



Legal Security in the Age of Artificial Intelligence: Challenges and Prospects

FATIHA NAAR

Faculty of Law and Political Sciences, Mouloud Mammeri University - Tizi Ouzou, Algeria

fatiha.naar@ummto.dz

Submission 24.06.2026

Acceptance: 13.09.2026

Publication: 02.10.2026

Abstract

This study examines the issue of legal security in the face of radical changes driven by rapid technological advancement and artificial intelligence applications. It is based on the premise that the stability of legal situations and legitimate expectations are now threatened by challenges inherent to the digital environment—specifically, the widening time lag between legislative drafting and technical innovation, the difficulty of legally classifying autonomous systems, and issues surrounding cyber sovereignty and data protection) by combining doctrinal analysis of Algerian and comparative law. Addressing these challenges, the study explores future prospects for ensuring legal certainty by advocating a shift toward "dynamic legislation," the internationalization of technology-related rules, and the implementation of proactive oversight mechanisms and digital ethics to complement statutory law; the aim is to develop a balanced legal approach that protects rights and legal situations without stifling technological progress.

Keywords: Legal security, artificial intelligence, technological development, modern technologies, challenges.

Introduction

The contemporary world is experiencing unprecedented technological growth, propelling societies into the era of widespread digitization and transforming the traditional environment of transactions into a virtual space characterized by the rapid flow of information and borderless globalization. While law serves as the instrument for regulating social activity and guaranteeing its stability, this major technological revolution—with all its constantly accelerating technologies—has created a new legal reality marked by a temporal and cognitive gap between the speed of technological innovation and the slowness of traditional legislative development. This disparity puts contemporary legal systems to the test and strikes at the very heart of their protective function.

Faced with this rapid transformation Faced with this rapid transformation Faced with this rapid transformation, countries have an imperative to evolve their legal systems to keep pace with rapid technological advancements and overcome the obstacles and challenges that hinder the development and enforcement of laws. At the same time, the principle of legal security stipulates that the acquired rights and legal status of individuals, recognized constitutionally



and legally, must not be affected under any circumstances, whether by annulment or modification. This principle is considered a cornerstone of the rule of law and the guarantee of the stability of legal positions. Legal certainty compels legislators to formulate rules characterized by clarity, relative stability, and predictability, thus enabling individuals to plan their actions and anticipate the legal consequences of their obligations without surprise or legislative ambiguity. However, the intrusion of technology into legal relations has brought about a conceptual upheaval, but it also carries risks that could affect the fundamental rights and freedoms of individuals.

This observation is particularly significant given that Artificial intelligence (AI) has moved from laboratories into courts, administrations, markets and private communications. Algorithms now price credit, triage public services, inform sentencing and generate evidence-like content, while smart contracts execute obligations without human intervention. Law, whose social function is to make conduct and its consequences foreseeable, is thus confronted with a technology that changes faster than legislation and whose internal logic is often opaque even to its designers. This tension concerns the core of **legal security**: the requirement that legal rules be accessible, intelligible, stable and predictable so that individuals can plan their conduct and rely on acquired rights. The Algerian constitution-maker has expressly adopted the principle: under Article 34 of the 2020 Constitution, the State, in legislating on rights and freedoms, must ensure the accessibility, readability and stability of legislation in order to guarantee legal securityⁱ.

In this context, problem is therefore: to what extent can contemporary legal systems reconcile the need to keep pace with AI with the requirements of legal security?

To address this question, it is necessary to examine the challenges of legal security in the face of artificial intelligence by outlining its scope and the associated challenges (first topic), and then to highlight the prospects and standards aimed at improving legal security within the digital environment (second topic).

First Topic:

Legal security in the face of artificial intelligence: content and challenges

Legal security represents the fundamental legislative bedrock that guarantees the stability of legal positions and protects the legitimate expectations of individuals and entities through clear, stable, and predictable laws. However, with the rapid proliferation of Artificial Intelligence (AI) as a disruptive technological phenomenon, this well-established legal framework finds itself in a direct confrontation with a novel digital reality that challenges traditional legal doctrines. AI systems, characterized by autonomous decision-making and self-learning capabilities, enforce a new paradigm that often transcends existing statutory laws, thereby forcing legal security to re-examine its core concepts and adapt its regulatory mechanisms.



To comprehensively analyze how the legal system addresses this evolving reality, this section is systematically divided into two main sections. The first section delineates the content and conceptual framework of legal security under smart technological environments. Building upon this conceptual foundation, the second section analyzes the prominent legal challenges posed by artificial intelligence.

First Section: The principle of legal security and its requirements

The principle of legal certainty extends beyond the mere framework of a rigid legislative rule to become a comprehensive legal philosophy aimed at ensuring the quality of legal texts and rationalizing their effects. Examining this principle requires an analysis across two dimensions: the legislative approach (A), and jurisprudential concepts that define its essence and fundamental dimensions (B).

A- The principle of legal security

Legal security is a structural principle of the rule of law. In Fuller's account, law fails as a system when its rules are not promulgated, are unclear, contradictory, retroactive or changed so frequently that subjects cannot orient their action by themⁱⁱ. Raz likewise locates the virtue of the rule of law in the capacity of rules to guide conduct, which presupposes that they are prospective, open, clear and relatively stableⁱⁱⁱ. The European Court of Human Rights translated these requirements into the "quality of law" test: a norm must be adequately accessible and formulated with sufficient precision to enable citizens to foresee, to a degree that is reasonable in the circumstances, the consequences of a given action^{iv}. The French Council of State warned in 2006 that the proliferation, instability and poor drafting of norms had become a structural threat to legal certainty^v.

