INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH AND INNOVATIVE STUDIES
ISSN: 2820-7157
www.ijsrisjournal.com

April 2026 Volume 5 Number 2 580-604

Received Date: 22 February 2026 Accepted Date: 14 March 2026 Published Date: 02 April 2026

Artificial Intelligence and ICT in Moroccan Law: A Comparative Analysis of the EU and the US and Prospects for Reform

ANASS Fykri [1], Brahim Atrouch [2]

1. Research Laboratory: Strategic Intelligence and Legal Management of Public Administrations, Faculty of Legal, Economic and Social Sciences of Aïn Sebaâ, Hassan II University, Casablanca, Morocco, anass.fykri-etu@etu.univh2c.ma
2. Research Laboratory: Strategic Intelligence and Legal Management of Public Administrations, Faculty of Legal, Economic and Social Sciences of Aïn Sebaâ, Hassan II University, Casablanca, Morocco, Atrouchbrahim@gmail.com

Abstract

Artificial intelligence is now emerging as a major technological shift, profoundly affecting contemporary economic, social and legal balances. In Morocco, this development forms part of recent public policies on digital transformation, which position artificial intelligence as a key driver of administrative modernisation and economic competitiveness. This study argues that the absence of a legal framework specifically dedicated to artificial intelligence should not be equated with a regulatory vacuum, given that algorithmic systems are already indirectly covered by a set of constitutional norms, sector-specific legislation and international commitments. However, this regulatory framework remains fragmented and structurally ill-suited to the technical specificities of artificial intelligence, characterised in particular by algorithmic opacity, functional autonomy and the complexity of the value chain. This inadequacy is manifested through the unsuitability of the traditional fault-based liability paradigm, the disruption of the traditional causation framework, and the difficulties in attributing liability in multi-stakeholder technical environments. A comparative analysis highlights these limitations, in light of the European model structured around Regulation (EU) 2024/1689 (AI Act), which is based on a risk-based approach incorporating mechanisms of allocated liability and appropriate presumptions of liability, as well as the US approach, which is more sector-specific and geared towards promoting innovation, notably through Executive Order 14179. Building on these insights, the study proposes the foundations for a renewed Moroccan legal framework based on the establishment of strict liability for high-risk systems, the introduction of allocated liability within the algorithmic value chain, and the development of evidentiary mechanisms adapted to the constraints of opacity and complexity inherent in artificial intelligence systems.

Keywords: artificial intelligence, Moroccan law, civil liability, algorithmic governance, evidence, causality, comparative law.

1. Introduction

Artificial intelligence today represents a technological transformation of unprecedented scale, profoundly affecting contemporary economic, social and legal structures, and necessitating a gradual reconfiguration of traditional regulatory frameworks. In Morocco, this development forms part of public policies on digital transformation, which assign artificial intelligence a strategic role in the modernisation of public action and the strengthening of economic

competitiveness. This dynamic is, however, hampered by the absence of a legal framework specifically dedicated to artificial intelligence systems, revealing a growing tension between the imperative of technological innovation and the need for legal certainty and the protection of fundamental rights. The central issue of this study is therefore to determine whether this absence of specific legislation should be interpreted as a genuine legal vacuum or whether, on the contrary, Moroccan law already offers, through its traditional mechanisms, sufficient resources to regulate algorithmic systems. The hypothesis adopted is based on the idea that artificial intelligence is already, albeit indirectly, addressed by a set of existing constitutionals, legislative and international norms, the application of which remains, however, fragmentary and structurally ill-suited to the technical specificities of AI systems. In particular, Moroccan civil liability law, based on the fault-based paradigm as enshrined in Article 78 of the Dahir establishing the Code of Obligations and Contracts (1913), appears insufficiently adapted to address systems characterised by their functional autonomy, algorithmic opacity and the multiplicity of actors involved in their lifecycle. The questioning of the traditional causal link and the difficulties in attributing liability within a complex algorithmic value chain reinforce this inadequacy and justify an in-depth doctrinal examination. From a methodological perspective, the absence of specific Moroccan case law on artificial intelligence, combined with the still-emerging nature of national legal doctrine, leads to a preference for an approach based on extrapolating the principles of general law to algorithmic issues, enriched by a comparative analysis of foreign models. In this regard, the European Union proposes, through Regulation (EU) 2024/1689 (AI Act), a structured regulatory model based on a risk-based approach and incorporating innovative mechanisms for allocated liability as well as appropriate presumptions of evidence, whilst the United States adopts a more flexible sectoral approach, notably through Executive Order 14179, reflecting a priority given to innovation at the risk of a certain degree of regulatory fragmentation. In this context, this study aims to identify the lessons that can be drawn from these comparative experiences in order to propose a Moroccan legal framework that reconciles technological innovation, legal certainty and the protection of fundamental rights, and is structured around two main themes: the first devoted to analysing the indirect legal framework for artificial intelligence under Moroccan law and its conceptual limitations, the second focusing on a comparative analysis designed to identify suitable avenues for reform.

2. The indirect legal framework for artificial intelligence in Moroccan law and its conceptual limitations

2.1 Constitutional foundations and applicable general principles

The 2011 Constitution of the Kingdom of Morocco constitutes the fundamental normative basis from which the legal framework for artificial intelligence under Moroccan law can be understood, albeit indirectly. Although this text does not expressly refer to algorithmic technologies, its provisions relating to fundamental rights and freedoms apply with particular force to artificial intelligence systems, insofar as they involve automated processing capable of affecting the legal sphere of individuals. In this regard, Article 24 explicitly enshrines the right to privacy, stipulating that ‘every person has the right to the protection of their private life’ and that ‘private communications, in whatever form, are confidential’ (Constitution of the Kingdom of Morocco, 2011, Art. 24). This constitutional guarantee has direct implications for artificial intelligence systems based on the collection, processing and use of personal data, in that it imposes a clear normative limit on any form of algorithmic interference in the private sphere. It thus contributes to the affirmation of a principle of personal data protection with constitutional status, the scope of which is reinforced in an environment characterised by the massification of data and the increasing sophistication of automated analysis techniques.

Building on this protection, Article 27 of the Constitution enshrines the right of access to information held by the public administration, elected institutions and bodies entrusted with a public service mission (Constitution of the Kingdom of Morocco, 2011, Art. 27). This right, initially conceived as an instrument of administrative transparency, takes on a particular dimension in the context of artificial intelligence systems, notably in that it can be invoked to justify a requirement for access to information relating to the algorithmic processing used by public authorities. It thus contributes to the emergence of a requirement for algorithmic transparency, closely linked to the principles of explainability and accountability of automated systems, and constitutes a potential lever for controlling decisions based on artificial intelligence.

