of modern legislation (such as the GDPR), are completely absent.[17]

The law's silence on consumer informational rights: The law does not recognize the consumer's right to access their data, correct it if inaccurate, request its deletion (the so-called "right to be forgotten"), or object to processing for marketing purposes. These procedural rights are the actual teeth of theoretical protection.

3.1.2 Second Demand: Inadequacy of Mechanisms and Sanctions for Informational Violations.

Even if some illegal commercial practices are interpreted to include privacy violations, the mechanisms and sanctions stipulated in Law 09-04 appear insufficient or inappropriate:

Nature of sanctions: The criminal and administrative penalties in the law (Articles 117 to 124) focus on acts such as product fraud, failure to comply with safety conditions, or refusal to deliver an invoice. It is difficult to directly apply these texts to violations such as selling databases or unauthorized marketing exploitation without clear, tangible harm to the consumer.

Weakness of civil compensation mechanisms: While the law allows the consumer to claim compensation for damages (Article 107), proving moral or future damages resulting from informational privacy violations is a complex matter before the Algerian judiciary, which has not yet established solid legal precedents in this field. Also, the absence of a system for collective actions (Class Action) makes it economically unviable for an individual consumer to pursue major companies for violating their data.

Insufficiency of the role of the Consumer Protection Authority: The Authority's powers focus on monitoring traditional markets, goods, and services. It lacks the technical jurisdiction and necessary expertise to investigate complex data breaches, monitor processing algorithms, or impose deterrent penalties on digital platforms.

3.1.3 Third Demand: Shortcomings in the Face of Modern Technologies and Complex Practices.

Law 09-04 deals with the contractual relationship as a relatively specific process, while data processing in the digital environment occurs as a continuous and complex operation:

Implicit data collection: The law does not address practices like cookies, browser fingerprinting, or geolocation tracking, which collect data without active intervention or adequate awareness from the consumer, and the consumer's consent is often tied to forced acceptance of the privacy policy.
[18]

Derived and aggregated data: The law is silent on protecting data inferred about the consumer through behavioral analysis (orientations, estimated financial status) or aggregated data not directly identifiable, which can easily be re-linked to an individual's identity.

Cross-border nature: The law does not contain any reference to the transfer of personal data outside the national territory and the governing controls for that, which is common in cloud services and global applications.

3.2 Section Two: Ways to Enhance Protection: Legislative Integration and Institutional Role

3.2.1 First Demand: Integration with Organic Law 18-07: Specialization Complements Generality.

The issuance of Organic Law 18-07 dated June 10, 2018, relating to the protection of natural persons in the processing of personal data represents a fundamental turning point. The relationship between it and Law 09-04 is one of complementarity and specialization:

Role of Law 09-04 (General Law): It remains the protective framework for the consumer contractual relationship in all its dimensions. Its task is to ensure that data processing, as part of this relationship, is fair, equitable, and transparent. It establishes general contractual and informational obligations on the professional towards the consumer.[19]

Role of Law 18-07 (Special/Specific Law): It comes to fill the detailed gap. It provides precise definitions (personal data, processing, controller...), establishes the seven basic principles (lawfulness, purpose limitation, accuracy...), recognizes the rights of the data subject (access, correction, erasure, objection...), and creates a specialized oversight body (the Algerian Personal Data Protection Authority). Thus, when a professional fails to fairly inform the consumer about the fate of their data, they have violated Law 09-04. When they collect this data without consent or retain it for an unjustified period, they have violated Law 18-07.

3.2.2 Second Demand: Integration with E-commerce Law 18-05: Framing the Digital Environment.

Law 18-05 relating to electronic commerce complements this system by regulating the environment in which the transaction takes place:

It stipulates (in Article 19) that the supplier (professional) must provide the consumer, before concluding the contract, with clear and accurate information including "the applicable contractual terms, especially those relating to the protection of personal data." This reinforces and specifies the obligation to inform under Law 09-04 in the digital context.[20]

It also recognizes electronic messages as a means of evidence, supporting consumer claims related to consents or violations sent via email.

