

Received Date: July 23, 2025**Accepted Date: August 13, 2025****Published Date: August 30, 2025**

The challenges of digital trust in Morocco between legal foundations and practical limitations

EL HOMRANI Soufyane

PhD of private law.

Abstract:

The article analyzes the central role of trust in the digital economy and its legal framework in Morocco. It highlights the legislative foundations of this trust thru consumer protection, the regulation of electronic transactions, and the safeguarding of personal data. However, in the face of the rapid transformations of digital commerce, the challenges of information transparency, and the issues raised by algorithmic profiling, this framework still appears insufficient. An ambitious reform, inspired by comparative law and centered on strengthening the National Commission for Data Protection, is therefore essential to consolidate digital trust in a sustainable manner.

Keywords: Digital trust - E-commerce - Transparency - Fairness - Personal data protection.

Introduction

Lubricant of social relations, essential for the fluidity of economic systems, trust undeniably constitutes an essential lever for growth. Indeed, mutual trust between individuals intensifies transactions, increases the number of contracts, and stimulates economic dynamics. However, in the digital age, this trust is no longer limited to interpersonal good faith but is shifting toward technical and legal mechanisms that organize exchanges, structure information, and secure data. In this sense, the rise of e-commerce platforms, accelerated by the

COVID-19 pandemic, has placed information and personal data at the heart of the commercial relationship. Consumer choices are now influenced by price comparison tools and commercial influence practices, the transparency of which often remains uncertain. To this are added online reviews, which, in their various forms such as comments, star ratings, or "like" and "dislike" mentions, reflect the emergence of a true society of judgment, thereby strengthening the freedom of expression of cyberconsumers. These practices, when insufficiently regulated, open the door to abuses such as fake reviews or biased rankings and consequently generate a deficit of trust that hinders the development of e-commerce by limiting consumer adoption.

At the same time, each search, click, or payment feeds databases exploited by profiling algorithms and targeted advertising mechanisms, which places privacy protection at the center of concerns. This dual observation reveals two major challenges: on the one hand, the fairness and transparency of information, and on the other hand, the protection and security of personal data. Indeed, while the European Union has consolidated its legal arsenal to meet these new challenges, Moroccan law, although based on solid foundations, remains, in our opinion, out of sync with the transformations of the digital economy.

The interest of this work lies in highlighting this gap, by measuring the new challenges posed by information transparency and the massive circulation of data, and by reflecting on the necessary reforms to strengthen digital trust

in Morocco. The issue can therefore be formulated as follows: How to adapt Moroccan law to digital transformations in order to ensure both the integrity of information and the effective protection of personal data. To address this, it is necessary on one hand to review the legal foundations of digital trust, whether it be its normative anchoring or its consolidation in commercial relations (1), and on the other hand to analyze the new challenges posed by transparency and fairness of information in the digital platform environment, as well as the challenges raised by the protection and security of personal data in the face of emerging technologies (2).

1. The legal foundations of digital trust

Trust is at the heart of the digital economy, and Moroccan law has sought to establish it thru a normative framework aimed at securing exchanges and protecting stakeholders. This edifice rests on two complementary components: on the one hand, the legal foundations that ensure the reliability of the digital system itself, and on the other hand, the mechanisms that strengthen trust between the consumer and the professional in their commercial relationships.

1.1. The normative foundations of trust in the digital system

Digital trust cannot be separated from the normative framework that structures the relationship between the consumer and the professional in the electronic environment. In Morocco, several legislative texts have marked this construction and reflect the legislator's desire to reconcile the opening of the digital market with the protection of the user. Each text was adopted in a particular context, addressing specific concerns and often drawing inspiration from foreign experiences, whether it be French, European, or American law.

The first manifestation of legal consideration of digital risks materialized with Law No. 07-03 on offenses related to automated data processing systems, integrated into the Penal Code in 2003. This text, largely inspired by the French Godfrain law of January 5, 1988, filled a legal void by criminalizing previously unpunished behaviors, such as fraudulent access or maintenance in a system, obstruction of its operation, or alteration of its data. Its adoption responded to the need to protect a still-nascent cyberspace and to reassure economic operators in the face of the rise of cybercrime. It also reflected Morocco's desire to join the international movement to secure computer systems, in a context where the first scandals related to computer hacking in Europe and the United States had revealed the vulnerability of digital infrastructures.