Furthermore, the principle of equality before the law, enshrined in Article 19 of the Constitution, is of particular importance in light of the risks of algorithmic discrimination. Indeed, artificial intelligence systems, particularly those used in recruitment, credit granting or administrative decision-making, are likely to reproduce, or even amplify, discriminatory biases already present in the training data.

Consequently, the constitutional requirement of equality imposes on the designers and users of these systems an implicit duty of care regarding the potential discriminatory effects of algorithms. This requirement, which forms part of the principle of the effectiveness of fundamental rights, tends to enshrine a form of horizontal applicability of constitutional norms, in that it applies not only to public authorities but also to private actors whose activities are likely to infringe upon guaranteed rights and freedoms.

Finally, the protection of human dignity, enshrined both in the preamble to the Constitution and in Article 22, which prohibits any infringement of the physical or moral integrity of individuals as well as cruel, inhuman or degrading treatment (Constitution of the Kingdom of Morocco, 2011, Art. 22), introduces a fundamental ethical limit on the automation of decisions affecting the individual. This requirement of dignity constitutes a particularly relevant legal basis for regulating, or even prohibiting, certain uses of artificial intelligence that are likely to infringe upon the psychological integrity or autonomy of individuals. In this regard, a convergence can be observed with European law, notably through Regulation (EU) 2024/1689 (AI Act), which prohibits certain artificial intelligence practices considered to pose an unacceptable risk to fundamental rights (European Parliament & Council of the European Union, 2024). This interplay between national constitutional principles and international standards illustrates the capacity of Moroccan law to indirectly regulate emerging technologies, whilst highlighting the limitations of a model based on general standards whose adaptation to the technical and organisational specificities of artificial intelligence remains incomplete and therefore calls for a more targeted regulatory approach.

2.2 The application of sector-specific legislation to artificial intelligence and its shortcomings

2.2.1. Law No. 09-08 on the protection of personal data: a cross-cutting pillar of the regulatory framework for algorithms

The legal framework for artificial intelligence under Moroccan law does not, at this stage, rest on a unified regulatory framework or one specifically dedicated to this technology. Rather, it stems from a gradual mobilisation of pre-existing sector-specific standards, of which Law No. 09-08 on the protection of natural persons with regard to the processing of personal data constitutes the main structural pillar. This approach is not arbitrary: it stems directly from the very nature of artificial intelligence systems, whose operation is intrinsically based on the use of data.

Indeed, contemporary artificial intelligence architectures, particularly those based on machine learning, involve complex operations of collection, structuring, training and inference based on massive volumes of data. However, from a legal perspective, these operations correspond to ‘processing of personal data’ within the meaning of Law No. 09-08, which adopts a particularly broad interpretation of this concept by including any operation, whether automated or not, applied to personal data (Law No. 09-08, Articles 1 and 2). Consequently, although this law was not designed to regulate artificial intelligence, it effectively serves as the normative framework of reference for understanding its legal implications.

This central role gives Law No. 09-08 a cross-cutting function: it does not regulate artificial intelligence as such, but it provides a framework for one of its essential constituent elements, namely data, which enables it to exert an indirect yet decisive influence on algorithmic systems.

- Scope of application and functional extension to artificial intelligence systems

The scope of Law No. 09-08 stems primarily from the broad definition of personal data set out in Article 1. By defining personal data as ‘any information, of whatever nature, concerning an identified or identifiable natural person’ (Law No. 09-08, Art. 1), the Moroccan legislature has adopted a comprehensive approach, independent of the medium or method of processing. This approach allows for the seamless integration of all data utilised by artificial intelligence systems, including that derived from complex digital environments such as platforms, connected devices or recommendation systems.

However, the main challenge lies in the classification of so-called ‘inferred’ data, i.e. data produced by algorithmic systems based on statistical correlations. Whilst the law does not expressly target this category, a teleological reading of Article 1 leads to the conclusion that such data falls within the scope of protection provided that it enables, directly or indirectly, the identification of a natural person. This interpretation is all the more justified given that identifiability, as defined by the text, includes indirect identifications based on economic, behavioural or social factors.

Furthermore, Article 2 of the Act extends its scope to any processing of personal data, whether automated or not, provided that it has a territorial link with Morocco, in particular where the data controller uses means located within the national territory (Act No. 09-08, Art. 2). This provision is of particular importance in the contemporary digital

ecosystem, characterised by the deterritorialisation of infrastructure and the widespread use of cloud computing.

In theory, it allows foreign entities operating artificial intelligence systems accessible from Morocco to be subject to Moroccan law. However, this territorial extension faces substantial practical limitations, particularly due to the absence of effective mechanisms for international cooperation and the asymmetry in supervisory capacities. This results in a tension between the normative scope of the text and its actual effectiveness, which is particularly acute in the context of globalised technologies.

- The underlying principles: normative standards put to the test by algorithmic logic

Law No. 09-08 is based on a set of guiding principles that govern the processing of personal data, foremost among which is the principle of purpose limitation. According to Article 3, data must be collected for 'specified, explicit and legitimate' purposes and may not subsequently be processed in a manner incompatible with those purposes (Law No. 09-08, Art. 3). This principle reflects a teleological conception of processing, in which the legitimacy of data use is contingent upon the predictability of its objectives.

However, this requirement is profoundly undermined by the logic inherent in artificial intelligence. Machine learning systems are characterised by their ability to extract unforeseen correlations and generate secondary uses of data, often not anticipated at the time of their initial collection. The purpose of processing thus tends to evolve dynamically, which contradicts the requirement for a purpose determined ex ante. This tension reveals a partial mismatch between traditional legal norms and the evolving properties of algorithmic systems.

Similarly, the principle of proportionality – reflected in the requirement for data that is 'adequate, relevant and not excessive' (Law No. 09-08, Art. 3) – appears difficult to reconcile with data-intensive computing practices. Artificial intelligence models, particularly in deep learning, require massive volumes of data to achieve optimal performance, which tends to favour a logic of accumulation rather than minimisation.

Furthermore, the rights granted to data subjects, such as the right of access, rectification and objection (Law No. 09-08, Articles 7 to 9), are based on the premise of transparency in processing. This premise is, however, undermined by the opacity of complex algorithmic models, whose decision-making mechanisms often defy intelligible understanding, even for their designers.

