

Legal Governance of Artificial Intelligence in Consumer Protection: A Comparative Study in Light of Algerian and Comparative Legislation

Dr. Bouhafsi Amel¹, Pr. Taieb Brahim Ouis², Dr. Kissi Samia³

¹Faculty of law and Politicards Science, Sidi Bel Abbés University, Algeria, Email:

bouhafsi.am@gmail.com

²Faculty of law and Politicards Science, Sidi Bel Abbés University, Algeria, Email:

tavebbrahimouis@yahoo.fr

³Faculty of Law, University of Tlemcen, Algeria, Email: kissisamia6@gmail.com

Soumission: 01/03/2026

Acceptation: 15/07/2026

Publication: 03/10/2026

Abstract

As consumers increasingly turn to e-commerce to obtain digitalised products and services (connected goods, digital content and services), and as commercial practices themselves become digitalised (customer targeting, price and product comparison, chatbots), the legal framework for consumer protection both at global and, especially, national level is being put to the test. A significant tension exists between the technological contributions of artificial intelligence (AI), which drive "digital consumption," and the need to protect consumers from the risks that AI generates, particularly risks linked to the diffusion of liability among economic actors. This study analyses the current and emerging regulatory framework, at international and national level, for the consumer market, in order to assess its capacity to meet the challenges posed by AI, and asks which regulatory mechanisms for AI could ensure a fair balance between consumer protection and AI development in the digital market. The study adopts a descriptive and analytical, and at points comparative, methodology.

Keywords: Artificial intelligence, Consumer, Economic operators, Legal liability, AI risks.

Introduction

Today's world is undergoing an unprecedented digital transformation, in which artificial intelligence has become central to the delivery of consumer services from e-commerce platforms to technical-support systems, banking and healthcare. This rapid development, however, raises fundamental questions about the fairness of these systems and their accountability towards consumers (Floridi & Cowls, 2022).

Consumers and AI are today objects of both interest and concern at once. Online, whether on e-commerce platforms or social media, the consumer is met by chatbots or intelligent conversational agents asking, "Can I help you?" These agents propose commercial offers tailored specifically to the consumer, or target their personal data profile, since performance-analysis techniques enable algorithms sometimes described through the notion of "captology," the study of technology's influence on behaviour to present consumption products or content to the user (Jean, 2021).

Consumers therefore interact, directly or indirectly, with AI far more often than they may realise.

The question of the consumer's position vis-à-vis AI concerns everyone. The European Parliament, for example, adopted two resolutions, in 2020 (European Parliament, 2020) and 2021 (European Parliament, 2021), aimed at improving the digital single market and European consumers' use of AI, and it also endorsed a proposal for a European AI regulation in 2021 (European Commission, 2021). These three texts affirm the need to guarantee consumer protection and trust in the field of AI. This raises the question of what becomes of the consumer's contractual relationship with the professional "in the age of AI," and what an AI-embedded consumer contract entails a category no longer expressly established in law since Ordinance No. 2005-136 of 17 February 2005, and rarely used in case law, yet still widely favoured by legal scholarship (Calais-Auloy, Temple, & Dépincé, 2020).

In this context, the concept of fair and responsible AI emerges as an ethical and legal framework intended to ensure that such systems operate in the consumer's interest and do not cause harm or discrimination. The principle of fairness requires that AI system outputs be free of algorithmic bias that could produce unequal treatment between categories of consumers on grounds that are not objectively justified, such as race, sex, age or disability (Colorado General Assembly, 2024), while the principle of responsibility requires clear rules determining who bears legal liability for harm caused by the decisions or recommendations of these systems, together with oversight bodies capable of holding offenders to account (European Law Institute, 2025).

The importance of addressing this topic is illustrated by several key considerations:

- The wide diffusion of AI applications: reports indicate that more than 85% of customer-service interactions in large enterprises will take place through AI systems by 2026 (Gartner Research, 2025), meaning that most consumers will be subject to algorithmic decisions without direct human intervention.
- The risks of bias and discrimination: studies document numerous instances of AI systems discriminating against particular categories of consumers on the basis of sex, ethnicity, geographic location or economic status (Obermeyer et al., 2019), with some credit-scoring systems shown to rely on criteria that deprive certain groups of fair access to financing (Bartlett et al., 2022).
- The trust gap: opinion surveys indicate declining consumer trust in automated systems, with 68% of consumers expressing concern that AI systems might make unfair decisions affecting them (Edelman Trust Barometer, 2025), making clear frameworks for fairness and accountability necessary.

This study proceeds from a central research question: which regulatory mechanisms for AI can be devised to ensure a fair balance between consumer protection and the development of AI within the digital market? The study relies on an analytical and descriptive methodology, reviewing academic research and specialised reports, analysing practical cases, and drawing guiding principles from leading models in the field. The topic is addressed according to the following plan: (1) the concept of fair AI and its role in serving consumers; (2) the legal protection of consumers from the risks of AI.

This two-part structure is deliberate: Part One clarifies what "fair and responsible AI" means for consumers; Part Two asks how far existing law national and comparative translates that ideal into enforceable rights.

1. The Concept of Fair AI and Its Role in Serving Consumers

Fair and responsible AI represents a qualitative shift in customer service, aiming to deliver balanced experiences that respect consumers' rights and achieve fairness in digital transactions. This section examines the concept of fair and responsible AI, and how it can improve the customer experience in consumer service.

1.1. The Concept of Fair and Responsible AI and Its Principles

1.1.1. The Concept of Fair and Responsible AI

Artificial intelligence (AI) is the capacity of machines or programs to perform tasks that normally require human intelligence, such as perception, reasoning, learning, decision-making and problem-solving. AI has advanced rapidly in recent years thanks to the availability of large volumes of data, powerful computing resources, and breakthroughs in algorithms and techniques.

AI has increasingly been applied across various fields and industries, such as healthcare, education, entertainment, finance and manufacturing (Fastercapital.com, n.d.).

One of the areas in which AI has had the greatest impact, however, is the consumer sector. "Consumer AI" refers to the use of AI to improve products and services designed for, or used by, individual customers rather than companies or institutions.

Consumer AI can be seen in many aspects of daily life. Smartphones and personal assistants, for instance, use AI to understand our voices, recognise our faces, suggest our next actions and improve battery life; AI also powers virtual assistants that help with various tasks, such as Siri, Alexa, Google Assistant and Cortana.

Consumer AI often relies on the collection and analysis of personal data identity, location, activity and behaviour which raises the question of who owns, controls and accesses that data, and how it is used, shared and protected. AI also exposes consumers to potential threats such as hacking, phishing and identity theft, through the collection of data that is more exposed to risk and of greater value.