Algerian doctrine has received these requirements and emphasized three dimensions: the clarity and intelligibility of rules, their relative stability, and the protection of legitimate expectations and acquired rights. The constitutionalization of the principle in 2020 turns it into an obligation addressed to the legislator^{vi}. In the digital environment, this obligation acquires a new object: not only the text of the law but also the technical systems through which law is increasingly applied, since a decision produced by an opaque algorithm may be as unforeseeable for its addressee as an unpublished rule^{vii}.

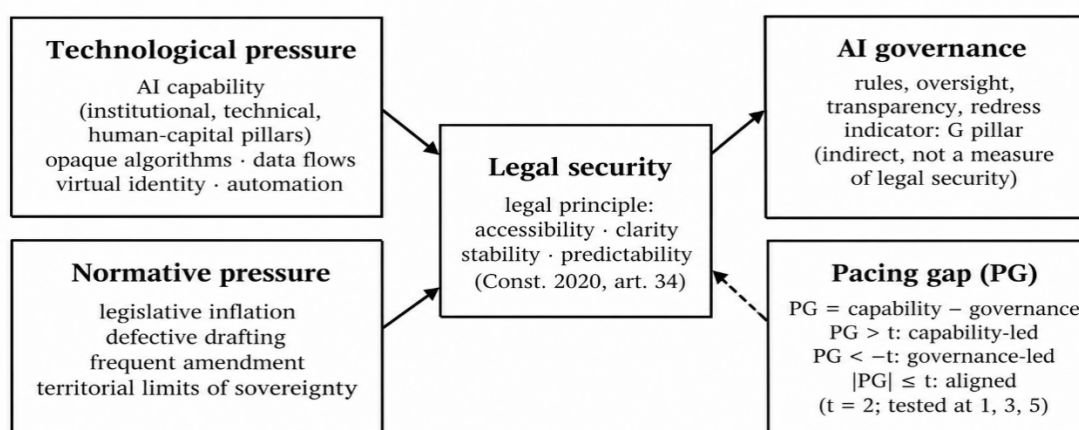
B- From doctrine to measurement: concepts and hypotheses

Three concepts must be kept apart. **Legal security** is a legal principle concerning the qualities of the legal order (accessibility, clarity, stability, foreseeability). **AI governance** is an institutional and regulatory concept: the set of rules, authorities and procedures through which a state steers and controls AI. The **governance and safeguards pillar (G)** of the Global AI Index is an empirical indicator of the second, defined by the source as enforceable rules,



independent oversight, transparency obligations and redress mechanisms^{viii}. G is used here as an **indirect indicator of institutional conditions relevant to legal security**: enforceable rules and transparency relate to accessibility and foreseeability, and oversight and redress to contestability. It does not measure the clarity, stability or quality of legal texts, and a high G score does not show that legal security is achieved. The doctrinal analysis suggests that legal security is threatened when these conditions lag behind the technological capacity deployed in society; the pacing-problem literature predicts such a lag^{ix}, whereas the governance literature stresses institutional and regulatory factors^x and research on governance indicators suggests that the general quality of legal institutions conditions the capacity to adopt and enforce safeguards. Figure 1 summarizes this framework, which motivates the operational concept of the **pacing gap (PG)**: AI capability minus governance.

Figure 1: Analytical framework linking technological and normative pressures, legal security and the governance response



Source: Authors' elaboration. Dashed box: the empirical indicator used in Section II (indirect, not a measure of legal security)

Second Section: Challenges Posed by artificial intelligence:

The integration of intelligent algorithms into all aspects of economic, social, and judicial life has led to a structural disruption of established concepts; the rules of tort liability, theories of legal personality, and even mechanisms for protecting privacy and intellectual property are no longer able to accommodate the hybrid nature of these technologies.

The integration of intelligent algorithms into all aspects of economic, social and judicial life has led to a structural disruption of established concepts; the rules of tort liability, theories of legal personality and even mechanisms for the protection of privacy and intellectual property are no longer able to adapt to the hybrid nature of these technologies.



Consequently, legal security today faces a dual challenge: on the one hand, the legislative vacuum that fail to keep pace with rapid technological developments (A); on the other hand, the ambiguity of the machine, or black box phenomenon, which threatens transparency and procedural justice (B).

A- Normative challenges: inflation, defective drafting and instability

Achieving the principle of legal security is hindered by a set of challenges related to legal rules or legislative texts. These challenges are represented in the phenomenon of legislative inflation (1), defective legal drafting, or the use of drafting that carries different inaccurate interpretations (2), in addition to the possibility of legal texts being changed and amended (3).

1- Legislative inflation. Under the pressure of technological urgency, legislators tend to multiply sectoral texts. The risk is less a legislative vacuum than a saturation of fragmented rules that overlap and become difficult to know^{xi}. In Algeria, the digital field is regulated by successive special laws, each tied to a component of legal security: Law No. 09-04 on the prevention of offences related to information and communication technologies (ICT) (enforceability)^{xii}; Law No. 15-03 on the modernization of justice, which organizes electronic procedures (procedural foreseeability)^{xiii}; Law No. 18-05 on electronic commerce (transactional security)^{xiv}; Law No. 18-07 on personal-data protection, which created an independent national authority (art. 22) and therefore a channel of redress^{xv}; and Law No. 26-02 on trust services and electronic identification (identification and proof)^{xvi}. None of these texts is specific to AI, and their existence does not by itself show that legal security is achieved: their articulation with the general rules of civil, commercial and criminal law must be solved case by case^{xvii}.

2- Defective drafting. Legal security requires terms precise enough to be applied predictably. Technological legislation is exposed to vague or rapidly obsolete concepts (“automated system”, “platform”, “intelligent processing”). Bennett Moses shows that regulating “technology” as such is a structural source of ambiguity, because rules drafted around a particular technical configuration quickly become over- or under-inclusive^{xviii}. Vague drafting shifts normative choices to administrative and judicial interpretation^{xix}.