In this regard, Article 11 of the Act, which regulates decisions based exclusively on automated processing, is of particular importance. By prohibiting a decision producing legal effects from being based solely on automated processing aimed at evaluating certain aspects of an individual's personality (Law No. 09-08, Art. 11), the legislator anticipates, in a nascent manner, the challenges associated with algorithmic decisions. However, this provision remains insufficient in the face of the current sophistication of artificial intelligence systems, which combine automation, probabilistic methods and adaptive learning.

- The regime governing sensitive data and the institutional limits of the CNDP

Law No. 09-08 establishes a strengthened legal regime for sensitive data, defined as data revealing, in particular, ethnic origin, political opinions, religious beliefs or health status (Law No. 09-08, Articles 1 and 12). In principle, the processing of such data is subject to prior authorisation, in particular by the National Commission for the Control of Personal Data Protection (CNDP), except in strictly defined cases (Law No. 09-08, Art. 21).

This framework is particularly relevant in the context of artificial intelligence, where the risks of algorithmic discrimination are well documented, particularly when models are trained using historically biased data. In this respect, the law provides a regulatory framework capable of preventing certain abuses by imposing stricter oversight on the most sensitive processing operations.

However, the effectiveness of this regime depends heavily on the institutional capacities of the CNDP. Whilst this authority has extensive legal powers regarding oversight, investigation and sanctions (Law No. 09-08, Art. 27 et seq.), its effectiveness remains limited by a relative lack of technical expertise in the field of artificial intelligence. Decree No. 2-09-165 of 21 May 2009 implementing the aforementioned law sets out the CNDP's operating procedures and investigative powers, particularly regarding the supervision and detection of infringements, but it does not confer any specific competence in the areas of algorithmic auditing or bias assessment. This situation reveals a structural disconnect between legal competence and technical competence, which constitutes one of the main obstacles to the effective regulation of artificial intelligence systems. In the absence of tools suited to the analysis of algorithmic models, the oversight exercised by the regulatory authority risks

remaining purely formal, without any real capacity to understand the internal mechanisms of the systems.

Thus, whilst Law No. 09-08 constitutes an essential foundation for the indirect regulation of artificial intelligence in Morocco, its application highlights structural tensions between traditional legal categories and contemporary technological dynamics. These limitations therefore call for an examination of other legal instruments, particularly in criminal law and the law of obligations, which could complement this framework and address the specific challenges posed by artificial intelligence.

2.2.2. Law No. 05-20 on cybersecurity: an infrastructural regulation of artificial intelligence

Unlike Law No. 09-08, which approaches artificial intelligence through the prism of personal data, Law No. 05-20 on cybersecurity adopts an approach based on the security of information systems. It does not directly target information content, but rather the technical infrastructure that enables its processing, circulation and storage. This shift reflects a change in perspective: regulation no longer focuses on data as a legal object, but on the technical environment in which it is used.

Article 1 of Law No. 05-20 specifies in this regard that the purpose of the Act is to establish the security rules applicable to the information systems of public bodies, critical infrastructure and digital operators, whilst establishing a national framework for cybersecurity governance (Law No. 05-20, 2020, Art. 1). This provision highlights the structural purpose of the Act: to ensure the resilience of digital architectures against cyber threats, by guaranteeing the availability, integrity and confidentiality of information systems.

In the context of artificial intelligence, this law is of particular importance, albeit indirectly. As AI systems are integrated into complex digital environments, their reliability depends closely on the security of the infrastructure that supports them. In other words, algorithmic robustness cannot be separated from infrastructural robustness. Law No. 05-20 thus contributes to the regulation of artificial intelligence systems by addressing their technical underpinnings.

- The security of information systems as a prerequisite for the reliability of artificial intelligence systems

Law No. 05-20 establishes a set of obligations for entities regarding the security of information systems, which have a direct bearing on the operation of artificial intelligence systems. Article 4 requires entities, in particular, to identify the risks to their information systems and to implement appropriate technical and organisational measures to prevent incidents and limit their effects (Law No. 05-20, 2020, Art. 4). This requirement is part of a proactive risk management approach, which is an essential prerequisite for any reliable use of artificial intelligence.

Indeed, AI systems, due to their reliance on data and digital infrastructure, are particularly vulnerable to breaches of the integrity or availability of information systems. Any alteration of training data, intrusion into systems or infrastructure failure may compromise not only security but also the relevance of the results produced by the algorithms. From this perspective, cybersecurity obligations appear to be a condition for the technical validity of algorithmic decisions.

Furthermore, the law requires the implementation of mechanisms for detecting and managing cybersecurity incidents. Article 7 stipulates that entities must have the means to monitor and detect events likely to affect the security of their information systems, whilst Article 8 requires incidents to be reported to the national authority (Law No. 05-20, 2020, Articles 7 and 8). These mechanisms help to establish a framework of continuous monitoring, which is essential in the context of artificial intelligence systems, the operation of which often relies on real-time data flows.

Furthermore, the requirement to put in place business continuity and disaster recovery plans, as set out in Article 9, strengthens the resilience of information systems in the face of disruptions (Law No. 05-20, 2020, Art. 9). This aspect is particularly relevant for artificial intelligence systems deployed in critical sectors, where a service interruption could have significant consequences, particularly in economic or social terms.

Thus, Law No. 05-20 contributes to securing the technical environment in which artificial intelligence systems operate, by imposing a set of organisational and technical standards that determine their reliability.

- Infrastructure-focused regulation: the limitations of an indirect approach to artificial intelligence

Despite its importance, Law No. 05-20 remains fundamentally focused on the technical and organisational aspects of cybersecurity, without addressing the substantial challenges associated with the operation of artificial intelligence systems. This limitation stems from the very purpose of the legislation, which aims primarily to protect information systems against

cyber threats, rather than to regulate algorithmic decision-making processes.

Indeed, whilst the law defines cybersecurity as the set of measures designed to guarantee the availability, integrity and confidentiality of information systems (Law No. 05-20, 2020, Art. 2), it does not address issues relating to the transparency of algorithms, the accountability of automated decisions or the risks of algorithmic discrimination. Yet these issues lie at the heart of contemporary legal challenges related to artificial intelligence.