This brings us to the notion of fair and responsible AI, which refers to a set of ethical, legal and technical principles intended to ensure that AI systems operate in a manner that respects human rights, avoids bias and discrimination, is subject to accountability, and is transparent in its processes and decisions (OECD, 2019). This concept did not emerge in a vacuum, but developed in response to growing risks accompanying the wide diffusion of AI applications in areas central to people's lives, such as employment, credit, healthcare and e-commerce (Eubanks, 2018). Fair and responsible AI is a natural extension of the broader concept of "ethical AI," but is distinguished by its particular focus on two central dimensions: *fairness*, concerned with ensuring that systems do not cause unjustified harm to particular categories of users or affected persons, and *responsibility*, concerned with identifying who bears legal and ethical liability for the acts and decisions of these systems (Hickok, 2023).

The distinction matters: ethics alone can rest on voluntary codes, whereas a legal conception of fairness demands enforceable standards and remedies for the consumer actually harmed which is why legislators have felt compelled to intervene rather than leave the matter to self-regulation.

1.1.2. Principles of Fair and Responsible AI

Fair and responsible AI rests on a set of principles, the most important of which are as follows.

(a) Fairness

Fairness in AI is the absence of algorithmic bias that could produce unequal treatment between individuals or groups on grounds that are not objectively justified, such as race, sex, age, disability, religion or national origin. Algorithmic bias can be classified into several main types:

- Design bias: arises when the engineering choices made by developers reflect mistaken assumptions or biased values (Crawford, 2021).
- Data bias: arises when training data is not adequately representative of all segments of society, or when data contains historical biases reflecting past discrimination (Barocas & Selbst, 2016).
- Interaction bias: arises when users interact with the system in ways that reinforce existing biases or create new ones (Zou & Schiebinger, 2018).

To ensure fairness, AI systems must be capable of achieving equity. Although machine learning is inherently a form of statistical discrimination since such models are increasingly used to guide high-stakes decisions affecting people discrimination becomes objectionable when it systematically advantages privileged groups while systematically harming unprivileged ones, a pattern that can arise from bias in training data, whether through biased labelling or under- or over-sampling, producing models with undesirable bias (IBM, n.d.-a). For this reason, the following are necessary:

- Diverse and representative data: ensuring that training data is diverse and representative of the populations a model is meant to serve, incorporating data from different demographic groups to avoid under-representation or bias, regularly auditing training data for bias, and using tools and methods to identify and correct bias in datasets before model training (IBM, n.d.-a).
- Bias-aware algorithms: incorporating fairness metrics into the development process to assess how model predictions affect different subgroups, monitoring and minimising disparities in outcomes across demographic groups, and applying algorithmic constraints so that the model adheres to predetermined fairness standards during training and deployment.
- Bias-mitigation techniques: applying techniques such as resampling, reweighting and adversarial training to mitigate bias in model predictions.
- Diverse development teams: assembling multidisciplinary, diverse teams to participate in AI development, since diverse teams can bring different perspectives that help identify and correct biases which homogeneous teams might overlook.
- AI ethics review boards: establishing boards or committees to assess the potential biases and ethical implications of AI projects, capable of providing guidance on ethical considerations throughout the development lifecycle.

None of these measures is sufficient alone: diverse data addresses data bias but not design bias, which is why leading frameworks, notably the EU's risk-based approach discussed below, combine several mechanisms cumulatively.

(b) Transparency

Users must be able to see how a service works, assess its functions, and understand its strengths and limits (IBM, n.d.-a). Increased transparency helps consumers better understand how an AI model or service was created, helping them determine whether the model is suitable for a given use case, or assess how it might produce inaccurate or biased conclusions. Transparency comprises several interrelated dimensions: disclosure, meaning that users are informed they are interacting with an AI system and told of its capabilities and limits; explainability (OECD, 2024), the capacity to provide comprehensible explanations of how a system reached a given decision; and auditability, the capacity for independent review of a system's performance and decisions.

These three dimensions raise distinct concerns. Disclosure resembles traditional information duties and integrates easily into existing pre-contractual obligations. Explainability is harder, since many capable AI systems remain "black boxes" even to their developers. Auditability, finally, is less an individual right than a systemic safeguard exercised on the consumer's behalf by regulators or accredited third parties which matters for enforcement design, since it determines whether the consumer must act alone or may rely on institutional oversight.

(c) Responsibility and accountability

This principle requires that clearly identified parties bear legal and ethical liability for harm or decisions caused by AI systems, while accountability requires effective mechanisms to hold those parties to account when they fail to meet their obligations. This is achieved by establishing clear rules identifying who is responsible for a system's actions whether the developer, distributor, user, or a combination of these facilitating human oversight of critical decisions, establishing clear lines of accountability, maintaining continuous monitoring of AI systems to identify and address ethical concerns, biases or problems that may arise over time, and regularly reviewing AI models for compliance with ethical guidelines, in addition to adopting the fairness mechanisms noted above, while requiring developers and distributors to conduct periodic risk assessments and document the measures taken to prevent harm (Colorado General Assembly, 2024).

A recurring difficulty is the length of the AI value chain: a chatbot may combine a foundation model, a fine-tuning layer and a deployment interface from different companies, with the consumer's own supplier last in the chain often having the least insight into how it works. The European and American approaches, examined below, allocate this liability differently; Algerian law does not yet answer it at all.

(d) Protection of privacy and safety

Many regulatory frameworks, including the General Data Protection Regulation, require organisations to comply with specific privacy principles when processing personal information, given that malicious third parties with access to a trained machine-learning model even without access to the training data itself may be able to disclose sensitive personal information about the individuals whose data was used to train the model. This includes data minimisation (collecting and processing only the data necessary for the intended purpose), informed consent (obtaining clear consent for data processing, particularly where used for unforeseen purposes), security and reliability (designing systems resistant to malicious attack and able to

operate safely in unforeseen circumstances), and safety (European Commission, High-Level Expert Group on AI, 2019).

Privacy and safety are often the most tangible of the four principles for consumers, since a data breach causes concrete harm in a way abstract algorithmic bias may not which helps explain why, as the second part shows, existing Algerian legislation addresses data-related AI harms better than it addresses bias and liability allocation.

1.2. The Role of Fair AI in Serving Consumers

Fair AI plays a pivotal role in improving consumer experience and protecting consumer rights in the digital era. As reliance on intelligent systems across various aspects of life increases, it becomes essential that these technologies be equitable, transparent and accountable.