A few years later, Law No. 53-05 on the electronic exchange of legal data marked a decisive step in the recognition of digital transactions and the securing of online contractual relationships. Adopted in 2007, it was set in a context marked

by the exponential increase in the number of Internet users and the need to provide the country with a legal framework capable of supporting digital development strategies. By inserting a chapter 1st "bis" in the first title of the first book of the Dahir of Obligations and Contracts, the legislator laid a fundamental milestone by granting electronic writing an evidentiary force equivalent to that of traditional writing, provided that the author's identification and the integrity of the content are guaranteed. This principle of equivalence, inspired by European Directive 1999/93/EC and reflected in the French reforms of the same period, has allowed for the modernization of Moroccan law by adapting it to the requirements of electronic commerce.

Law 53-05 also regulated electronic signatures by equating them with handwritten signatures when they are based on a reliable identification process. Reliability is presumed when the signature is secure and, if applicable, time-stamped, which strengthens the parties' confidence in digital exchanges. In contractual matters, the text establishes specific guaranties, such as the obligation for the parties to be able to verify and correct the details of the offer before confirming their commitment, as well as the implementation of an electronic acknowledgment of receipt. It also provides for mechanisms adapted to particular situations, such as the recognition of detachable electronic forms when the law requires their use for the exercise of a right of withdrawal, as well as the equivalence between the electronic act and the act on paper in contracts requiring multiple originals. These contributions have helped establish genuine legal security for electronic transactions, an essential condition for the growth of online commerce.

However, the rapid and continuous evolution of information technologies has compelled the Moroccan legislator to thoroughly revise certain provisions of Law 53-05, particularly those related to electronic signatures, cryptography, and electronic certification. The objective was to provide more flexible alternatives better suited to concrete challenges as well as the security levels required by the use of electronic certificates. Indeed, the rigidity of the mechanisms established in 2007 and the lack of large-scale projects in digitalization supported by electronic certification have limited the spread of these tools, restricting their adoption to specialized contexts and marginalizing their daily use by citizens, businesses, and even administrations.

It is in this context that a study entrusted to the National Defense Administration to define a roadmap for the evolution of digital certification offerings in Morocco led to the adoption, at the end of 2020, of Law No. 43-20 related to trust services for electronic transactions. This new text aims to modernize the Moroccan legal framework, make it more flexible, and remove the obstacles that had hindered the development of electronic certification, while aligning with

the accelerated evolution of digital technologies and the need to strengthen trust in dematerialized exchanges.

With its 84 articles, Law 43-20 draws inspiration from the legislation of pioneering countries in the field, such as the United States, Canada, France, Malaysia, or South Korea, and complies with international standards, notably the European eIDAS regulation. It regulates trust services by establishing three levels of electronic signature. The simple level, intended for practical and streamlined use, facilitates usage but does not benefit from a presumption of reliability, the burden of proof then falling on the one who invokes it. The advanced level, based on intermediate technical requirements such as the use of an electronic certificate, is intended for transactions with medium or high stakes but also remains without a presumption of reliability. Finally, the qualified level, which requires the use of robust and certified cryptographic processes, is the only one that benefits from a presumption of reliability and targets very high-stakes applications. In parallel, the law provides for a range of complementary trust services, such as the validation and preservation of electronic signatures, electronic seals, electronic timestamps, electronic registered mail, and website authentication. Each of these services is defined and regulated by application texts compliant with international standards, and subject to strict obligations to ensure their security and reliability. The law also distinguishes between accredited trusted service providers, subject to a rigorous compliance and supervision regime, and non-accredited providers, to whom a more flexible regime applies. In terms of cryptology, the legislator has also limited the scope of control to only those uses likely to threaten national defense or state security, while establishing a National Authority responsible for overseeing these services and ensuring their compliance.

Thus, by repealing certain provisions of Law 53-05 and introducing a coherent and updated framework, Law 43-20 has eliminated legal ambiguities that fueled uncertainty among operators and strengthened user protection. These individuals, in their capacity as true players in the digital economy, are now at the center of a system articulated around the essential concept of information, which permeates all the protective legislations adopted for their benefit.

1.2. The consolidation of trust between the actors in the commercial relationship

Digital trust is not only exhausted in securing technical systems and electronic exchanges, it also relies on the quality of relationships between stakeholders, particularly between the consumer and the professional. Indeed, loyalty, transparency, and the protection of fundamental rights are essential conditions in the connected environment to establish a climate of adherence. It is in this perspective that the Moroccan legislator adopted two major laws that structure

interpersonal trust in the digital space, namely, Law No. 09-08 on the protection of natural persons with regard to the processing of personal data and Law No. 31-08 enacting consumer protection measures.