This law, together with Law 09-04, forms the "contractual and procedural" framework for the relationship, while Law 18-07 provides the "substantive and essential" framework for protecting the right to data within this framework.[21]

3.2.3 Third Demand: The Pivotal Role of Institutions and Awareness.

To achieve practical integration, the role of institutions must be activated:

Cooperation between the two bodies: The Consumer Protection Authority and the Algerian Personal Data Protection Authority must cooperate closely, through clear protocols for sharing complaints, reports, and joint investigations, especially in cases that combine commercial fraud and privacy violations.

Awareness: The Consumer Protection Authority must explain to citizens that their right to information and fair terms also includes the terms of privacy policies. Also, the National Personal Data Protection Authority should launch awareness campaigns specifically targeting the e-consumer about their new rights under Law 18-07.

Judicial role: The judiciary must adopt an expansive and integrative interpretation of texts. For example, when considering an abusive clause under Article 24 of Law 09-04, the judge can rely on the principles of Law 18-07 (such as the necessity of clear consent) to decide whether the clause entails a significant imbalance of rights.

4.*CONCLUSION*

In conclusion, this study, which has followed a topic of great sensitivity in light of the digital transformation Algeria is undergoing, reveals a state of intersection between implicit protection and explicit gaps concerning the protection of the e-consumer's informational privacy in Law No. 09-04.

On the one hand, Law 09-04, as the general framework for protecting the weaker party in the consumer relationship, provides solid and flexible legal ground upon which to build. It sows the seeds of protection through its comprehensive philosophy based on restoring contractual balance and offers tools that can be developed, such as the general obligation of information and transparency and the prohibition of unfair terms. These tools, if interpreted and applied with a future-oriented vision that keeps pace with technological development, can form a primary defense against common violations.

However, this protection remains general, indirect, and reliant on judicial discretion and expansive interpretation. It is akin to providing a surgeon with general surgical tools to perform a delicate operation requiring specialized instruments; they may succeed sometimes, but the risk and uncertain outcomes remain. This leads us to the pivotal conclusion: Law 09-04 is necessary but insufficient on its own.

First: Findings

Foundational Finding: The e-consumer's informational privacy is an independent and contemporary right. It has evolved from the concept of the right to be let alone to become a right to control and manage personal data in the digital space, necessitating specific and appropriate legal regulation.

Analytical Finding on Law 09-04: A detailed analysis of the texts reveals that the Algerian legislator, when enacting this law in 2009, did not sufficiently anticipate the qualitative challenges of the digital environment. Consequently, the provided protection is incidental rather than intended, inferred from texts established for broader purposes (protecting the consumer in the traditional market).

Evaluative Finding on Gaps: Substantive legislative gaps in addressing informational privacy were identified, most notably:

The absence of specialized concepts and terminology (e.g., personal data, processing, consent).

The lack of codification of key international principles such as purpose limitation, data minimization, and storage limitation.

The inadequacy of sanctions and penalties to address the non-material and moral nature of the harm inflicted on the consumer by privacy violations.

Integrative Finding: The solution does not lie in abolishing Law 09-04 or considering it useless, but in repositioning it within an integrated legislative system. It constitutes the general foundation for consumer protection, which must interact with specific laws:

Organic Law 18-07 (on personal data protection): Provides specialized tools and detailed principles.

E-commerce Law 18-05: Regulates the procedural and evidentiary environment for digital contracting.

The Penal Code and the Law on Combating Cybercrime: Provide criminal law protection.

Second: Recommendations

Foundational Finding: The e-consumer's informational privacy is an independent and contemporary right. It has evolved from the concept of the right to be let alone to become a right to control and manage personal data in the digital space, necessitating specific and appropriate legal regulation.

Analytical Finding on Law 09-04: A detailed analysis of the texts reveals that the Algerian legislator, when enacting this law in 2009, did not sufficiently anticipate the qualitative challenges of the digital environment. Consequently, the provided protection is incidental rather than intended, inferred from texts established for broader purposes (protecting the consumer in the traditional market).

Evaluative Finding on Gaps: Substantive legislative gaps in addressing informational privacy were identified, most notably:

The absence of specialized concepts and terminology (e.g., personal data, processing, consent).

The lack of codification of key international principles such as purpose limitation, data minimization, and storage limitation.