1.2.1. Protection of Consumer Rights

Fair AI plays an important role in protecting consumer rights by combating bias and discrimination, since it aims to identify and mitigate biases present in data and algorithms, thereby preventing discrimination against particular categories of consumers (Al-Naqib, 2024) in areas such as financial services for example, refusing loans or imposing higher insurance premiums on the basis of non-objective factors employment, by excluding qualified candidates on the basis of unintended algorithmic bias, or pricing, by offering different prices for the same service based on consumer characteristics. A 2025 University of California study found that AI systems used in mortgage lending exhibited systematic bias against racial minorities of up to 37%, compared with borrowers of similar creditworthiness from other backgrounds (University of California, Berkeley Center for Law & Technology, 2025).

Fair AI also contributes to building trust and consumer loyalty, trust being a decisive factor in the success of any AI system serving consumers (Gillespie, 2024). IBM, for example, has developed a framework (IBM, n.d.-a) articulating the principles that form the pillars of trust, intended to answer the question: "What does it take to trust the output of an AI model?" trustworthy AI being regarded within IBM as a strategic and ethical necessity that any organisation can use to guide its own AI efforts.

Among these pillars is explainability, since the ability to explain and clarify is more necessary than ever for designing trustworthy AI. IBM's approach to explainability rests on two connected elements: prediction accuracy, achieved by running simulations and comparing AI outputs against results in the training dataset the most common technique for this purpose being Local Interpretable Model-agnostic Explanations (LIME), which explains a classifier's prediction through the underlying machine-learning algorithm, allowing these predictions to be traced by narrowing the scope of the model's rules and features and decision understanding, the human factor, requiring practitioners to be able to understand how, and why, the AI reaches its conclusions.

The pillars of trust also contribute to strengthening transparency and fairness, as well as to building a positive reputation, since institutions known for applying fairness standards gain a competitive advantage and, importantly, experience fewer disputes through reduced complaints and appeals.

The relationship between fairness and customer loyalty directly affects consumer behaviour: consumers recommend the service to others and are more tolerant of occasional technical errors. According to a study

published in the Journal of Consumer Research, institutions perceived as "fair" in their use of AI enjoy higher loyalty rates than institutions that do not apply fairness standards (Johnson & Smith, 2024).

These two functions protecting rights and building loyalty are not always aligned: a reputational case for fairness holds only while it remains commercially advantageous. This is the gap that legal protection, examined in the second part, is meant to fill.

1.2.2. Improving the Quality of Services Provided to Consumers

Fair AI can analyse consumer preferences and behaviours to provide recommendations, products and services better tailored to individual needs, and can improve efficiency and responsiveness by automating routine tasks, such as answering common queries through chatbots, thereby speeding up response times and improving the overall efficiency of customer service (uxwritingar.com, n.d.). Proactive support further allows intelligent systems to anticipate potential problems and offer solutions in advance, enhancing customer satisfaction and loyalty.

Fair systems are, by their nature, high-quality systems, since they contain diverse, bias-free data that is, more accurate models and serve all consumers equally; ease of understanding a system also facilitates its improvement. A 2025 Google Research study found that models subjected to debiasing processes showed improved overall accuracy in addition to improved fairness (Google Research, 2025).

Improving service quality for consumers also means systems usable by all categories of consumers, services available across different geographic regions and economic circumstances, and systems that accommodate consumers' linguistic and cultural diversity. According to a report by Microsoft Accessibility, 74% of consumers with disabilities encountered difficulties dealing with AI systems that did not observe inclusive design standards (Microsoft Accessibility, 2025).

This points to a broader observation: quality and fairness are two faces of the same design choice, since a system trained predominantly on one demographic's data will tend to both perform less well and treat other groups less fairly.

1.2.3. Regulatory Compliance and Avoidance of Legal Risk

The world is witnessing growing legislation imposing fairness standards on AI systems, including the EU AI Act, which classifies systems by risk and imposes strict fairness requirements for high-risk systems (European Parliament, 2025).

Likewise, the United States has multiple bills at both federal and state level imposing fairness testing, in addition to the OECD, which has developed AI principles affirming that systems must be fair and non-discriminatory.

Disregarding fairness standards carries significant legal risk, chiefly substantial financial penalties fines for violating the EU AI Regulation can reach €30 million or 6% of annual global revenue in addition to a rising number of class actions against institutions using discriminatory AI systems, while regulators may prohibit the use of systems that do not comply with fairness standards (CNIL, 2024).

ISO also recommends, in its ISO/IEC 42001:2024 standard, that organisations adopt a proactive approach to managing fairness in AI, including conducting impact assessments on consumer rights before deploying any system (International Organization for Standardization, 2024).

Some practical applications may be noted:

- Chatbots and virtual assistants: providing instant, round-the-clock support, answering queries and directing customers.
- Personalised recommendation systems: suggesting products and services based on browsing and purchase history.
- Customer-sentiment analysis: understanding customer opinions and feedback to improve service quality.
- Robotic process automation: streamlining repetitive tasks and improving call-centre efficiency.

Taken together, fair and responsible AI is best understood not as one self-executing standard but as a bundle of commitments fairness, transparency, accountability, privacy and safety each requiring its own institutional infrastructure. Voluntary adoption improves outcomes but is, by definition, unenforceable by the consumer who has actually suffered harm, which is why the state of positive law, examined next, is decisive.

2. Legal Protection of Consumers from the Risks of AI

Consumer legal protection, whether in Algeria or elsewhere, faces new challenges amid the rapid development of AI technologies. While current legislation seeks to keep pace with these developments, there remains scope to adapt existing laws and to develop a new legislative framework to ensure effective consumer protection against the potential risks of AI.

Two remarks frame what follows: none of the instruments below were drafted with AI specifically in mind, each extending pre-existing categories to a technology whose autonomy was not contemplated; and the comparison is meant not to transplant a foreign model wholesale, but to identify, through contrast, the specific gaps in Algerian law.

2.1. The National Legislative Framework for Protecting Consumers from the Risks of AI

Among the most important mechanisms established by the Algerian legislature for consumer protection in the digital environment is protection at the pre-contractual stage of electronic contracting particularly against deceptive and misleading electronic advertising, together with the pre-contractual information obligation followed by protection at the post-contractual stage.

2.1.1. Consumer Protection Before and After Contracting under the E-Commerce Law

The Algerian legislature has established protection for the electronic consumer through the E-Commerce Law (Law No. 18-05, 2018) against misleading electronic advertising.