The adoption of Law No. 09-08 in 2009 indeed marks an important step in anchoring the right to digital privacy. This law, inspired by the European directive 95/46/EC and the French law of January 6, 1978, on data processing and freedoms, aimed to provide Morocco with a coherent framework in a context of globalization of data flows and the rise of the digital economy. It establishes the protection of personal information as a condition of trust and organizes the relationship between data controllers and citizens. It is based on principles of consent, determined purpose, and proportionality, and requires data controllers to implement appropriate security measures. On the other hand, the concerned person is granted essential rights, namely, the right to access, rectification, deletion, and opposition to certain uses of their data.

However, the major innovation lies in the creation of the National Commission for the Control of Personal Data Protection (CNDP), an independent administrative authority responsible for ensuring compliance with the law, authorizing certain processing, and raising awareness among stakeholders. The CNDP plays the role of a trusted third party between the State, businesses, and citizens, ensuring that data circulation takes place within a framework that respects privacy. In this regard, Law 09-08 is part of an international dynamic; in Europe, the General Data Protection Regulation (GDPR) has consolidated protection by elevating it to a fundamental right, while in the United States, texts like the California Consumer Privacy Act (CCPA) as amended by the (CPRPA) grant consumers similar rights, pending a possible unified federal framework such as the proposed American Data Privacy and Protection Act (ADPPA). These comparisons illustrate a shared conviction that control over personal data is a prerequisite for sustainable trust among digital market players. the price must include all applicable fees and taxes. To this general obligation is added, for contracts concluded at a distance and particularly those formed electronically, a reinforced information obligation provided for by Article 29, which requires the professional to communicate detailed information in a clear and understandable manner about the subject of the contract, the identity of the supplier, the price, the terms of execution, and the existence of a right of withdrawal. This gradation in the intensity of the information obligation aims to restore contractual balance and ensure free and informed consent from the consumer in the digital environment.

Law 31-08 also enshrines other essential rights such as the right of withdrawal, which allows the consumer to reconsider their decision within a specified period, protection against

abusive clauses that prohibit professionals from imposing unbalanced conditions, as well as the right to product and service safety. These mechanisms reflect a clear desire to place the consumer at the center of the commercial relationship and to restore contractual balance in an environment often dominated by more powerful actors.

In this sense, trust among digital stakeholders rests on two complementary pillars, namely, Law No. 09-08, which protects privacy by ensuring control over personal data, and Law No. 31-08, which governs contractual relationships by ensuring transparency and fairness in transactions. Their articulation reflects the Moroccan legislator's desire to strengthen consumer protection and establish a more balanced and sustainable online market.

2. The new challenges of digital trust in the era of digital consumption

The digital transformation has redefined the conditions of online trust by raising new challenges that go beyond traditional consumer protection mechanisms. On one hand, loyalty and transparency of information become essential in the face of price comparison websites, online reviews, and commercial influence that now guide consumer choices. On the other hand, securing personal data has become an imperative in an environment marked by targeted advertising, profiling, and dark patterns, which reveal the limitations of Moroccan law No. 09-08. It would therefore be necessary to highlight, within the current challenges of digital trust, first the issue of clear and fair information, then that of normative adaptation in terms of data protection, in order to sustainably consolidate digital trust.

2.1. The challenges of transparency and fairness of information in the age of platforms

Today, electronic commerce undeniably stands out as one of the major drivers of economic globalization, and Morocco is not immune to this trend. Thus, the Moroccan consumer, once attached to traditional distribution channels, now increasingly turns to digital platforms to search, compare, and acquire goods and services. Indeed, the COVID-19 pandemic played a decisive role in this shift due to the restrictions that forced households to adopt digital platforms for their purchases and payments. This acceleration has certainly favored the rise of online commerce, but it has also revealed the growing dependence of consumers on information disseminated by digital platforms and intermediaries. From then on, the loyalty and transparency of this information become an essential condition for digital trust.

Among the mechanisms that crystallize these issues are price comparison tools, whose apparent objectivity sometimes masks opaque logics. Presented as tools serving consumer autonomy, they allow for a quick overview of a range of offers

and identification of the most competitive products. However, the order in which these results are displayed can be misleading. In Europe, for example, several investigations have revealed that some comparison sites favored partner companies that paid commissions, without clearly informing the user. The case law has reminded that such practices fall under deceptive commercial practices, especially when a comparison site does not reflect the actual ranking criteria and misleads the consumer by influencing their choice. Also, case law condemns any act of favoritism or preference based on a dominant position. In this sense, the internet giant "Google" was condemned by the European Commission for favoring its own price comparison tools, namely "Google Shopping" and "Google Product Search," by giving them a better ranking compared to their competitors in a non-objective manner.