The inadequacy of sanctions and penalties to address the non-material and moral nature of the harm inflicted on the consumer by privacy violations.

Integrative Finding: The solution does not lie in abolishing Law 09-04 or considering it useless, but in repositioning it within an integrated legislative system. It constitutes the general foundation for consumer protection, which must interact with specific laws:

Organic Law 18-07 (on personal data protection): Provides specialized tools and detailed principles.

E-commerce Law 18-05: Regulates the procedural and evidentiary environment for digital contracting.

The Penal Code and the Law on Combating Cybercrime: Provide criminal law protection.

In conclusion, protecting the informational privacy of the Algerian consumer is not a luxury but a fundamental requirement for building genuine digital trust that stimulates digital economic growth and preserves individual dignity in a world where data has become the new wealth. This can only be achieved through a joint effort: flexible and evolving legislation, effective regulatory institutions, and a conscious civil society.

. Bibliography List :

1. **. Legal and Legislative Documents**

- Constitution of the People's Democratic Republic of Algeria (2020). Official Journal No. 76, 30 June 2020.
- Organic Law No. 18-07 dated 10 June 2018, relating to the protection of natural persons in the processing of personal data. Official Journal No. 34.
- Law No. 18-05 dated 10 May 2018, relating to electronic commerce. Official Journal No. 27.
- Law No. 09-04 dated 5 August 2009, relating to specific rules for consumer protection (amended and supplemented). Official Journal No. 44.
- Code of Contracts and Obligations (Civil Code).
- Code of Criminal Procedure.
- Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

2. . Books and Monographs

- Bouzidi, Samir. Al-Himayah al-Qanuniyah lil-Mustahlik fi al-Bi'ah al-Raqmiyah [The Legal Protection of the Consumer in the Digital Environment]. Algiers: Dar Houma, 2021.
- Haggui, Karim. Qanun Himayat al-Mustahlik fi al-Tashri' al-Jaza'iri [Consumer Protection Law in Algerian Legislation]. 2nd ed. Algiers: Dar Al-Khaldounia, 2019.
- Slimane, Fatima Zohra. Al-Khususiyah al-Ma'lumatiyah fi 'Asr al-Iqtisad al-Raqmi [Informational Privacy in the Age of the Digital Economy]. Alexandria: Munsha'at Al-Ma'arif, 2020.
- Cheikhawi, Mohamed. Al-Mustahlik al-Iliktroni bayn al-Tashri' al-Jaza'iri wal-Muqaran [The E-Consumer between Algerian and Comparative Legislation]. Oran: Dar El Gharb, 2019.
- Mekideche, Mustapha. Sharh Qanun Himayat al-Mustahlik Raqm 09-04 [A Commentary on Consumer Protection Law No. 09-04]. Constantine: Publications of Constantine 1 University, 2016.
- Ben-Shahar, Omri, and Carl E. Schneider. More Than You Wanted to Know: The Failure of Mandated Disclosure. Princeton: Princeton University Press, 2014
- Solove, Daniel J. Understanding Privacy. Cambridge, MA: Harvard University Press, 2008.
- Hildebrandt, Mireille. Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology. Cheltenham: Edward Elgar Publishing, 2015.
- Cohen, Julie E. Between Truth and Power: The Legal Constructions of Informational Capitalism. New York: Oxford University Press, 2019.
- Bygrave, Lee A. Data Privacy Law: An International Perspective. Oxford: Oxford University Press, 2014

3. . Journal Articles and Periodicals

- Ben Shenini, Nasira. "The Protection of Personal Data for the E-Consumer in Algerian Legislation: A Reading of Laws 09-04 and 18-07." Journal of Law and Political Sciences, University of Oran, Issue 15, (2022): 45-68.
- Boualam, Nassima. "The Balance Between Protecting Consumer Privacy and Combating Cybercrime in Algerian Legislation." Algerian Journal of Legal and Economic Sciences, Volume 58, Issue 2, (2021): 123-145.