Article 6(6) of Law 18-05 on Electronic Commerce provides that electronic advertising is any communication intended, directly or indirectly, to promote the sale of goods or services through electronic communications, in an appealing and attractive manner designed to attract the consumer's attention and encourage them to contract, with a view to generating financial profit (Houhou, 2006). However, an electronic supplier may present its advertising improperly, using deceptive or fraudulent methods to mislead the consumer and cause confusion regarding essential characteristics of the product (Si Youcef, 2009).

Accordingly, the Algerian legislature has established a criminal penalty for anyone who fails to respect the rules governing electronic advertising, particularly anyone rendering it deceptive or misleading a fine ranging from 50,000 to 500,000 Algerian dinars in addition to a civil dimension consisting of the victim's right to compensation (Law No. 18-05, 2018, Art. 40).

In addition to the consumer's right in relation to electronic advertising, there is the right to pre-contractual electronic information, given the lack of equivalence between the parties to such contracts, where presence is virtual and compounded by geographic distance, and where the contracted item cannot be genuinely inspected (Mahmoud, 2009).

Pre-contractual information is the supplier's obligation to inform and enlighten the consumer with comprehensive information concerning the sale carried out via the internet or any electronic means, on the basis of which the consumer freely decides whether or not to contract (Khaled, 2012).

However, a reading of Article 11 of Law 18/05 shows that the Algerian legislature did not define the electronic information obligation as such, but merely required the electronic supplier to inform the digital consumer by presenting the electronic offer in a visible, legible and comprehensible manner. A penalty was established for breach of this obligation a fine of 50,000 to 500,000 Algerian dinars and the court hearing the case may order suspension of access to all electronic payment platforms for a period not exceeding six months (Law No. 18/05, 2018, Art. 39).

As for post-contractual consumer protection, the consumer has the right to receive the goods or services within the agreed time limits. In the absence of a specific definition in the E-Commerce Law, one turns here to the general law of obligations concerning delivery of the item sold, whereby the item is placed at the buyer's disposal so that they may take possession of and use it without hindrance, even where physical delivery has not occurred (Kadada, 2000). The product may be returned to the electronic supplier if the latter fails to respect the delivery date agreed in the contract, and the supplier may be released from all or part of its liability where it is shown that non-performance, or defective performance, is attributable to the electronic consumer or to force majeure (Law No. 18/05, 2018, Art. 18(2)).

The consumer also has a right of withdrawal, whose primary purpose is to protect the genuineness of consumer consent by granting an additional period to consider and arrange the matter of the contract, pursuant to Article 11(14) of Law 18/05 referred to above. However, the legislature required the electronic supplier only to provide information concerning the conditions and time limits of withdrawal, leaving it to the supplier to regulate the right of withdrawal as to its recognition, duration and conditions of exercise (Abdel Baqi, 2008). Article 23, meanwhile, provides that the electronic supplier must take back its goods where delivery does not conform to the order or where the product is defective; the electronic consumer must return the item in its original packaging within a maximum of four working days from the date of actual delivery, stating the reason for rejection, with return costs, replacement with an equivalent item, or cancellation of the order and refund of sums paid being at the supplier's expense, without prejudice to the consumer's right to claim compensation where harm has occurred; sums paid must be refunded within 15 days from the date the product is received.

It may be concluded that Law No. 18-05 on electronic commerce, although it contains provisions concerning electronic advertising, information, receipt, service, withdrawal and the electronic commercial register, does not expressly address the use of AI systems in the provision of services or products to consumers.

This silence is significant: the rules on electronic advertising presuppose an identifiable advertiser composing a message, not a generative system that autonomously produces personalised content in real time. This does not make Law 18-05 irrelevant to AI-mediated commerce; it means its categories must be interpreted expansively, or supplemented, to protect consumers as effectively as in conventional electronic commerce.

2.1.2. Consumer Protection under the Algerian Civil Code and the Law on Consumer Protection and Fraud Suppression

(a) The Civil Code (Order No. 75-58, as amended and supplemented)

Harm arising from the use of AI techniques may be compensated, since fault is presumed by law (Shakhatouh, 2023). Article 124 of the Algerian Civil Code provides that any act whatsoever that causes harm to another obliges the person from whom the act originated to compensate for that harm.

As regards the types of compensation for harm arising from the use of AI techniques, compensation may be in kind restoration of the situation to what it was before the harm occurred, as though the harm had never taken place or compensation in the alternative, awarded by the judge where compensation in kind is not possible, taking the form of a monetary payment to the injured party commensurate with the harm suffered. This latter form is best suited to harm arising from AI use, whether paid in a lump sum or in instalments, for example as a lifetime annuity; regardless of the method of compensation, what matters is the scope of harm covered (Jordan Court of Cassation, 2018).

In discussing civil liability arising from the use of AI techniques, the claimant may be the "user" the client or consumer of computers and programs used for social, professional or personal purposes (Al-Sanhuri, 1998) who suffers harm as a result of AI use, or the programmer or another party; the claimant may also be the successor of the injured party, whether public or private.

The defendant is the party liable for contractual fault or for a harmful act, whether liable for their own act, for the act of another, or for a thing in their custody (Civil Code, Art. 132 cited in the source variously as Order No. 75-58 and Order No. 75-68), and the defendant in an action for liability arising from AI use may take several forms a programmer, an operator, a manufacturer, or an owner.

Under Algerian legislation, the central difficulty lies in its current inability to address harm arising from autonomous AI systems, since it is difficult to determine who is responsible among the developer, operator and user when a system takes an unforeseen decision. If Article 132 of the Algerian Civil Code, concerning the liability of the custodian of things, were applied to AI, the latter could be regarded as a "thing" subject to custodial liability but the question then arises: who is the custodian? The system? The owner? The user? The developer? And how is causation to be established where the decision is the product of a complex algorithm?

The same applies to the Algerian Criminal Code (Law 06-23), where Article 288 et seq. regulate criminal liability on the basis of personal fault. The difficulty is that AI lacks criminal capacity, and criminal intent cannot be attributed to it for example, if a surgical robot causes a patient's death, who is liable? The supervising surgeon? The software company? The hospital?

(b) The Law on Consumer Protection and Fraud Suppression

Algerian legislation relies on the Law on Consumer Protection and Fraud Suppression, Law No. 09-03 (Law No. 09-03, 2009), issued on 25 February 2009 and amended and supplemented by Law No. 18-09 (Law No. 18-09, 2018), dated 10 July 2018, as the basic framework for consumer protection. This law sets rules concerning the offering of goods and services for consumption, establishes controls to ensure product safety and the integrity of transactions, and includes provisions on labelling, instructions and advertising aimed at providing clear information to consumers in particular Article 9, which guarantees safety from defective products. Its application to AI software, however, encounters several difficulties, most notably:

- The impossibility of fully predicting the behaviour of an AI system.
- Self-learning, which alters the system's behaviour over time.
- The use by some Algerian banks of AI systems to assess creditworthiness: where such a system refuses to grant a loan to a person who is entitled to it, based on discriminatory data, no express provision determines liability, and proof remains difficult before the courts.