This position was confirmed by the European legislator through Directive 2019/2161, known as the "New Deal for Consumers," which requires platforms to explicitly inform users about the ranking criteria and to specify whether the published reviews are authenticated. Following this European evolution, France has transposed these requirements, notably through Article L.111-7 of the Consumer Code, which now regulates platforms by requiring them to clearly indicate the ranking parameters. In Morocco, on the other hand, the law remains silent. Neither Law 31-08 on consumer protection nor other texts require comparators to specify their criteria, thus exposing the buyer to a risk of misinformation.

Online reviews illustrate another facet of this issue. Indeed, e-reputation has become a strategic lever; a well-rated product has a better chance of being chosen, while a poorly rated service can be quickly discredited. However, the proliferation of fake reviews directly threatens this credibility. In reality, some merchants buy positive reviews, while others orchestrate smear campaigns against their competitors. In France, the legislator now requires platforms to specify the methods for verifying reviews. In Morocco, on the other hand, no specific text governs online reviews. The only possible recourse lies in the provisions of the Penal Code related to defamation and public insult, which allow a merchant unfairly attacked to defend themselves. However, this framework does not cover the broader issue of artificially generated false reviews. The Moroccan consumer thus remains exposed, and the professional vulnerable to manipulative practices not sanctioned by a specific legal framework.

This issue intensifies with the rise of social media and influencers, who play a decisive role in consumer choices, especially among the younger generations. A simple recommendation can trigger massive sales, but the line between authentic testimony and disguised advertising remains blurry. To address this, the French legislator adopted Law No. 2023-451 of June 9, 2023, which constitutes the first comprehensive framework for regulating commercial

influence. It defines commercial influencers and imposes strict obligations on them, notably the use of the terms "advertisement" or "commercial collaboration" in a visible and permanent manner, under penalty of two years of imprisonment and a 300,000 euro fine. The law goes further by requiring the mention "retouched images" when content has been modified, as well as "virtual images" when they are generated by artificial intelligence. Failure to comply with these rules is punishable by one year of imprisonment and a fine of 4,500 euros, although some regret that the financial penalties are not proportionate to the sometimes considerable profits generated by these illicit practices.

In the same vein, the Professional Advertising Regulatory Authority (ARPP) requires that the commercial nature of the message be clearly indicated and that the received compensations (payment, gift, invitation, etc.) be specified, while prohibiting the use of ambiguous mentions such as "#ad" or "#freegift".

In Morocco, Law 31-08 certainly prohibits deceptive commercial practices, but it does not expressly address digital influence. The absence of suitable regulations weakens consumer protection, particularly as they are exposed to disguised advertising content.

These developments show that transparency of information and fairness of business practices have become central conditions for digital trust. However, the cyberconsumer's trust is not limited to the veracity of messages or the sincerity of online reviews. It also plays out on a more sensitive and technical ground: that of the protection and security of personal data. Indeed, every search conducted, every transaction made, and every trace left in the digital space feeds into information databases exploited by profiling algorithms and targeted advertising mechanisms. It is precisely in this area that the shortcomings of the Moroccan legal framework appear most concerning, necessitating a thorough reflection on the adaptation of Law 09-08 to contemporary standards.

2.2. The challenges of protecting and securing personal data in the face of emerging technologies

Beyond information, it is the management of personal data that is today crystallizing concerns. Indeed, the development of profiling technologies, the generalization of targeted advertising, and the proliferation of cookies and other digital trackers weaken the right to privacy and raise the question of the adequacy of Law No. 09-08. This system adopted in 2009 and inspired by European Directive 95/46/EC, sets the principles of legality, fairness, and proportionality, but it no longer meets the contemporary requirements of a digital environment dominated by algorithms and massive data exploitation.