Similarly, the audit mechanisms provided for by the law, particularly for sensitive information systems, focus primarily on the technical security of infrastructure rather than on the evaluation of the algorithmic models themselves. The audit aims to verify the systems' compliance with cybersecurity requirements, without incorporating an analysis of bias, explainability or the decision-making logic of the algorithms.

This disconnect reveals a structural limitation of the framework: the regulation of artificial intelligence is approached through its technical underpinnings, without taking into account its functional dimension. In other words, the law guarantees the security of the conditions under which the algorithm operates, but not the legitimacy of its results.

The result is a partial approach to regulation which, whilst essential, cannot on its own address the challenges posed by artificial intelligence. System security is a necessary, but not sufficient, condition for a comprehensive legal framework for algorithmic technologies.

2.2.3. The Code of Obligations and Contracts: civil liability in crisis in the face of artificial intelligence

Moroccan civil liability law, as set out in the Dahir establishing the Code of Obligations and Contracts, is based on a traditional legal framework centred on the relationship between fault, damage and causation. This model, historically designed to address individualised human behaviour, assumes that the event giving rise to the damage is attributable to a specific person and that it can be analysed through traditional legal categories. However, the emergence of artificial intelligence systems, characterised by their functional autonomy and learning capacity, highlights the structural limitations of this framework. The application of the provisions of the DOC to situations involving algorithmic systems thus reveals a growing tension between the requirements of positive law and contemporary technological realities.

- Fault-based liability: a theoretical construct undermined by the depersonalisation of the harmful act

The tort law regime in Moroccan law is based on Article 77 of the Code of Obligations and Contracts, which provides that any human act causing damage obliges the perpetrator to pay compensation, provided that such act constitutes the direct cause of the damage (Code of Obligations and Contracts, 1913, Art. 77). This provision establishes a fundamental requirement: that the damage must be linked to identifiable human conduct. Article 78 supplements this provision by defining fault as the omission of a required act or the commission of a prohibited act, even in the absence of intent to cause harm (Code of Obligations and Contracts, 1913, Art. 78). Civil liability is thus based on a subjective logic, centred on the conduct of a legal person.

However, artificial intelligence represents a significant departure from this concept. Damage may result from an autonomous algorithmic process, the operation of which relies on learning and adaptation mechanisms that are, in part, beyond the direct control of their designers or users. In such a scenario, identifying fault becomes particularly problematic, insofar as the harmful event no longer stems from immediately perceptible human behaviour, but from an algorithmic decision-making sequence. This depersonalisation of the causative event leads to a dilution of liability amongst a multitude of actors – designer, developer, data provider, user – without it being possible to isolate a legally defined fault.

Furthermore, the requirement for a direct causal link, set out in Article 77, is itself undermined. Artificial intelligence systems operate according to probabilistic logic, in which the result stems from a combination of variables rather than a linear causal relationship. Consequently, establishing a direct link between a specific event and the damage becomes uncertain. This evidential difficulty is compounded by the opacity of algorithms, which prevents access to the internal mechanisms that led to the disputed decision. Consequently, the victim faces a practical impossibility of proving fault and causation, conditions that are nevertheless essential for the application of liability under Articles 77 and 78 of the DOC.

Consequently, the fault-based liability model, as conceived by the Moroccan legislature, appears structurally ill-suited to artificial intelligence systems, due to its reliance on a framework of identifiable human behaviour and direct causality.

- Liability for things: a limited avenue for adaptation in the face of algorithmic autonomy

In view of the difficulties in directly attributing fault, the DOC provides for a mechanism of liability for things, enshrined in Article 88, according to which any person is liable for damage caused by things in their custody, provided that such things are the direct cause of the damage, unless the existence of a fortuitous event, force majeure or the victim's fault can be demonstrated (Code of Obligations and Contracts, 1913, Art. 88). This regime has a notable feature: it is based not on fault, but on the custody of the thing, which allows for a partial objectification of liability.

In the context of artificial intelligence, this mechanism could, on the face of it, provide a relevant legal basis, by treating the algorithmic system as a 'thing' within the meaning of Article 88. The liable party would then be the one exercising power of use, direction and control over the system. However, this transposition faces several conceptual limitations.

Indeed, the concept of custody implies effective control over the thing. However, artificial intelligence systems, particularly those with learning capabilities, can evolve autonomously, producing results not anticipated by their user. This relative autonomy calls into question the very idea of control, which nevertheless forms the basis of the custodian's liability. Consequently, it becomes difficult to determine whether the user, the designer or another party can be classified as a custodian within the meaning of Article 88. Furthermore, Article 88 requires that the thing be the direct cause of the damage. However, as with liability for fault, algorithmic causality is diffuse and probabilistic in nature, which complicates the fulfilment of this requirement. Thus, although liability for things offers a theoretical avenue for adaptation, it remains insufficient to fully grasp the specific characteristics of artificial intelligence systems.

- Contractual liability and the limits of the consumer protection framework

Contractual liability constitutes another mechanism capable of regulating artificial intelligence systems, particularly in relations between technology providers and users. In accordance with Article 230 of the Civil Code, legally binding obligations are binding on those who have entered into them, which implies that failure to perform them gives rise to the debtor's liability. This principle allows, in theory, for the failures of an artificial intelligence system to be attributed to the supplier, on the basis of a breach of their contractual obligations.

However, this framework has significant structural limitations. On the one hand, it presupposes the existence of a contractual relationship, which excludes third-party victims, even though artificial intelligence systems may have effects on persons who are not parties to the contract. On the other hand, contractual practice tends to include clauses limiting or excluding liability, which reduce the effective scope of this mechanism.

Law No. 31-08 on consumer protection provides a partial remedy for this situation. Article 3 imposes a general duty of information on the supplier, aimed at enabling the consumer to ascertain the essential characteristics of the product or service (Law No. 31-08, 2011, Art. 3). Furthermore, Article 15 defines as an unfair term any stipulation creating a significant imbalance to the detriment of the consumer (Law No. 31-08, 2011, Art. 15). Nevertheless, these mechanisms remain insufficient in light of the specific characteristics of artificial intelligence. The duty to provide information does not guarantee an effective understanding of algorithmic systems, the functioning of which remains opaque. Similarly, the sanctioning of unfair terms does not allow for an understanding of the issues related to the internal logic of the systems, particularly with regard to automated decision-making.