A review of several academic studies suggests that Law 09-03 on consumer protection and fraud suppression is inadequate given the rapid development of the e-commerce sector in Algeria, requiring the legislature to keep pace with this development (Roucho, 2022), particularly since Algerian legislation contains no clear legal definition of AI, which hinders the determination of applicable legal rules.

In addition, a further legislative gap exists in that industrial property laws do not provide full and comprehensive protection for AI applications, compared with literary and artistic property rights (Tarchoune, 2024). This is because the purpose of establishing a legal rule to protect an AI system is to protect the system itself, not the trademark; although an AI system may be linked to a trademark, the trademark's purpose is purely commercial marketing, and it becomes clear that rules established to protect trademarks cannot be applied to AI systems, since the system would not benefit from such protection. The Algerian legislature has implicitly, rather than expressly, brought AI protection within the scope of literary and artistic property rights, since it falls within digital works, which are protected under Order 03/05 (Order No. 03-05, 2003) on copyright and related rights.

Read together, these provisions reveal a consistent pattern: Algerian law offers meaningful, if partial, protection at each stage, yet none of it was designed around what makes AI-generated harm distinctive unpredictability, post-deployment learning, and multiple contributing actors.

2.2. Consumer Protection from AI Risks in Comparative Legislation

Studying comparative legislation is of great importance for understanding the options available to the Algerian legislature, given that the United States and the European Union adopt radically different approaches to balancing innovation and consumer protection.

These two models represent opposite starting points: should the law classify AI risk *ex ante*, or rely on *ex post* enforcement once harm has materialised? The EU has chosen the first path; the US has largely defaulted to the second. Algeria currently sits closer to the American default, if only because it has not yet adopted any *ex ante* regime at all.

2.2.1. The European Union

The European Union has established an ambitious legal framework to protect consumers from the risks of AI, resting on three complementary pillars: preventing dangerous practices, imposing strict transparency rules, and facilitating compensation for injured parties making it the most advanced system of its kind in the world.

The EU AI Act is the world's first comprehensive legal framework for AI. It regulates the development and/or use of AI within the European Union and entered into force on 1 August 2024. The Act adopts a risk-based regulatory approach, applying different rules to AI according to the risk it poses (prohibited, high, limited, minimal) to ensure safety, transparency and respect for human rights, with a ban on dangerous practices applying from February 2025.

The Act also sets certain rules for general-purpose AI models, such as IBM's open-source foundation model "Granite" and Meta's "Llama 3" model (IBM, n.d.-b).

Penalties can range from €7.5 million or 1.5% of worldwide annual turnover to €35 million or a corresponding percentage of worldwide annual turnover, depending on the type of non-compliance. In the same way that the EU's General Data Protection Regulation (GDPR) inspired other countries to adopt data-privacy laws (IBM, n.d.-c), experts expect the EU AI Act to spur the development of AI governance and ethics standards worldwide.

The EU AI Act applies to:

- Providers: persons or institutions that develop an AI system or a general-purpose AI model (GPAI), or that have it developed on their behalf, and that place it on the market or provide the AI system as a service under their name or trademark. For example, where the foundation model is a general-purpose AI model, a chatbot (IBM, n.d.-d) or generative AI tool (IBM, n.d.-e) built on that model would itself constitute an AI system.
- Deployers: persons or institutions that use AI systems for example, an institution using a third-party AI-powered chatbot to handle customer-service queries.
- Importers: persons and institutions established in EU member states that bring to the EU market AI systems belonging to a person or company established outside the EU.

The Act also applies to providers and deployers outside the EU where they use their AI, or AI outputs, within the EU. Providers outside the EU offering AI services within the EU must appoint authorised representatives within the EU to coordinate compliance efforts on their behalf.

The exceptions to the Act's application are cases of purely personal use of AI and its models, and systems used solely for scientific research and development.

The EU AI Act has entered into force progressively: the ban on certain practices took effect on 2 February 2025, aimed at preventing uses that violate fundamental rights. Among the practices prohibited outright

are (European Parliament, 2024): biometric categorisation systems based on sensitive characteristics; the indiscriminate scraping of facial images from the internet or CCTV footage to build facial-recognition databases; emotion recognition in workplaces and schools; social scoring evaluating individuals on the basis of their social behaviour and using that evaluation against them in unrelated contexts; predicting criminal behaviour where based solely on profiling a person or assessing their characteristics; and AI that manipulates human behaviour through deceptive or coercive means that weaken a person's capacity to make an informed decision, or that exploits individuals' vulnerabilities, such as those of children, persons with disabilities, or persons in difficult economic circumstances.

There are also limited-risk applications requiring that users be informed they are dealing with a machine (such as a chatbot), and minimal- or no-risk applications, such as spam filters, which are not subject to significant restrictions; high-risk applications (such as recruitment, education and healthcare applications) are subject to strict restrictions, whose provisions take effect from August 2026.

The EU AI Act also imposes transparency requirements: general-purpose AI (GPAI) systems and the models underlying them must meet certain transparency requirements, including compliance with EU copyright law and the publication of detailed summaries of content used in training. More powerful general-purpose AI models that may pose systemic risks face additional requirements, including model evaluations, systemic risk assessment and mitigation, and incident reporting; artificial or manipulated image, audio or video content must also be labelled. These provisions (the general-purpose model rules) took effect from August 2025.

The Act also provides measures to support innovation and small and medium-sized enterprises: national regulatory sandboxes and real-world testing must be established and made available to SMEs and start-ups to develop and train innovative AI before bringing it to market.

As regards compensating injured parties, the updated Product Liability Directive (PLD) is the principal instrument: a compensation claim may be brought directly against the developer where AI software causes harm to a consumer, benefiting from a reduced burden of proof in complex cases (EY Law, n.d.). However, proving fault or causation in AI cases remains complex, which is why consumer-protection organisations such as BEUC have called on the Commission to begin immediately drafting new rules to fill this gap and ensure that victims do not face significant difficulty in obtaining their rights (Leonte, 2025).