3- Instability of texts. Digital laws are amended or replaced at a pace that strains the stability component of legal security. Law No. 18-07 was substantially amended and supplemented by Law No. 25-11 of 24 July 2025^{xx}, and Law No. 15-04 on electronic signature and certification^{xxi} was repealed, eleven years after its adoption, by Law No. 26-02 of 17 February 2026^{xxii}. Such reforms are legitimate responses to technological change, but they illustrate the dilemma identified by Collingridge: early in a technology's life the law lacks information to regulate it well, whereas later the technology is entrenched and harder to change^{xxiii}. A doctrinal answer, developed in Section II, is to separate stable framework principles from technical rules that can



evolve through secondary instruments.

B- Technological challenges: opacity, sovereignty and digital identity

The challenge posed by digital technology appears as a major obstacle threatening the stability of the legal framework, creating a significant gap between the speed of technological innovation and the slowness of traditional legislation, and thus testing the concept of "legal security". Indeed, these unprecedented challenges have forced legal systems to rethink their traditional approaches. These challenges are linked to various technological factors, such as a lack of familiarity with the technical skills required by modern technologies, due to a lack of transparency and the presence of opaque algorithms (1), as well as inability national sovereignty in the face of data globalization (2), and the crisis of virtual identity and the difficulty of establishing digital evidence (3).

1- Algorithmic opacity and the limits of a “right to explanation”. Machine-learning systems produce outputs whose internal reasoning is not transparent to users, judges or even designers^{xxiv}. When such systems inform recidivism assessments, as in *State v. Loomis*, the defendant cannot fully contest the basis of a decision that affects liberty^{xxv}. EU law responds through several distinct mechanisms, which should not be conflated. **Rights to information:** the GDPR requires controllers to provide “meaningful information about the logic involved” in automated decision-making^{xxvi}; the Court of Justice of the European Union (CJEU) has held that this requires an explanation of the procedure and principles actually applied, with any trade secrets weighed by the supervisory authority or court^{xxvii}. **A qualified restriction on automated decisions:** Article 22 GDPR gives the data subject a right not to be subject to a decision based *solely* on automated processing, including profiling, that produces legal or similarly significant effects; it admits exceptions (contract, authorization by law, explicit consent) and, in the first and third cases, requires safeguards including at least the right to obtain human intervention, to express one's point of view and to contest the decision^{xxviii}. It is therefore not a general prohibition of automated decision-making; the CJEU has nonetheless read “decision” broadly, covering a credit score on which a third party draws strongly^{xxix}. Whether these provisions amount to a general “right to explanation” remains contested^{xxx}. **Transparency and human-oversight duties** under the AI Act, which requires providers of high-risk systems—including systems intended to assist judicial authorities—to supply instructions enabling deployers to interpret outputs and to design systems for effective human oversight.)^{xxxi}. **An explanation right for individual decisions:** affected persons may obtain clear and meaningful explanations of the role of a high-risk system in a decision that produces legal or similarly significant effects^{xxxii}. **Redress**, including complaints to market-surveillance authorities^{xxxiii}. The timetable matters for legal security: Regulation (EU) 2026/1744 postponed the application of the obligations for Annex III high-risk systems to 2 December 2027 and for Annex I systems to 2 August 2028^{xxxiv}, which defers the practical reach of mechanisms and.



Opacity thus threatens the predictability and contestability dimensions of legal security, and the legal response consists of converting technical properties—traceability, explainability—into enforceable, but carefully delimited, obligations^{xxxv}. It also complicates the attribution of civil liability for harm caused by autonomous systems^{xxxvi}.

2- The erosion of territorial sovereignty. Data flows and digital services disregard borders, while enforcement remains largely territorial. Cyber-attacks routed through several jurisdictions raise conflicts of jurisdiction that weaken the deterrent function of national law^{xxxvii}. Large platforms act as private regulators through their terms of service, and the EU's capacity to externalize its standards—the “Brussels effect”—means that the rules governing AI in one jurisdiction may in practice be set elsewhere^{xxxviii}, which intensifies regulatory competition^{xxxix}. International instruments differ in legal force. The Council of Europe Framework Convention (CETS No. 225) is the only **legally binding** international treaty on AI; it binds only its parties and enters into force after five ratifications, including three member States of the Council of Europe^{xl}. By contrast, the OECD Recommendation on AI (revised in 2024) and the UNESCO Recommendation on the Ethics of AI are **non-binding recommendations**^{xli}; United Nations General Assembly resolution 78/265 is a **non-binding** political commitment^{xlii}, and resolution 79/325 creates **institutional soft-law** mechanisms—an independent international scientific panel and a global dialogue on AI governance—without binding obligations^{xliii47}; corporate ethics charters are **voluntary principles**^{xliv}.

3- Virtual identity and digital evidence. Legal security presupposes that the author of an act can be identified, that the act can be proven and that decisions can be enforced. Anonymous or platform-controlled virtual identities weaken all three^{xlv}. Digital evidence is volatile and manipulable, and generative AI makes the fabrication of convincing documents, voices and images cheap. Algerian law has responded by recognizing electronic writing and signatures, organizing electronic procedures and, since 2026, regulating trust services and electronic identification^{xlvi}, but the probative regime of AI-generated or AI-altered content remains largely unaddressed^{xlvii}.

Second Topic:

Prospects on strengthening legal security in light of the technological revolution

While rapid technological advancements have presented a number of challenges and risks that have threatened the stability of legal frameworks and created a significant legislative gap, they also pose not only a threat to legal security but also offer promising prospects and unprecedented opportunities for its development and strengthening.

The digital age requires the contemporary legal system to move beyond a purely defensive or traditional regulatory stance and instead embrace technology itself, leveraging its advanced tools to serve justice and ensure the stability of transactions.