2.2.4. Intellectual property and Law No. 2-00: the inadequacy of the anthropocentric conception of authorship in the face of creations generated by artificial intelligence

Moroccan intellectual property law, as set out in Law No. 2-00 on copyright and related rights, is based on a fundamentally anthropocentric conception of creation. This conception, inherited from classical copyright traditions, establishes an intrinsic link between the work and the natural person who created it. However, the emergence of artificial intelligence systems, capable of autonomously producing content of high creative value, highlights the structural limitations of this paradigm. An analysis of the provisions of Law No. 2-00 thus reveals a growing mismatch between existing legal categories and the new forms of creation arising from algorithmic technologies.

- The legal definition of the author: an explicitly human construct excluding artificial intelligence

Law No. 2-00 adopts an explicit conception of the author, defining them as a natural person who is the originator of the creation. Article 1 indeed provides that 'the author is the natural person who created the work' (Law No. 2-00, 2000, Art. 1). This definition is decisive in that it excludes, as a matter of principle, any entity lacking legal personality and subjectivity, in particular artificial intelligence systems.

This conception is reinforced by the general structure of the text, particularly through the provisions relating to moral and economic rights. Article 9 enshrines moral rights attached to the person of the author, such as the right of authorship and the right to respect for the integrity of the work (Law No. 2-00, 2000, Art. 9). These prerogatives necessarily imply the existence of a subject endowed with consciousness and will, capable of maintaining a personal connection with their work.

Similarly, Article 10 confers upon the author a set of exclusive economic rights, including in particular the right of reproduction, adaptation and communication to the public (Law No. 2-00, 2000, Art. 10). These rights reflect a logic of legal ownership based on the existence of an identifiable holder, which, once again, excludes artificial intelligence systems.

Thus, under current Moroccan law, an artificial intelligence system cannot be classified as an author. This exclusion is not implicit, but results directly from the legal definition of the author, which constitutes a conceptual barrier preventing any legal recognition of algorithmic creation as a work attributable to a non-human entity.

- The criterion of originality: an implicit requirement for a human imprint thwarted by algorithmic creation

Under Moroccan law, copyright protection is conditional upon the existence of an original work. Article 3 of Law No. 2-00 specifies that protection applies to works constituting 'original intellectual creations' (Law No. 2-00, 2000, Art. 3). Although the text does not explicitly define originality, it is traditionally understood as the expression of the author's personality.

However, this requirement comes into direct conflict with the characteristics of artificial intelligence systems. The content generated by these systems is the result of an algorithmic process based on the statistical analysis of data and the reproduction of existing structures, without it being possible to identify any direct human creative input in the final result.

Two situations must therefore be distinguished. Where artificial intelligence is used merely as a tool at the service of a human author, originality may be attributed to the latter's intervention, particularly through the creative choices made in the design or use of the system. Conversely, when the artificial intelligence system produces content autonomously, without identifiable human intervention in the creative act, the classification of the work as original becomes legally uncertain.

Indeed, the absence of a personal human imprint leads, in principle, to the exclusion of copyright protection. This solution, whilst consistent with the logic of the text, produces a paradoxical effect: content that appears to be creative may find itself deprived of any legal protection due to the absence of an identifiable human author. This situation highlights the limitations of the originality criterion as it is currently conceived.

- The question of rights ownership: a regulatory gap regarding creations generated by artificial intelligence

The exclusion of artificial intelligence from the status of author gives rise to a major related difficulty: that of determining the rights holder of the generated works. Indeed, the legal system is based on the idea that rights arise for the benefit of the author, a natural person, and may then be transferred to successors in title or legal persons (Law No. 2-00, 2000, Art. 11).

However, in the case of a work generated autonomously by an artificial intelligence system, no human author can be identified as the original rights holder. This situation creates a significant regulatory gap, insofar as the law provides for no specific mechanism for attributing rights in such a scenario.

Several theoretical solutions may be considered, such as attributing rights to the system's designer, the user, or the person who provided the data. However, none of these solutions finds explicit support in Law No. 2-00. In the absence of a clear legal classification, these creations risk falling outside the scope of protection, which creates legal uncertainty detrimental to both economic actors and users.

This gap highlights a structural limitation of Moroccan intellectual property law, which remains structured around the figure of the human author, without incorporating the new forms of creation arising from artificial intelligence.

- The use of protected works in the training of artificial intelligence systems: a tension between innovation and protection

Another major issue lies in the use of copyright-protected works in the training of artificial intelligence systems. Article 10 of Law No. 2-00 grants the author an exclusive right to reproduce and adapt their work (Law No. 2-00, 2000, Art. 10). Furthermore, Article 1 specifies that reproduction includes, in particular, the storage of a work in electronic form, even if only temporarily (Law No. 2-00, 2000, Art. 1).

However, the training of artificial intelligence models specifically involves the mass reproduction of content, often protected, in order to enable the system to learn structures and correlations. In the absence of authorisation from the rights holders, these operations could, in principle, be classified as infringements of copyright.

Admittedly, the law provides for certain exceptions, notably reproduction for private or educational purposes (Law No. 2-00, 2000, Articles 12 and 15), but these appear difficult to apply to the practices of training artificial intelligence models, which are part of an industrial and commercial framework.

Furthermore, Moroccan law does not currently provide for a specific framework governing 'text and data mining', unlike certain developments observed in other legal systems. This absence creates significant legal uncertainty, insofar as artificial intelligence stakeholders operate within an uncertain regulatory environment, oscillating between the risk of infringement and the need for innovation.

An analysis of Law No. 2-00 highlights a profound mismatch between Moroccan intellectual property law and contemporary technological realities. The strictly human definition of the author, the requirement for originality based on a personal imprint, the absence of rules regarding ownership of works generated by artificial intelligence, and the text's silence on model training reveal a structural inadequacy in the current legal framework.

This situation underscores the need for regulatory change, either through the introduction of a specific regime applicable to creations generated by artificial intelligence, or through an adaptation of traditional copyright concepts. Failing this, positive law risks being progressively marginalised in the face of the profound changes in modes of creation brought about by algorithmic technologies.

3. Contributions from international law

The legal framework for artificial intelligence cannot be addressed exclusively at the national level. Indeed, data flows, the dematerialisation of digital services and the interconnection of information systems give AI an intrinsically transnational dimension. In this context, Morocco, as a State party to several international instruments, is subject to a set of obligations that contribute, directly or indirectly, to the regulation of algorithmic systems.

However, whilst these instruments help to establish a regulatory framework, their adaptation to the specificities of artificial intelligence remains incomplete, revealing a disconnect between existing international legal frameworks and contemporary technological developments.