The AI Act classifies systems by degree of risk, with escalating penalties:

- Unacceptable (prohibited) risk: dangerous practices classified under Article 5 of the AI Act (manipulation, exploitation, social scoring); penalties for non-compliance can reach €35 million or 7% of annual worldwide turnover.
- High risk: systems affecting safety or fundamental rights (employment, credit, education); penalties can reach €15 million or 3% of annual worldwide turnover.
- Limited risk: interactive systems (chatbots), which need only comply with transparency requirements; penalties vary according to the degree of risk and impact.

- Minimal risk: applications such as spam filters or ordinary video games, for which there are no penalties, though adherence to voluntary codes of conduct is recommended.

What distinguishes the European approach, finally, is that it does not leave consumer protection to judicial interpretation alone, but imposes clear, direct rules on designers and marketers before any product is placed on the market. The revised Product Liability Directive, in force since 1985 and updated in November 2024 with application extending to March 2026, treats software and AI as "products" for this purpose although it currently suffers from a temporary gap regarding ease of compensation, owing to the withdrawal in 2025 of the dedicated liability legislation (the AI Liability Directive, AILD), a 2022 proposal to facilitate proof of causation for high-risk systems that was abandoned after the European Commission announced it could not secure sufficient consensus.

Algeria could follow the European model in prohibiting dangerous practices in particular.

Beyond its specific prohibitions, the European model offers a template for translating the four principles discussed earlier into a single, coherent instrument rather than scattered rules though its compliance costs could burden smaller domestic actors disproportionately absent comparable sandbox support.

2.2.2. The United States

In the United States, legal protection for consumers against AI risks is developing through a combination of federal legislation and state laws. There is as yet no comprehensive federal law regulating AI, resulting in what is known as a "regulatory patchwork," where requirements differ by state and sector. The United States relies on enforcing existing laws against deceptive and discriminatory practices while leaving room for innovation.

(a) State laws

In the absence of any comprehensive federal law, US states have emerged as the principal legislative actors, with California, as usual, leading the field (Data Management University, 2026) and rapidly becoming the de facto national standard. The California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA) regulate data, the lifeblood of AI. The CCPA, which entered into force on 1 January 2020, established a core set of consumer privacy rights for California residents, granting them broad rights over any personal information held by companies, including the right to access, delete and correct their data, and to opt out of its sale or sharing.

The California Privacy Rights Act (CPRA) entered into force on 1 January 2023 and amended and significantly expanded the CCPA, adding new rights and establishing a dedicated enforcement agency.

On 29 September 2025, California enacted the landmark AI Transparency Act (SB 53), requiring developers of large frontier AI models to disclose detailed safety protocols, risk-assessment procedures and measures taken to prevent misuse of their AI systems or harmful outcomes; the law targets companies developing highly capable AI systems to ensure accountability and build public trust.

Utah's AI Policy Act (SB 149) focuses on transparency by requiring clear and conspicuous disclosure when generative AI is used to interact with consumers. New Hampshire's House Bill 1432 criminalises the fraudulent use of deepfake technology, and South Dakota's Senate Bill 79 criminalises the use of AI to generate computer-based child sexual abuse material.

Texas's Responsible AI Governance Act (TRAIGA), which entered into force on 1 January 2026, establishes a comprehensive legal framework governing the ethical development, deployment and use of AI systems in Texas, and prohibits the use of AI systems designed for harmful purposes.

New York City's Local Law 144, on Automated Employment Decision Tools, which entered into force on 5 July 2023, regulates the use of AI and machine-learning tools in employment decisions such as hiring and promotion, requiring employers to conduct bias audits of the tools used, notify job applicants or employees of their use, disclose the data sources and functions of the tools, and provide alternatives or accommodations on request, so as to ensure transparency, integrity and accountability throughout decision-making.

Many other states have established regulatory sandboxes and frameworks encouraging innovation while preserving privacy and civil rights, reflecting a growing patchwork of AI governance at state level a direct result of the total absence of comprehensive federal AI legislation. At state level, legislative activity has accelerated markedly: 38 states enacted around 100 AI-related laws in 2025 alone. The trend suggests that states favour transparency and user-directed disclosures over imposing excessive compliance requirements, while gradually developing accountability mechanisms, particularly regarding fairness and anti-discrimination.

Colorado's AI Act (SB 205, the "CAIA") imposes obligations on developers and deployers of AI systems, particularly those considered high-risk, with a focus on avoiding algorithmic discrimination (Colorado General Assembly, 2024). It will enter into force in June 2026, together with obligations to notify consumers when a system is used against them and to grant them rights to correct data and appeal decisions; violations are punishable by fines of up to \$20,000 per violation.

(b) Federal legislation

The Federal Trade Commission (FTC) plays a role in enforcing federal competition and consumer-protection laws, which prohibit anti-competitive, deceptive and unfair commercial practices, including those relating to AI (U.S. Federal Trade Commission, n.d.); the Commission has launched investigations into AI-powered chatbots to understand how companies measure, test and monitor them for potential risks. The US administration has also issued executive orders aimed at regulating AI, focusing on balancing innovation with protecting users and society from risk (Al-Sayed, 2023). These orders include encouraging transparency and watermarking AI-generated content, and conducting tests on advanced systems.

The American model is characterised by flexibility and speed in penalising overt fraud while avoiding the stifling of innovation through rigid rules, but it suffers from considerable legal fragmentation, since laws differ from state to state, and existing laws may not be sufficient to address the complexities of AI, particularly regarding "unintentional discrimination" or the difficulty of proving harm in court. This places the United States in a position quite different from the European Union, which favours comprehensive, proactive regulation.

Algeria could also draw on the American model in activating existing consumer-protection laws, while adding a requirement to disclose the use of AI in services provided to citizens.

The American experience shows that AI-specific consumer protection can emerge incrementally, provided a well-resourced enforcement authority polices unfair practices and some jurisdictions legislate ahead of the rest, as California and Colorado have done. Algeria would need to pursue such reform nationally and designate which authority is responsible for enforcement a question current legislation leaves open.

Conclusion

Achieving a balance between innovation in AI and consumer protection requires a multi-faceted approach combining effective legislation, responsible business practices, and greater consumer awareness.

AI represents a transformative force with immense potential, but for society to benefit from it fairly, potential risks such as algorithmic bias, privacy violations, misinformation and discrimination must be addressed.

It is clear, in conclusion, that the greatest challenge facing legislators and policymakers in the era of digital transformation is not merely keeping pace with the rapid development of AI technologies, but achieving a precise balance between encouraging technological innovation and ensuring effective consumer protection. The various legislative models examined here the European model, based on risk classification, and the American model, based on the enforcement of existing laws all agree that the principles of algorithmic fairness and accountability form the cornerstone of any successful legal system.