Accordingly, this topic aims to anticipate future solutions and objectives to be achieved to promote legal security; by highlighting the role of digitization and artificial intelligence as a tool for modernizing the legislative and judicial structure (First Section), then focuses on the role of emerging technologies and flexible legislative environments as a technical and legal guarantee of stability and protection of transactions (second Section).

First Section: Adapting technology to serve justice and the law

The transition towards modernizing the judicial system requires a precise conceptual framework that distinguishes between "modernizing the means" and "adapting the ends." The link between technology and justice is not established simply by introducing software into the courtrooms, but rather through adapting technology to serve justice and the law. This implies a structural process aimed at framing and constraining digital tools to operate within the framework of established constitutional and procedural principles. This adaptation constitutes the philosophical foundation that ensures technology does not transform from a tool serving the law into a power that dominates it. This necessitates a complete restructuring of the technological environment to align with the requirements of a fair trial, the rights of the defense, transparency, and judicial impartiality. This comprehensive digital transformation unfolds through an examination of its dimensions and concrete manifestations in judicial work: namely the digitization of the judicial system (1), as well as the use of artificial intelligence to enhance the quality of legislative drafting to meet the requirements of a fair trial (2), and the unification of judicial interpretation (3).

1- **Digitalization of the judicial system** Adapting the digital transformation of the judicial system represents a legislative approach that goes beyond the technical reduction represented by the "automation" of paper transactions, to reach the re-engineering of the institutional structure of justice according to a correlation that combines the efficiency of technology and the preservation of the constitutional guarantees of a fair trial^{xlvi}.

This concept is founded on the principle of the rule of law over technology, where technology is not an end in itself, but rather a flexible tool structurally adapted to align with established legal principles such as the principle of confrontation, the openness of hearings, the right to defense, and the impartiality of the judge. Within this framework, digital transformation extends to building a comprehensive and independent virtual litigation environment. This begins procedurally with the electronic filing of lawsuits and initiating proceedings through unified platforms, progresses through the real-time exchange of memoranda and pleadings between litigants, and culminates in remote video trials employing secure interactive communication technologies. Ultimately, it leads to the issuance of a judicial ruling bearing an electronic signature and protected by biometric digital fingerprints to prevent any breach or manipulation of the validity of judicial documents.



In the context of criminal and civil evidence, this adaptation requires the legislator to update traditional theories of evidence by recognizing the absolute legal validity of electronic documents and digital evidence extracted from cyberspace, based on the use of advanced technologies such as blockchain, which ensures the integrity of judicial evidence from alteration and grants judgments and decisions absolute immunity against forgery through distributed and unalterable records.

This procedural effect extends to the stage of judgment enforcement, where the system transforms into an integrated network environment, directly interconnected with the state's financial, banking, real estate, and commercial institutions, thus enabling the imposition of intelligent seizures on debtors' funds and real estate in an instantaneous and immediate manner upon issuance of the digital enforcement formula, eliminating the problem of slow execution from which traditional justice has long suffered.

As for the judicial decision-making process and the use of artificial intelligence, legal jurisprudence prohibits reliance on independent automated justice, and adapts algorithms and big data to play only an auxiliary and advisory role for the human judge^{xlix}. These intelligent systems analyze thousands of judicial precedents, extract arguments, and search for similar cases to guide the judge towards the most accurate and unified judicial interpretation, while keeping the absolute discretionary power and the formation of the emotional and explanatory conviction exclusively in the hands of the judge, in order to avoid the risks of algorithmic bias resulting from feeding the machine with standard data that may violate the principle of equality before the law.

However, to ensure the absolute confidentiality inherent in judicial proceedings, advanced encryption protocols are used to protect judges' virtual deliberation rooms before judgments are handed down, thus preventing any leaks or clandestine eavesdropping that could compromise the integrity of the justice system and the privacy of those involved in legal proceedings. This transformation results in a humanization of technology and the removal of its cognitive and physical barriers for individuals, thanks to the design of simplified interactive interfaces and the use of intelligent voice assistants based on natural language processing^l.

This allows illiterate individuals, members of vulnerable groups, and people with disabilities to access the judicial system directly and without restriction, without technical intermediaries, thus making digital justice a cornerstone of strengthening legal certainty, guaranteeing institutional integrity, and consolidating public trust in the rule of law.

2- Employing artificial intelligence to improve the quality of legislative drafting

The application of artificial intelligence to the quality of legal drafting represents a real qualitative leap in the transition between the purely procedural aspect of the digitization of justice — often limited to electronic archiving and the mechanical flow of files — and the



substantive aspect which touches on the very essence of legal material, the philosophy of its formulation and its normative structure.

Legal texts, whether found in legislation, civil contracts, or court decisions, are the essential vehicle for translating the will of the legislator or the parties to the contractual relationship. Therefore, the application of machine learning and natural language processing techniques to the legal field is not intended to replace human capabilities, but rather to refine the text linguistically and semantically in order to protect it from any vague or ambiguous expressions that could lead to multiple interpretations. This helps prevent malicious interpretations or contradictory court decisions that could undermine the stability of the law and compromise the principle of legal certainty.

The strategic value of this technological adaptation is evident in the ability of intelligent algorithms to impose automatic and immediate control over the state's legislative hierarchy. These systems are fed by the entire legal arsenal, from the constitutional document down to the most basic executive decrees, allowing drafters to proactively verify compliance with standards and reveal any legislative conflicts or contradictions before the text is published and implemented. In this way, the legislative environment is integrated and strengthened against challenges of invalidity or unconstitutionality^{li}.