3.1. Convention 108: a foundational international framework but one not originally designed for artificial intelligence

The legal framework for artificial intelligence cannot be addressed exclusively at the national level, insofar as data flows, the dematerialisation of digital services and the interconnection of information systems confer an intrinsically transnational dimension on these technologies. In this context, Morocco's accession to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (known as Convention 108) marks its integration into a key international framework for data protection. Deposited on 28 May 2019, the instruments of ratification enabled the Convention to enter into force for the Kingdom on 1 September 2019, thereby confirming its commitment to a universal regulatory system. Convention 108 is, in fact, the main legally binding international instrument open to states beyond the European framework in the field of personal data protection.

The core of this framework rests on the protection of the fundamental rights and freedoms of natural persons in the face of automated data processing. Article 1 of the Convention explicitly states that its objective is to guarantee to every person respect for their fundamental rights, and in particular their right to privacy, with regard to the automated processing of personal data concerning them (Convention 108, 1981, Art. 1). This purpose gives the Convention a cross-cutting scope, in that it regulates all automated processing operations, regardless of the sector concerned.

In this regard, the Convention establishes a set of fundamental guiding principles. Article 5 imposes requirements regarding data quality, stipulating in particular that data must be collected fairly, for specified and legitimate purposes, and that it must be adequate, relevant and not excessive in relation to those purposes (Convention 108, 1981, Art. 5). Article 7, for its part, requires the implementation of appropriate security measures to protect data against the risks of unauthorised access, loss or destruction (Convention 108, 1981, Art. 7). Finally, Article 8 enshrines a set of rights for data subjects, in particular the right of access, rectification and redress (Convention 108, 1981, Art. 8). These provisions constitute an essential normative framework, fully applicable to artificial intelligence systems due to their structural dependence on data.

Furthermore, the Convention helps to regulate cross-border data flows, a key factor in the development of artificial intelligence technologies. Article 12 provides that States Parties may not, for the sole purpose of protecting privacy, restrict data transfers to another State Party, thereby enshrining a principle of free movement conditional upon the existence of an adequate level of protection (Convention 108, 1981, Art. 12). This provision helps to facilitate international data exchanges whilst maintaining a minimum level of safeguards, which is particularly relevant in a globalised digital environment.

However, despite its foundational scope, Convention 108 has a key limitation in the contemporary context. Adopted in 1981, it was designed in a technological environment predating the emergence of modern artificial intelligence. Whilst it provides a framework for automated data processing, it does not address specific issues related to advanced algorithmic systems, such as complex automated decision-making, algorithmic bias or the requirement for model explainability. This shortcoming reveals a disconnect between the original regulatory framework and current technological developments.

It is precisely in this context that the 2018 Amending Protocol, known as 'Convention 108+', comes into play, aiming to modernise the framework. This text retains the Convention's general structure whilst substantially strengthening the obligations placed on data controllers. In particular, it introduces heightened transparency requirements, mandating enhanced information for data subjects (Convention 108+, 2018, Art. 8), as well as a principle of accountability, requiring data controllers to demonstrate the lawfulness of their processing activities (Convention 108+, 2018, Art. 10). Furthermore, it enshrines a risk management approach, requiring a prior assessment of the impact of processing on individuals' rights and freedoms (Convention 108+, 2018, Art. 10).

Above all, the modernised Convention introduces safeguards directly relevant to artificial intelligence. Article 9 thus enshrines the right not to be subject to a decision producing significant effects based exclusively on automated processing, without taking into account the views of the data subject (Convention 108+, 2018, Art. 9). This provision represents a major step forward, in that it explicitly addresses the risks associated with automated decision-making, which lies at the heart of artificial intelligence systems.

Nevertheless, the effectiveness of these safeguards depends largely on their implementation at national level. The Convention requires States Parties to take the necessary measures to give effect to its principles in their domestic law (Convention 108, 1981, Art. 4), whilst the modernised version provides for the establishment of independent supervisory authorities with investigative and sanctioning powers (Convention 108+, 2018, Art. 15). In the Moroccan context, this requirement relates directly to the role of the CNDP, whose effectiveness determines the actual scope of these international standards.

Thus, Convention 108 and its modernised version constitute a fundamental international framework for the regulation of artificial intelligence systems, providing general principles applicable to data processing. However, their adaptation to the technical and functional specificities of artificial intelligence remains incomplete, which highlights the need for further regulatory development at the international level.

3.2. International intellectual property instruments: indirect and incomplete regulation of creations resulting from artificial intelligence

Morocco is a party to several key international instruments on intellectual property, foremost among which are the Berne Convention for the Protection of Literary and Artistic Works and the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). Although these instruments do not specifically target artificial intelligence, they indirectly contribute to its regulation by establishing the conditions for the protection, exploitation and circulation of works and intangible assets at the international level.

The Berne Convention is based on a set of fundamental principles, notably the principle of protection without formalities, the principle of national treatment and that of the independence of protection. These principles, enshrined in particular in Article 5, imply that literary and artistic works enjoy automatic protection in the contracting states, without the need for prior registration, and that foreign authors enjoy the same rights as nationals. This normative framework is indirectly incorporated into the TRIPS Agreement, which requires Member States of the World Trade Organisation to comply with the substantive provisions of the Berne Convention (TRIPS Agreement, 1994, Art. 9). Thus, international intellectual property law is based on a cumulative normative framework, within which the TRIPS Agreement plays a role in unifying and strengthening standards.

The TRIPS Agreement, for its part, constitutes a central instrument in that it establishes minimum standards of protection applicable to all WTO member states. It requires states to ensure effective protection of intellectual property

rights in various fields, including copyright, trade marks, patents and designs (TRIPS Agreement, 1994, Art. 1 et seq.). With regard to copyright, Article 10 explicitly provides that computer programs are protected as literary works, and that compilations of data may also be protected where they constitute intellectual creations by reason of the selection or arrangement of their contents (TRIPS Agreement, 1994, Art. 10). These provisions are of particular importance in the context of artificial intelligence, insofar as they allow certain essential elements of algorithmic systems—notably software and certain databases—to be brought within the scope of intellectual property.

However, the contribution of these instruments to the regulation of artificial intelligence remains indirect and limited. Firstly, they are based on a traditional conception of creation, founded on human intervention. Whilst the texts do not expressly define the author as a natural person, their general framework—notably through the reference to rights arising from the Berne Convention—is based on such a conception. Consequently, they do not allow for the recognition of artificial intelligence systems as rights holders, which aligns with the limitations observed in Moroccan domestic law.