The concept of "fair AI" requires more than the mere absence of explicit discrimination: it calls for ensuring that algorithmic decisions are transparent, explicable, and subject to human oversight where necessary. "Responsibility," in turn, means clearly identifying who bears liability when harm is caused to the consumer whether developer, operator or distributor together with effective mechanisms for establishing causation and providing swift compensation.

The current Algerian legislature suffers from an insufficiency of legal texts protecting consumers from the risks of AI: although existing laws form a solid foundation, they were not designed to keep pace with these evolving technologies. It has therefore become necessary for the Algerian legislature to take the initiative in closing this legislative gap, drawing on international trends such as the European model, while taking account of the specificity of the national context and balancing the encouragement of innovation with the protection of consumer rights.

Ultimately, legal consumer protection remains a merely theoretical framework unless accompanied by effective oversight mechanisms, investment in judicial and technical capacity-building, and awareness campaigns informing consumers of their rights and of the risks of these technologies. The road ahead is long, but beginning now to close the legislative gaps is the genuine investment in a fairer and safer digital future for all.

Three findings deserve to be underlined. First, fairness and accountability are, or ought to be, organising principles of consumer law in the age of AI, much as good faith organised it in the age of standard-form contracting. Second, there is no single correct regulatory technique: the EU's *ex ante* classification and the US's *ex post* enforcement both achieve real, if imperfect, protection. Third, existing Algerian instruments were not built to answer what autonomous systems now ask who is an algorithm's custodian, how is causation proven and answering them will require deliberate legislative choices.

Recommendations

- Developers and deployers of AI systems should provide transparent reports on how these systems operate, including the data sources used, their limitations, and how decisions are made; such reporting should be standardised across sectors so that consumers and regulators can compare disclosures meaningfully rather than relying on each operator's own format.
- Clear rules for accountability should be established, identifying liability in the event of harm resulting from AI use, whether material or moral, and specifying, as between developer, distributor and end-user, who bears the burden of proving or disproving fault where a system's decision-making process cannot be fully reconstructed after the fact.
- Diversity should be ensured within AI development teams to represent varied backgrounds, helping to identify and address potential biases before a system is deployed rather than after consumers have already been affected.
- Robust data-governance practices and safeguards should be applied to protect end-user privacy and sensitive data, building on and extending the data-minimisation and informed-consent principles already recognised, in embryonic form, in existing Algerian legislation.
- Consumer awareness and education programmes should be developed on how AI systems work, their potential risks, and how to use them safely and responsibly, targeting in particular the categories of consumers the elderly, persons with disabilities, and those with limited digital literacy shown by comparative studies to be most exposed to AI-related harm.
- Ethical practices in AI development should be strengthened through sector-specific codes of conduct developed in consultation with consumer-protection bodies, so that ethical commitments are not left solely to the discretion of individual economic operators.
- Clear legislation and regulations should be developed governing the design, development, deployment and use of AI systems, with a focus on consumer protection; such legislation should, at a minimum, provide a legal definition of AI for the purposes of Algerian law, designate a competent enforcement authority, and clarify the allocation of liability along the AI value chain, so as to close the specific gaps identified in this study.

References

- Abdel Baqi, O. M. (2008). *La protection contractuelle du consommateur: Étude comparée entre la charia et la loi*. Dar Mansha't al-Maarif.
- Al-Naqib, M. (2024, February 16). *Technology on the scales of justice: Advancing AI with an ideal balance in consumers' favour* [In Arabic]. malwaemal.com
- Al-Sanhuri, A. R. A. (1998). *Al-Wasit fi sharh al-qanun al-madani* (Part 7, Vol. 2, General theory of obligations: Sources of obligation). Dar Ihya al-Turath al-Arabi.
- Al-Sayed, K. A. R. (2023, November 12). The United States issues regulations to govern artificial intelligence. *Al-Sharq Newspaper*. <https://al-sharq.com/opinion/12/11/2023/...>
- Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review*, 104(3), 671–732. <https://doi.org/10.2139/ssrn.2477899>

- Bartlett, Robert & Morse, Adair & Stanton, Richard & Wallace, Nancy, 2022. "Consumer-lending discrimination in the FinTech Era," *Journal of Financial Economics*, Elsevier, vol. 143(1), pages 30-56. <https://ideas.repec.org/a/eee/jfinec/v143y2022i1p30-56.html>
- Calais-Auloy, J., Temple, H., & Dépincé, M. (2020). *Droit de la consommation* (10th ed.). Dalloz.
- CNIL. (2024). *Deliberation SAN-2024-012: Sanction against financial institution for algorithmic discrimination*. Commission Nationale de l'Informatique et des Libertés.
- Colorado General Assembly. (2024). *Consumer Protections for Artificial Intelligence Act*, Senate Bill 24-205. <https://leg.colorado.gov/bills/sb24-205>
- Crawford, K. (2021). *The atlas of AI: Power, politics, and the planetary costs of artificial intelligence*. Yale University Press.
- Data Management University. (2026, March 19). *AI regulations in the USA: What businesses need to know*. <https://www.ewsolutions.com/ai-regulations-in-the-usa-what-businesses-need-to-know/>
- Edelman Trust Barometer. (2025). *Special report: AI and consumer trust*. <https://www.edelman.com/trust/2025/trust-barometer>
- European Commission, High-Level Expert Group on AI. (2019). *Ethics guidelines for trustworthy AI*. <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>
- European Law Institute. (2025). *ELI model rules on digital assistants and consumer contracts*. <https://www.europeanlawinstitute.eu/news-events/upcoming-events/events-sync/news/eli-publishes-guiding-principles-and-model-rules-on-digital-assistants-for-consumer-contracts/>
- European Parliament. (2024, March 8). *Artificial intelligence act: MEPs adopt landmark law* [Press release]. europarl.europa.eu/news/en/press-room/20240308JPR19018
- European Parliament. (2025). *EU AI Act: Regulation (EU) 2025/1689*. Official Journal of the European Union. <https://eur-lex.europa.eu/legal-content/TR/LSU/?uri=CELEX:32024R1689>
- Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.
- EY Law. (n.d.). *Prepare your company: The EU's revised Product Liability Directive brings new challenges*. <https://www.eylaw.be/insights/prepare-your-company-the-eus-revised-product-liability-directive-brings-new-challenges>
- Fastercapital.com. (n.d.). *Consumer AI: Overcoming the ethical challenges of consumer AI adoption* [In Arabic]. fastercapital.com/arabpreneur
- Floridi, L., & Cowls, J. (2022). A unified framework of five principles for AI in society. *Harvard Data Science Review*, 4(1), 1–15. <https://doi.org/10.1162/99608f92.8cd550d1>
- Gartner Research. (2025). *Predicts 2026: AI in customer service and support*. <https://www.gartner.com/en/newsroom/press-releases/2025-12-17-customer-service-and-support-leaders-must-prioritize-blending-human-strengths-with-ai-intelligence-in-2026>
- Gillespie, T. (2024). *Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press.