Furthermore, this technological, justice-focused perspective aims to revolutionize the financial and investment transaction sector through standardized document and contract generation systems. These systems ensure a high degree of standardization, minimizing human error and omission in drafting essential clauses such as penalty clauses and dispute resolution mechanisms, thereby fostering trust and stability in the business environment^{lii}. Moreover, the quality of drafting doesn't stop there; it extends to proactive and predictive drafting, based on the analysis of massive datasets and millions of court precedents. Intelligent software can adapt the text to trends established by case law and predict the success rate of a clause or the likelihood of it generating litigation. The legal system thus shifts from managing disputes after the fact to preventing them from the outset, achieving the ultimate goal of legal technology: establishing lasting legal certainty and strengthening the foundations of an effective justice system.

3- Predictive Justice and Harmonization of Jurisprudence

Legal security is one of the fundamental pillars that ensure the stability of societies and the confidence of individuals in the legislative and judicial system. Legal security requires that legal rules be clear, consistent, and their practical outcomes predictable, free from judicial surprises.

Indeed, with technological development, the concept of legal security has moved from the realm of "philosophical security based on the text" to the realm of "statistical certainty based on data and established judicial models".



Artificial intelligence plays a pivotal role in supporting judicial work and achieving legal security through two integrated mechanisms: Predictive Justice Mechanism and Harmonization of Jurisprudence.

Recent legal studies have confirmed that "predictive justice," based on artificial intelligence algorithms, does not aim to replace human intervention, but rather serves as a decision-making tool to reduce the number of cases and alleviate the burden on the courts. This system can provide judges and parties to a dispute with probability estimates of the outcome of a judgment and trial, thereby encouraging the use of alternative dispute resolution methods before any legal proceedings^{liii}.

In addition, the harmonization of judicial interpretation guarantees legal security. Contradictory court decisions in similar cases constitute one of the greatest threats to this certainty. In this context, artificial intelligence, through case law analysis systems, intervenes to link lower courts to the established rulings of higher courts (such as the Supreme Court or the Court of Cassation). This helps to avoid aberrant individual interpretations and establish a predictable and consistent legal framework, thus protecting the interests of individuals and investors^{liv}.

The contribution of artificial intelligence in this area is evident, it constitutes an intelligent guidance tool that allows the human judge to extrapolate historical judicial trends with extreme accuracy, thus ensuring the formulation of judicial decisions^{lv} in accordance with established precedents and avoiding conflicts, which consequently leads to the establishment of a safe, stable and predictable judicial environment for individuals and institutions.

Second Section: Emerging technologies as a guarantee for transaction stability

If development the judicial and legislative system is the cornerstone of protecting legal security, guaranteeing the stability of everyday transactions for individuals and investors in the digital environment is its essential complement. Traditional legal rules, based on physical mechanisms, are no longer sufficient to ensure the stability and security of electronic transactions in a constantly evolving virtual environment. Therefore, it has become urgent to move towards a parallel technological security, where modern technology is no longer merely an object of legal regulation, but itself becomes a tool for producing and strengthening legal security.

Therefore, emerging technologies can become a safety valve that protects legal positions and prevents disputes before they arise, this is achieved through Blockchain technology by giving absolute certainty to digital documents and records (1), and by analyzing the effectiveness of smart contracts as a guarantee of the automatic and autonomous execution of obligations (2), to conclude by indicating the role of flexible regulatory sandboxes as a newly developed mechanism that allows the legislator to test technological innovations and protect those dealing with them at the same time(3).



1- Blockchain technology and digital proof value

The concept of legal security is closely linked to the principle of certainty and stability of transactions, which requires the existence of official and customary means of proof with absolute authority and resistance to falsification and manipulation. Faced with digital transformation, Blockchain technology has emerged as a revolutionary tool contributing to the long-term preservation of digital documents, thus addressing the shortcomings of paper documents and traditional centralized electronic systems, which are vulnerable to hacking^{lvi}. However, Blockchain's contribution to strengthening the authority of digital immutability rests on two key points:

- **The impossibility of altering digital data:** Blockchain technology relies on a distributed ledger system, where legal transactions (such as property transfers or patents) are recorded in encrypted blocks of code, simultaneously distributed across thousands of computers worldwide. This technological structure makes it impossible for anyone, even the competent authority, to modify, delete, or falsify data after it has been recorded, as any modification requires the approval of a majority of computers on the network, which is technically impossible. This absolute immutability provides digital documents with superior cybersecurity protection, thus guaranteeing users an optimal level of legal security^{lvii}.
- **The Disintermediation:** In the traditional system, legal security relies on the presence of a trusted third party, such as a notary, a bank, or a land registry office. Blockchain technology, on the other hand, creates an environment without human intermediaries. Recording a legal transaction on the network gives it a permanent and tamper-proof digital history (time stamp), providing irrefutable evidence in court to establish priority and standing, and significantly reducing the number of disputes related to falsified contracts or competing property claims^{lviii}.

2- Smart contracts as a guarantee for the automatic implementation of obligations

The performance of contractual obligations is one of the most crucial stages in the life of a contractual relationship, as it is often fraught with the risk of delay or refusal by the debtor, threatening stability, transactions, and the principle of legal certainty. In this context, modern technologies introduce the concept of "smart contracts," a revolutionary technical mechanism that transforms traditional contractual clauses into digital and programmable conditions. These contracts execute automatically and immediately upon the occurrence of the event creating the obligation, without human intervention or recourse to complex enforcement mechanisms^{lix}. The legal value and promising prospects of smart contracts are evident in achieving legal security across two mechanisms:

- **Self-implementation mechanism and conflict prevention:** Unlike traditional contracts, which are subject to ambiguities in interpretation or delays in execution, smart



contracts are formulated as plain code, based on a logic where "if the first condition is met, the second obligation is automatically fulfilled." For example, in the context of digital insurance or e-commerce contracts, the software system is obligated to transfer ownership or pay compensation immediately and automatically upon confirmation of the event (such as the delivery of goods or a flight delay). This automatic execution eliminates any possibility of evading obligations, thus proactively protecting legal interests and preventing disputes^{lx}.