Secondly, these instruments do not explicitly address the issue of the use of protected works in the context of training artificial intelligence systems. However, Article 9 of the TRIPS Agreement specifies that copyright protection extends to expressions and not to ideas, whilst the articles relating to exclusive rights imply that any unauthorised reproduction or use of a work is likely to constitute an infringement of the rights of the right holder (TRIPS Agreement, 1994, Articles 9 and 13). In this context, the training practices for artificial intelligence models, based on the mass reproduction of protected content, could in principle fall within the scope of these prohibitions. However, in the absence of specific provisions governing such uses, international law leaves a zone of legal uncertainty.

Furthermore, the TRIPS Agreement specifies that protection extends to expressions but not to ideas, procedures or methods of operation (TRIPS Agreement, 1994, Art. 9, para. 2). This distinction is of particular importance for artificial intelligence, insofar as the algorithmic models themselves could be regarded as methods or processes, which may fall outside the scope of copyright protection. This situation further complicates the legal regime applicable to AI systems.

Finally, these instruments contain no provisions relating to creations generated autonomously by artificial intelligence systems. They do not allow for determining whether such creations should be protected, nor for identifying a potential rights holder. This lack of legal classification constitutes a major regulatory gap, giving rise to legal uncertainty, particularly in economic sectors based on the automated production of content.

As a result, international intellectual property law, whilst imposing substantial obligations on States regarding the protection of intellectual creations, remains structurally ill-suited to the changes brought about by artificial intelligence. Designed to regulate human creative activities, it is only able to address algorithmic systems in an indirect and fragmentary manner. This situation highlights the need for the international framework to evolve in order to incorporate the specific characteristics of artificial intelligence, particularly regarding ownership of rights, the use of training data and the legal classification of generated creations.

4. The structural conceptual limitations of the current model

4.1. The collapse of the traditional causal link

Moroccan civil liability law, as set out in the Dahir establishing the Code of Obligations and Contracts, is based on a classical framework in which the causal link constitutes a central condition for the imposition of liability. Article 77 provides that any human act causing damage obliges its perpetrator to pay compensation, provided it is established that the act is the direct cause (Code of Obligations and Contracts, 1913, Art. 77). Article 78 supplements this requirement by specifying that liability also presupposes the existence of a fault having caused the damage, which must itself have a direct causal link with the harm suffered (Code of Obligations and Contracts, 1913, Art. 78). It follows that the Moroccan legal system is based on a rigorous and demanding conception of causation, founded on the identification of a direct chain of events between a triggering event and a specific loss.

This framework follows a classical logic, both linear and deterministic, whereby an identifiable behaviour produces an identifiable effect. Legal causation is thus conceived as a direct, continuous and intelligible relationship between a human action and its harmful consequences. This model presupposes not only the possibility of isolating a specific triggering event, but also that of demonstrating its decisive causal role in the occurrence of the damage.

However, the emergence of artificial intelligence systems, particularly those based on machine learning mechanisms, profoundly challenges this framework. These systems are

characterised by their ability to evolve autonomously after being deployed, by integrating new data and modifying their internal parameters without direct human intervention. Consequently, algorithmic behaviour can no longer be understood as the mere execution of predefined instructions, but as a dynamic and evolving process, capable of producing results not anticipated by its designers or users.

In this context, the damage no longer necessarily results from a single identifiable event, but from a complex chain of interdependent factors. The initial training data, system updates, interactions with the digital environment and conditions of use all contribute jointly to the production of the algorithmic result. This multiplicity of causes makes it particularly difficult to identify a direct cause within the meaning of Articles 77 and 78 of the Swiss Code of Obligations and Contracts. The causal link thus tends to become diluted within a distributed decision-making chain, in which no single element can be isolated as being, on its own, decisive.

This difficulty is compounded by the opacity of algorithmic systems, which limits the ability to access the internal mechanisms that led to the production of the disputed result. The impossibility of explaining precisely how the system works undermines the demonstration of the direct causal link required by positive law. The victim is thus faced with a situation in which they must establish a causal link whose constituent elements are largely inaccessible to them.

This results in a profound alteration of the traditional causal model. Algorithmic causality appears diffuse, evolving and partially unpredictable, which contradicts the requirement for direct and certain causality set out in Articles 77 and 78 of the Swiss Code of Obligations and Contracts. Consequently, the existing legal framework proves structurally unsuited to addressing the harm caused by artificial intelligence systems, highlighting the need to reconfigure the foundations of civil liability to take account of the specific characteristics of these technologies.

4.2. The multiplicity of actors and the inefficiency of the allocation of liability

Artificial intelligence is characterised by a complex technical and functional structure, based on a fragmented value chain in which a multitude of actors are involved at different stages of the system's life cycle. This multitude includes, in particular, algorithm designers, data providers, infrastructure operators, technical integrators and end users. Such an organisation, based on the interdependence of contributions, differs profoundly from the situations envisaged by traditional civil liability law, which relies on the identification of a specific party responsible for the damage.

Indeed, the Swiss Code of Obligations and Contracts structures civil liability around a logic of individualised attribution. Article 77 makes the incurrence of liability contingent upon the existence of a human act constituting the direct cause of the damage, whilst Article 78 links this liability to the fault of the perpetrator, which must itself be the direct cause of the harm (Swiss Code of Obligations and Contracts, 1913, Articles 77 and 78). This model thus presupposes the possibility of identifying a specific legal person to whom the triggering event can be attributed with certainty. It is based on a unitary conception of liability, in which the damage is attributed to a clearly identifiable perpetrator.

However, this logic is profoundly challenged by artificial intelligence systems, whose operation results from continuous interaction between multiple actors. The damage may be linked to the initial design of the algorithm, the quality of the training data, the technical operating conditions, or even the use made of it. This multiplicity of factors makes it particularly difficult to identify a single triggering event that meets the requirements of Articles 77 and 78 of the Swiss Code of Obligations and Contracts. Liability thus tends to be fragmented amongst several parties, without it being possible to determine with certainty the respective share of each in causing the damage.