- Google Research. (2025). *Debiasing techniques in large language models: Impact on accuracy and fairness*. <https://research.google/blog/google-research-2025-bolder-breakthroughs-bigger-impact/>
- Hickok, M. (2023). Accountability by design: A framework for responsible AI. *AI and Ethics*, 3, 1–14.
- Houhou, Y. (2006). *Le contrat de vente électronique en droit algérien*. Dar Belkis.
- IBM. (n.d.-a). *What is responsible AI?* IBM Think Topics. <https://www.ibm.com/think/topics/responsible-ai>
- IBM. (n.d.-b). *What is the EU AI Act?* IBM Think Topics. <https://www.ibm.com/think/topics/eu-ai-act>
- IBM. (n.d.-c). *What is data privacy?* IBM Think Topics. <https://www.ibm.com/think/topics/data-privacy>
- IBM. (n.d.-d). *What is a chatbot?* IBM Think Topics. <https://www.ibm.com/think/topics/chatbots>
- IBM. (n.d.-e). *What is generative AI?* IBM Think Topics. <https://www.ibm.com/think/topics/generative-ai>
- International Organization for Standardization. (2024). *Artificial intelligence management system (ISO/IEC 42001:2024)*. <https://www.infosectrain.com/courses/iso-iec-42001-lead-implementer-training>
- Jean, A. (2021). *Les algorithmes font-ils la loi?* Éditions de l'Observatoire.
- Johnson, E., & Smith, E. (2024). Fairness perceptions and consumer loyalty in AI-driven services. *Journal of Consumer Research*, 51(3), 412–428.
- Khaled, K. S. A. (2012). *La protection du consommateur électronique* (1st ed.). Dar Al-Jamiaa Al-Jadida.
- Leonte, R. (2025, April 30). *The quiet exit of the AI Liability Directive*. GNP. gnp.ro
- Mahmoud, A. D. A. (2009). *Consumer protection in electronic contracting: A comparative study* [Unpublished master's thesis]. An-Najah National University.
- Microsoft Accessibility. (2025). *State of AI accessibility: Consumer perspectives*. Microsoft Corporation.
- Obermeyer, Z., et al. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. *Science*, 366(6464), 447–453. <https://doi.org/10.1126/science.aax2342>
- OECD. (2019). *Recommendation of the Council on Artificial Intelligence* (OECD/LEGAL/0449). <https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449>
- OECD. (2024). *Explanatory memorandum on the updated OECD AI principles*. [OECD Publishing](https://www.oecd.org/publishing/).
- Kadada, K. A. H. (2000). *Al-Wajiz fi sharh al-qanun al-madani al-jazairi* (Part 4, Contract of sale). Diwan al-Matbouat al-Jamiiya.

- Roucho, A. (2022). Legal protection of the electronic consumer under Algerian legislation. *Chuaa Journal of Economic Studies*, 6(2), 457–468. <https://asjp.cerist.dz/en/article/201068>
- Shakhathouh, H. J. M. (2023). *Legal protection of the consumer under the use of AI technology* [Conference presentation]. Fourth International Conference on Legal and Political Frameworks for Good Governance, Jadara University, Jordan. https://www.researchgate.net/publication/376757680_To_legally_protect_the_consumer_under_the_use_of_artificial_intelligence_technology
- Si Youcef, Z. H. (2009). *La responsabilité civile du producteur*. Dar Houma.
- Tarchoune, I. (2024). Protection of artificial intelligence through industrial property rights law. *Academic Journal of Legal Research*, 15(1), 88–99. <https://asjp.cerist.dz/en/article/248734>
- U.S. Federal Trade Commission. (n.d.). *Artificial intelligence*. <https://www.ftc.gov/industry/technology/artificial-intelligence>
- University of California, Berkeley Center for Law & Technology. (2025). *Algorithmic bias in mortgage lending: A longitudinal study*.
- uxwritingar.com. (n.d.). *Strategies for leveraging AI in customer service* [In Arabic]. uxwritingar.com/customer-experience/35388
- Zou, J., & Schiebinger, L. (2018). AI can be sexist and racist – it's time to make it fair. *Nature*, 559, 324–326. <https://doi.org/10.1038/d41586-018-05707-8>

Legal sources

Algeria

- Civil Code, Art. 132 (Order No. 75-58 of 26 September 1975, as amended and supplemented; cited elsewhere in sources as Order No. 75-68).
- Order No. 03-05 of 19 July 2003 on Copyright and Related Rights. Official Gazette, (44).
- Law No. 09-03 of 25 February 2009 on Consumer Protection and Fraud Suppression. Official Gazette, (15).
- Law No. 18-05 of 24 Sha'ban 1439 AH / 10 May 2018 on Electronic Commerce. Official Gazette, (28).
- Law No. 18-09 of 10 July 2018 amending and supplementing Law No. 09-03. Official Gazette, (35).
- Criminal Code (Law No. 06-23).
- **European Union**
- European Parliament. (2020). Resolution of 20 October 2020, "Digital Services Act: Improving the Functioning of the Single Market" (2020/2018(INL)).
- European Parliament. (2021). Resolution of 20 May 2021, "Shaping the Digital Future of Europe" (2020/2216(INL)).

- European Commission. (2021). Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), COM(2021) 206 final.
- Regulation (EU) 2025/1689 on Artificial Intelligence (EU AI Act).
- Commission Nationale de l'Informatique et des Libertés. (2024). Deliberation SAN-2024-012.

United States

- California Consumer Privacy Act (CCPA) (2018) (effective January 1, 2020).
- California Privacy Rights Act (CPRA) (2020) (effective January 1, 2023).
- California Senate Bill 53, AI Transparency Act (2025).
- Colorado Senate Bill 24-205, Colorado AI Act ("CAIA") (2024).
- New Hampshire House Bill 1432.
- New York City Local Law 144, Automated Employment Decision Tools (2023).
- South Dakota Senate Bill 79.
- Texas Responsible AI Governance Act (TRAIGA) (2026).
- Utah Senate Bill 149, AI Policy Act.

Case law

- Jordan Court of Cassation (Civil Chamber). (2018). Ruling No. 4443/2018 (October 25, 2018).