- **Transactions eliminate the need for traditional enforcement:** Legal security essentially rests on the creditor's certainty of receiving payment. Smart contracts offer this certainty by transferring enforcement power from individuals, law enforcement, and judicial bodies to the code itself. In this way, parties are freed from the delays of litigation and the difficulties of cross-border enforcement in the digital space, making technology the ultimate guarantor of the stability and permanence of contractual commitments^{lxi}.

3- Flexible Regulatory sandboxes

Contemporary legal systems face a major dilemma: the time lag between the rapid pace of technological innovation (such as FinTech applications, virtual law, smart contracts...) and the slowness of traditional legislative processes. Hastily adopting rigid laws risks hindering the effectiveness of these innovations, while their lack of regulation could compromise the legal certainty of individuals. It is in this context that "legislative sandboxes" have emerged as an innovative and flexible legal mechanism, striking a balance between the imperative of technological innovation and the requirements of legal security. These environments contribute to strengthening legal security through two mechanisms:

- **Establishing a Temporary Legal Framework for Startups:** A regulatory sandbox is a flexible, temporary, and geographically defined regulatory framework within which supervisory authorities (such as central banks or ministries of justice) allow companies to test their innovative technologies on a small scale and in a controlled manner, temporarily exempting them from certain stricter legal constraints. The value of this mechanism lies in creating a "legal safe haven" that protects innovators from any legal liability related to the absence of legislation and allows them to clearly understand the compliance of their projects with public order^{lxii}.

- **Operator's protection and creating proactive legislation:** These environments not only protect businesses but also offer proactive safeguards to ensure the legal certainty of consumers and investors using these technologies under state supervision. Furthermore, this experimental period allows legislators to understand the technical aspects of technological products, which subsequently helps them draft definitive legislation characterized by clarity, realism, and stability—the three fundamental elements of the principle of legal security.

Finally, Regulatory sandboxes allow supervised experimentation under temporary and



controlled derogations, generating information for later legislation^{lxiii}. Under the AI Act as amended, each Member State must ensure that at least one AI regulatory sandbox is operational at national level by 2 August 2027^{lxiv} 75. For legal security, sandboxes are valuable only if their entry criteria, safeguards for participants and exit conditions are themselves set out in clear and published rules; otherwise they risk creating zones of legal uncertainty.

Conclusion:

This study examined whether legal security can be preserved in the age of AI by combining doctrinal analysis with across the legislative approach. Doctrinally, AI challenges legal security normatively, through legislative inflation, imprecise drafting and the instability of digital statutes, and technologically, through algorithmic opacity, the erosion of territorial sovereignty. While technology initially appeared as a genuine threat to the stability of the law and the security of transactions, this study has demonstrated, through both theoretical and practical examples, that this same technology holds promising potential for protecting and strengthening the law, provided it is properly regulated and its tools are adapted to serve the interests of justice.

Therefore, a number of results were formulated, which we summarize below:

- The legal Security in the digital age is no longer limited to rigid legislation, but requires the integration of "technological certainty" (such as blockchain and artificial intelligence) as a complementary pillar of rights protection.
- Legislative Flexibility Does Not Mean Absence: Research has shown that to address the technological revolution, legislators must adopt flexible and proactive mechanisms that ensure the regulation of modern technologies without hindering innovation or sacrificing legal certainty.
- Emerging technologies, such as smart contracts and predictive law, have been shown to contribute directly to harmonizing judicial interpretation and preventing conflicting decisions, thereby strengthening the confidence of individuals and investors in the legal system.

Recommendations:

- Adopt a principle-based framework law on AI, defining stable obligations of transparency, human oversight, accountability and redress, and delegating technical rules to revisable regulations.
- Consolidate digital legislation (data protection, trust services and electronic identification, electronic commerce, cybercrime and e-justice) to reduce fragmentation and repeated amendment, supported by regulatory impact assessment.
- Establish a published legal framework for AI regulatory sandboxes, with clear entry, safeguard



and exit rules.

- Provide graduated rights to information, human review, contestation and individual explanation for automated administrative and judicial decisions, and regulate the probative value of AI-generated evidence.