In this sense, targeted advertising perfectly illustrates these limitations and raises the alarm regarding the respect for the

privacy of the cyberconsumer. By allowing advertisers to track the internet user's navigation and send them personalized messages based on their behavior, it relies on a particularly intrusive collection and analysis of data. If in Europe, the GDPR

Conclusion

Ultimately, digital trust appears as the indispensable foundation of the contemporary economy, as it conditions the fluidity of exchanges, the protection of cyberconsumers, and the stability of commercial relations. Moroccan law, by mobilizing instruments such as Law 31-08 on consumer protection, Law 53-05 on electronic transactions, Law 43-20 on trust services, and Law 09-08 on personal data protection, has undoubtedly laid the foundations for a solid legal framework. However, the analysis conducted has highlighted that this edifice, despite its undeniable contributions, remains insufficiently adapted to the rapid changes in the digital economy and the new challenges posed by the information society.

These observations call for an ambitious and comprehensive reform that would integrate the advancements of comparative law and establish a true accountability for digital stakeholders. The strengthening of the National Commission for the Protection of Personal Data is also a priority, as only an independent authority, equipped with enhanced resources and deterrent powers, will be able to ensure the effectiveness of rights and establish lasting trust.

Digital trust must no longer be seen as a mere technical corollary, but as a strategic requirement for economic and social development. It conditions both the citizens' adherence to the digital economy and Morocco's international attractiveness as a reliable partner. At a time when information and data represent a strategic resource comparable to energy or raw materials, only the establishment of a modern, demanding, and protective law will transform digital trust into a sustainable engine of growth, competitiveness, and prosperity. However, this task is all the more complex as the advent of artificial intelligence disrupts traditional benchmarks, by amplifying the collection and use of data, increasing the opacity of algorithms, and raising unprecedented questions about the responsibility and loyalty of autonomous systems. Tomorrow's digital trust can only be consolidated thru regulation capable of embracing these new challenges, by placing artificial intelligence at the heart of legal reflection.

References

Ouvrages :

- Kenneth J. Arrow, « Les limites de l'organisation », Paris, Presses Universitaires de France, 1976.
- ALMEIDA, N, « La société du jugement : Essai sur les nouveaux pouvoirs de l'opinion ». Armand Colin, Paris, 2007.
- Watin-Augouard, M., « Regards sur la loi Godfrain du 5 janvier 1988 relative à la fraude informatique », in Gohin, O. (coord.), « Annuaire du droit de la sécurité et de la défense » - 2, INSP, 2017.
- BANCK Aurélie, « RGPD : la protection des données à caractère personnel, 19 fiches pour réussir et maintenir votre conformité », Paris, Lextenso, 2020.

Articles :

- Anaïs Szkopinski, « Adoption de la proposition de loi encadrant l'influence commerciale, la fin des dérives ? », Dalloz actualité, 23 juin 2023.
- Laureline L'honnen-Frossard, « Publicité - Un an de droit de la publicité », les revues urisClasseur, Communication Commerce électronique n° 7-8, Juillet 2022, chron. 9.
- Nazarov, D.; Baimukhambetov, Y. « Clustering of Dark Patterns in the User Interfaces of Websites and Online Trading Portals (E-Commerce) ». Mathematics 2022.
- EL HOMRANI Soufyane, « Données bancaires et cybersécurité : plaidoyer pour une protection juridique renforcée au Maroc », Revue Droit des Affaires, Ed 59, Aout-sept, 2025.
- Vincent Dussart, « Contrepoint 2 à Michel Aglietta, Monnaie et confiance dans les sociétés marchandes », in Alain Caillé et Philippe Chanial (dir.), La confiance. Un dialogue interdisciplinaire, Paris, La Découverte, 2007.

Theses :

- Soufyane EL HOMRANI, Confiance numérique et protection du cyberconsommateur », thèse de doctorat en droit privé, FSJES Ain Chock Casablanca, Université Hassan II, soutenue le 4/07/2024.

Rapports:

- ARPP, « Posts sponsorisés d'influenceurs – Les bonnes pratiques en France », 2019.

- CNDP (Belge), « Le Règlement Général sur la Protection des Données-Lignes directrices en matière de cookies et autres traceurs », version du 03/01/2022.
- McKinsey, COVID-19 US Digital sentiment survey, avril 2020.
- Bulletin CNDP - Tiers de Confiance Numérique numéro 01, 8 juin 2020.
- CMI, Rapport d'activité monétique au 31 décembre 2020.

Jurisprudence :

- Arrêt de la Cour de cassation, civile, Chambre commerciale n°11-27.729, du 4 décembre 2012, Publié au bulletin.
- CJEU, Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. (Planet49), C-673/17.
- Commission UE, Affaire AT.39740 du 27 juin 2017 - Moteur de recherche Google (Shopping), Journal officiel de l'Union européenne C 9/11, 12.1.2018.