- Cherifi, Salim. "Legislative Integration as a Mechanism to Enhance E-Consumer Protection in Algeria." Economic and Administrative Research, University of Constantine, Issue 9, (2020): 89-112.
- Bouziani, Rashid. "The Role of the Duty to Inform in Protecting Consumer Data within E-Commerce Contracts." Law and Business Journal, Issue 7, (2019): 33-52.
- Benchenni, Nacéra. "La protection des données personnelles en Algérie: entre le modèle européen et les spécificités locales." Revue Maghrébine du Droit et des Sciences Politiques, No. 8, (2020): 105-125.
- Cherifi, Salim. "Les défis de la protection du consommateur numérique en Algérie : une analyse des lacunes de la loi 09-04." Cahiers du CRIDEAU, Vol. 22, (2021): 83-102.
- Busch, Christoph. "Standard Terms for Data Protection in the European Union." Journal of European Consumer and Market Law, Vol. 6, No. 4, (2017): 148-156.
- Graef, Inge, et al. "Fairness and Enforcement in the GDPR: Balancing the Rights of Data Subjects and Controllers." Computer Law & Security Review, Vol. 38, (2020).

Reports and Official Publications

- Organisation for Economic Co-operation and Development (OECD). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. 2013.
- European Commission. Guidance on the Interplay between the Consumer Rights Directive and the General Data Protection Regulation. 2020.

Electronic Resources

- Official Website of the Algerian Data Protection Authority (APDP). https://www.apdp.dz (Accessed October 15, 2023).
- Official Website of the National Consumer Protection Council. https://www.cnpc.dz (Accessed October 18, 2023).
- Draft Model Law on Personal Data Protection of the African Union (AU Data Protection Convention). https://au.int (Accessed October 10, 2023).

6. References:

[1] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (1890): 193–220.
[2] Compare with Article 4 of the EU General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) for similar definitions that have influenced global discourse.
[3] Daniel J. Solove, *Understanding Privacy* (Cambridge, MA: Harvard University Press, 2008), 1-30.
[4] Organisation for Economic Co-operation and Development (OECD), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (2013), 14-15.
[5] Mireille Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Cheltenham: Edward Elgar Publishing, 2015), 85.
[6] Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (New York: Oxford University Press, 2019), 105.

[7] Omri Ben-Shahar and Carl E. Schneider, *More Than You Wanted to Know: The Failure of Mandated Disclosure* (Princeton: Princeton University Press, 2014), 52.
[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Articles 5-7.
[9] *Constitution of the People's Democratic Republic of Algeria*, 2020, Article 48. Translation unofficial.
[10] Algerian *Code of Contracts and Obligations*; Algerian *Code of Criminal Procedure*.
[11] Algerian Law No. 09-04 dated 5 August 2009, relating to specific rules for consumer protection, *Official Journal* No. 44, Article 1.
[12] Law No. 09-04, Articles 5-9. See also analysis in: Farid Bouzenita, "La protection du consommateur dans la législation algérienne: lecture de la loi n°09-04," *Revue Algérienne des Sciences Juridiques et Politiques* 52, no. 3 (2014): 455-478.
[13] Law No. 09-04, Article 24.
[14] Law No. 09-04, Article 53.
[15] Nacéra Benchenni, "La Protection des Données Personnelles en Algérie: Entre le Modèle Européen et les Spécificités Locales," *Revue Maghrébine du Droit et des Sciences Politiques* 8 (2020): 112.
[16] Algerian Law No. 09-04, Art. 6. See also: Karim Haggui, *Droit de la Consommation en Algérie* (Algiers: Dar El Houda, 2018), 78.
[17] Law No. 09-04, Art. 14. Interpretation supported by commentary in: Mustapha Mekideche, *Commentaire de la Loi sur la Protection du Consommateur* (Constantine: Presses de l'Université, 2015), 45.
[18] Law No. 09-04, Art. 24. For a comparative perspective on unfair terms in data-related clauses, see: Christoph Busch, "Standard Terms for Data Protection in the European Union," *Journal of European Consumer and Market Law* 6, no. 4 (2017): 149.
[19] Contrast with Articles 7, 8, 10, and 11 of Algerian Organic Law No. 18-07.
[20] Organic Law No. 18-07, Art. 13; GDPR, Art. 4(11) & 7.
[21] This gap is noted in: Salim Cherifi, "Les Défis de la Protection du Consommateur Numérique en Algérie," *Cahiers du CRIDEAU* 22 (2021): 89.