Citations

-
- ⁱ Constitution of the People's Democratic Republic of Algeria, promulgated by Presidential Decree No. 20-442 of 30 December 2020, Official Journal of the Algerian Republic (JORA) No. 82 of 30 December 2020, art. 34.
- ⁱⁱ Lon L. FULLER, *The Morality of Law*, revised edition, Yale University Press, New Haven, 1969, pp. 33–94.
- ⁱⁱⁱ Joseph RAZ, *The Authority of Law: Essays on Law and Morality*, Clarendon Press, Oxford, 1979, pp. 210–229.
- ^{iv} European Court of Human Rights, *The Sunday Times v. the United Kingdom* (No. 1), Application No. 6538/74, judgment of 26 April 1979, Series A No. 30, § 49.
- ^v Council of State, 2006 Public Report: Legal Certainty and the Complexity of the Law, La Documentation française, Paris, 2006.
- ^{vi} Constitution 2020, op. cit, art. 34.
- ^{vii} Mireille HILDEBRANDT, "Law as computation in the era of artificial legal intelligence: Speaking law to the power of statistics", *University of Toronto Law Journal*, Vol. 68, Supplement 1, 2018, pp. 12–35. <https://doi.org/10.3138/utlj.2017-0044>; MOUHSSINE, Imane TAIBI, Karim SEFFAR, "La sécurité juridique au défi de la digitalisation", *Revue internationale Burak des Études Juridiques et Économiques*, Vol. 3, No. 1, 2026
- ^{viii} GLOBAL AI INDEX, *Global AI Index 2026 – Rankings and methodology*, <https://globalaiindex.org/rankings/> (consulted on 27/09/2026).
- ^{ix} Gary E. MARCHANT, Braden R. ALLENBY, Joseph R. HERKERT (eds.), *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem*, Springer, Dordrecht, 2011. <https://doi.org/10.1007/978-94-007-1356-7>; David COLLINGRIDGE, *The Social Control of Technology*, Frances Pinter, London, 1980.
- ^x Araz TAEIHAGH, "Governance of artificial intelligence", *Policy and Society*, Vol. 40, No. 2, 2021, pp. 137–157. <https://doi.org/10.1080/14494035.2021.1928377> . (consulted on 27/09/2026).
- ^{xi} Fatima-Zohra BOUDJEMA, Morad BESSAID, "The impact of technological development and information technologies on achieving legal security" [in Arabic], *Mediterranean Thought Journal*, Vol. 11, No. 1, 2022, pp. 466–484;
- ^{xii} - Law No. 09-04 of 5 August 2009 laying down special rules for the prevention of and fight against offences related to information and communication technologies, JORA No. 47 of 16 August 2009.
- ^{xiii} Law No. 15-03 of 1 February 2015 on the modernization of justice, JORA No. 6 of 10 February 2015.
- ^{xiv} Law No. 18-05 of 10 May 2018 on electronic commerce, JORA No. 28 of 16 May 2018.
- ^{xv} - Law No. 18-07 of 10 June 2018 on the protection of natural persons in the processing of personal data, JORA No. 34 of 10 June 2018, art. 22
- ^{xvi} Law No. 26-02 of 17 February 2026 laying down the general rules relating to trust services for electronic transactions and electronic identification, JORA No. 14 of 18 February 2026.
- ^{xvii} Chettouh RAHMOUN, "Algerian Legislation in the Face of the Need to Regulate E-commerce" " [in Arabic], *Afak For Sciences Journal*, Vol. 11, No. 3, 2026, pp. 313–330.
- ^{xviii} - Lyria BENNETT MOSES, "How to Think about Law, Regulation and Technology: Problems with 'Technology' as a Regulatory Target", *Law, Innovation and Technology*, Vol. 5, No. 1, 2013, pp. 1–20.



<https://doi.org/10.5235/17579961.5.1.1>.

- ^{xix} Rabah REKBI, "Legal Frameworks in the Era of Digital Technology", *Russian Law Journal*, Vol. 12, No. 2, 2024, pp. 2814–2825;
- ^{xx} - Law No. 25-11 of 24 July 2025 amending and supplementing Law No. 18-07 of 10 June 2018, JORA No. 48 of 2025.
- ^{xxi} Law No. 15-04 of 1 February 2015 laying down the general rules relating to electronic signature and certification, JORA No. 6 of 10 February 2015 (repealed by Law No. 26-02).
- ^{xxii} Law No. 26-02, op. cit, art. 115
- ^{xxiii} David COLLINGRIDGE, *The Social Control of Technology*, Frances Pinter, London, 1980.
- ^{xxiv} Frank PASQUALE, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Harvard University Press, Cambridge (MA), 2015; Harry SURDEN, "Machine Learning and Law", *Washington Law Review*, Vol. 89, No. 1, 2014, pp. 87–115.
- ^{xxv} Supreme Court of Wisconsin, *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016).
- ^{xxvi} Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), *Official Journal of the European Union* L 119, 4 May 2016, arts. 13(2)(f), 14(2)(g) and 15(1)(h).
- ^{xxvii} Court of Justice of the European Union (CJEU), Case C-203/22, *Dun & Bradstreet Austria*, judgment of 27 February 2025.
- ^{xxviii} GDPR, op. cit, art. 22(1)–(3).
- ^{xxix} Court of Justice of the European Union (CJEU), Case C-634/21, *OQ v Land Hessen (SCHUFA Holding AG)*, judgment of 7 December 2023.
- ^{xxx} Bryce GOODMAN, Seth FLAXMAN, "European Union Regulations on Algorithmic Decision-Making and a 'Right to Explanation'", *AI Magazine*, Vol. 38, No. 3, 2017, pp. 50–57. <https://doi.org/10.1609/aimag.v38i3.2741>; Sandra WACHTER, Brent MITTELSTADT, Luciano FLORIDI, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation", *International Data Privacy Law*, Vol. 7, No. 2, 2017, pp. 76–99. <https://doi.org/10.1093/idpl/ix005>.
- ^{xxxi} Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), *Official Journal of the European Union (OJ) L*, 2024/1689, 12 July 2024, as amended by Regulation (EU) 2026/1744, arts. 13, 14 and Annex III, point 8.
- ^{xxxii} *Ibid.* art. 86.
- ^{xxxiii} *Ibid.* art. 85.
- ^{xxxiv} Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), *OJ L*, 2026/1744, 24 July 2026.
- ^{xxxv} Margot E. KAMINSKI, "Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability", *Southern California Law Review*, Vol. 92, No. 6, 2019, pp. 1529–1616; Michael VEALE, Frederik ZUIDERVEEN BORGESIU, "Demystifying the Draft EU Artificial Intelligence Act", *Computer Law Review International*, Vol. 22, No. 4, 2021, pp. 97–112. <https://doi.org/10.9785/cr-2021-220402>.
- ^{xxxvi} Andrea BERTOLINI, *Artificial Intelligence and Civil Liability: A European Perspective*, study requested by the JURI Committee, European Parliament, Policy Department for Justice, Civil Liberties and Institutional Affairs, PE 776.426, Brussels, July 2025.
- ^{xxxvii} Selma Achba ABDELAZIZ, Mohamed MANSOURI, "International Law and Cyber Challenges: Protecting International Security in the Age of Technology", *Algerian Journal of Legal and Political Sciences*, Vol. 62,



No. 3, 2025, pp. 188–204.

^{xxxviii} Anu BRADFORD, *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, New York, 2020; Mihaela Daciana NATEA, Simion COSTEA (coords.), *EU Law and Politics at the Crossroads: Navigating the Complexities of AI, Digitalization, Data Protection, Security, and Radicalization*, L'Europe Unie / United Europe, No. 20 (special volume), Paris, 2023.

^{xxxix} - Nathalie A. SMUHA, "From a 'race to AI' to a 'race to AI regulation': regulatory competition for artificial intelligence", *Law, Innovation and Technology*, Vol. 13, No. 1, 2021, pp. 57–84. <https://doi.org/10.1080/17579961.2021.1898300>.

^{xl} Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Council of Europe Treaty Series (CETS) No. 225, Vilnius, opened for signature on 5 September 2024 (ratified by the European Union in 2026).

^{xli} OECD, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449, Paris, adopted 22 May 2019, amended 3 May 2024; UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, adopted by the General Conference on 23 November 2021, Paris.

^{xlii} UNITED NATIONS GENERAL ASSEMBLY, Resolution A/RES/78/265, *Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development*, adopted 21 March 2024.

^{xliii} UNITED NATIONS GENERAL ASSEMBLY, Resolution A/RES/79/325, *Terms of reference and modalities for the establishment and functioning of the Independent International Scientific Panel on Artificial Intelligence and the Global Dialogue on Artificial Intelligence Governance*, adopted 26 August 2025.

^{xliv} Anna JOBIN, Marcello IENCA, Effy VAYENA, "The global landscape of AI ethics guidelines", *Nature Machine Intelligence*, Vol. 1, No. 9, 2019, pp. 389–399. <https://doi.org/10.1038/s42256-019-0088-2>.

^{xlv} E. R. KOROTKEVICH, "Problems of virtual identity in the digital age (social and philosophical analysis)", *Advances in Economics, Business and Management Research*, Vol. 81 (Proceedings of MTDE 2019), Atlantis Press, 2019; Brahim DERDICHE, Omar NESSIL, "Digital Gaps and Challenges of Legal Security", *The International Tax Journal*, Vol. 52, No. 3, 2025, pp. 224–234.

^{xlvi} Law No. 15-03, op. cit; Law No. 26-02, op. cit.

^{xlvii} Adik Aleksandrovich LI, "Cyber Law: Addressing Legal Challenges in the Digital Age", *Uzbek Journal of Law and Digital Policy*, Vol. 1, No. 3, 2023; Anita MU'MIN, Muhammad Rafli CHANIAGO, SUARTINI, "Digitalization of Civil Transactions and Its Implications for Legal Certainty in the Era of Society 5.0", *Edusight International Journal of Multidisciplinary Studies*, Vol. 2, No. 2, 2025.

^{xlviii} Fatima-Zohra BOUDJEMA, Morad BESSAID, p.479.

^{xlix} Florence G'SELL, *The automation of judicial decisions, how far will it go? Legal professions facing the digital challenge*, *Journal Annales des mines*, No. 03, September 2018, p. 22.

^l Mokhtar KENNICHE, Djilali BENABOU, *The journey of Digital Transformation in the Algerian Justice Sector*, *Al-Mi'yar Journal*, Volume: 26, No. 07, 2022, pp. 297-323.

^{li} Boualem BENSMAILI, Abderrahmane BEN DJILALI, *Enhancing legal security in constitutional drafting: The role of artificial intelligence in the transition from the traditional to the smart model – Algeria as a model*, *jurisprudence Journal*, Volume: 18, No. 01, 2026, pp. 207-214..

^{lii} A group of researchers, *Law and Artificial Intelligence: Studies and visions in Legislation and Society*. Collective work, Democratic Arab for Strategic, political and Economic studies, Berlin, Germany, 2024.



^{liii} Arwa A. Al- Jaloud , Rulings on Artificial Intelligence Applications in the Judiciary: An Analytical Comparative Study , Marajea Scientific Publishing, 2024,p.77.

^{liv} Omar Taher Hemeda Ali, Artificial Intelligence and Judicial Precedent Analysis: A Tool for Building Legal Education Based on Judicial Reality, Journal of Architecture, Arts and Humanities, Volume 10, Special Issue (14), International Conference (Artificial Intelligence and Sustainable Development), 2025.p.08.

^{lv} Florence G'SELL, p.51, op. cit.

^{lvi} DE FILIPPI, Primavera, WRIGHT AARON, Blockchain and the Law: The Rule of Code. Harvard University Press,2018 , pp. 73-75.

^{lvii} KOULU Riika , Blockchains and Online Dispute Resolution: Smart Contrats as on Alternative to Enforcement, Journal of international Dispute Settlement, Volume: 13, No. 01, 2016, pp.45-50.

^{lviii} Michéle FINCK. Blockchain Regulation and Governance in Europe, Cambridge University Press, 2018, p. 89.

^{lix} WERBACH Kivin, Cornell CORNELL Nicolas, Contracts Ex Machina, Duke Law Journal, Volume: 67, No. 2, 2017, pp. 317–324.

^{lx} DE FILIPPI, Primavera, WRIGHT AARON, Blockchain and the Law: The Rule of Code, p. 77, previous reference.

^{lxi} SAVELYEV Alexander, Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law, Information and Communications Technology, Volume: 26, No. 02, 2017, p. 119.

^{lxii} Hilary J. Allen , Regulatory Sandboxes, The George Washington Law Review, Volume:87, No.3, 2019?, pp.584 585.

^{lxiii} Hilary J. ALLEN, "Regulatory Sandboxes", George Washington Law Review, Vol. 87, No. 3, 2019, pp. 579–645; Dirk A. ZETZSCHE, Ross P. BUCKLEY, Janos N. BARBERIS, Douglas W. ARNER, "Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation", Fordham Journal of Corporate & Financial Law, Vol. 23, No. 1, 2017, pp. 31–103.

^{lxiv} AI Act, op. cit, art. 57.