Admittedly, the Swiss Code of Obligations and Contracts provide mechanisms for extending liability beyond personal acts. Article 85 establishes vicarious liability, setting out the principle that a person may be held liable for damage caused by persons for whom they are responsible, particularly in the context of relationships of authority or supervision (Code of Obligations and Contracts, 1913, Art. 85). Similarly, Article 88 establishes liability for the acts of things, under which a person may be held liable for damage caused by things in their custody, provided that these are the direct cause of the damage (Code of Obligations and Contracts, 1913, Art. 88). These mechanisms reflect the legislator's intention to broaden the grounds for liability in order to cover situations in which the harmful event does not directly result from a personal act.

However, these regimes remain ill-suited to the complexity of artificial intelligence systems. Liability for the acts of others is based on the existence of a clearly established relationship of authority or supervision, which does not correspond to the nature of the relationships between the various actors in the algorithmic ecosystem, who operate autonomously and without a direct legal hierarchy. Similarly, liability for things presupposes the identification of a custodian exercising

control over the thing, as well as the existence of a direct causal link between that thing and the damage. However, in the case of artificial intelligence systems, control is often distributed among several actors, and the system itself evolves dynamically, which makes it uncertain who qualifies as a custodian within the meaning of Article 88.

In practice, this multiplicity of actors leads to a dilution of liability, insofar as the damage appears to be the result of a chain of technical and human interactions that are difficult to disentangle. This situation undermines the effectiveness of the right to compensation, by making it uncertain who is liable for the obligation to pay compensation. The victim is thus faced with increased evidential complexity, linked to the need to identify, from among a multitude of actors, the one whose conduct meets the conditions set out in Articles 77 and 78 of the Code of Obligations and Contracts.

As a result, Moroccan positive law does not currently provide a structured mechanism allowing for a clear and consistent allocation of liability in complex algorithmic environments. The absence of legal criteria suited to the plurality of actors and the interdependence of contributions reveals a structural shortcoming in the traditional model of civil liability, which appears to be based on an individualistic conception ill-suited to the technical realities of artificial intelligence.

4.3. The evidential challenge posed by complex algorithms

Moroccan civil liability law, as set out in the Code of Obligations and Contracts, is based on a fundamental principle whereby it is incumbent upon the victim to establish the constituent elements of liability, namely the triggering event, the damage and the causal link. Article 77 requires that a human act constituting the direct cause of the damage be demonstrated, whilst Article 78 makes liability contingent upon the existence of a fault that itself caused the damage (Code of Obligations and Contracts, 1913, Articles 77 and 78). This requirement necessarily implies that the facts giving rise to the damage must be accessible, identifiable and legally intelligible, so as to enable the victim to adduce evidence of them.

This evidentiary model is, however, profoundly undermined by the technical characteristics of artificial intelligence systems, particularly those based on deep learning mechanisms. These systems rely on complex computational architectures, the internal workings of which are difficult to interpret, even by their designers. The decision-making process no longer takes the form of a chain of explicit instructions, but rather the result of algorithmic processing involving a multitude of parameters and successive adjustments. In this context, identifying the event giving rise to the damage becomes particularly difficult, insofar as it does not correspond to a directly observable human act, but to an opaque technical process.

This opacity creates a significant information asymmetry between the various actors in the system and the victim. Designers and operators have, in principle, privileged access to the system's data, models and parameters, whilst the victim remains outside this process. This situation makes it particularly difficult for the victim to establish the elements required by Articles 77 and 78 of the Code of Obligations and Contracts. The victim is, in effect, practically unable to demonstrate the existence of a specific malfunction, to identify the exact source of the damage, or to legally characterise a wrongful act.

This evidential difficulty is all the more pronounced given that Moroccan law does not, as things stand, provide for specific mechanisms to adjust the burden of proof in the field of complex systems. The victim remains obliged to prove a direct causal link, even though such a link is, in the case of artificial intelligence systems, difficult to perceive and objectify. This requirement is also found in the regime governing liability for defective products, where the victim must establish the damage and the link between it and the product defect (Code of Obligations and Contracts, 1913, Art. 106-7). Here too, the technical complexity of the systems makes this demonstration particularly demanding.

Under these circumstances, the burden of proof appears particularly heavy, and in some cases even insurmountable. The inability to access the decisive technical elements and to reconstruct the algorithmic reasoning leads to a situation in which the conditions for liability, although formally met in law, cannot be effectively demonstrated in practice. This results in a breach of the effectiveness of the right to compensation, insofar as the victim, being unable to meet the evidential requirements set out in Articles 77 and 78 of the Swiss Code of Obligations and Contracts, is deprived of the possibility of obtaining compensation.

Thus, the traditional evidential regime appears structurally ill-suited to the specific characteristics of artificial intelligence systems. Based on a logic of accessibility and intelligibility of the facts, it comes up against the technical opacity and complexity of algorithmic systems, revealing a new conceptual limitation of the current model of civil liability.

4.4. The absence of a legal definition and classification of risks

Moroccan law, as it currently stands, contains no legal definition of an 'artificial intelligence system'. None of the applicable legislation – whether the Code of Obligations and Contracts, Law No. 09-08 on the protection of personal data, or the legislation on cybersecurity – provides an explicit legal definition that would define the scope of this concept. This lack of definition reflects a significant regulatory gap, insofar as it deprives positive law of a conceptual anchor that is essential to any regulatory endeavour.

Indeed, legal classification constitutes an essential preliminary step in legal reasoning, in that it determines the identification of the applicable legal regime. In the absence of a precise definition, artificial intelligence systems can only be understood through pre-existing legal categories, applied indirectly and often by analogy. This situation creates uncertainty regarding the applicability of existing rules, particularly in the area of civil liability, insofar as it is not always possible to determine whether a given system falls under a specific legal classification or whether it should be treated as a mere object, a service or a product.

This conceptual uncertainty is all the more problematic given that artificial intelligence systems come in a wide variety of forms and functions. Some systems are limited to assistance or recommendation functions, whilst others are capable of producing decisions with significant legal or economic effects. In the absence of a legal definition, these differences in nature and impact are not clearly reflected in the law, leading to an undifferentiated application of legal rules.

Furthermore, Moroccan law provides for no mechanism to classify artificial intelligence systems according to their level of risk. Unlike a differentiated approach that would allow legal obligations to be tailored to the seriousness of the issues at stake, the current legal framework is based on a uniform approach. The applicable rules do not distinguish between low-impact systems, such as recommendation or assistance tools, and high-impact systems, particularly when they operate in sensitive areas such as health, justice or security.

This lack of regulatory gradation has two consequences. On the one hand, it leads to insufficient regulation for high-risk systems, insofar as these are not subject to any specific, enhanced requirements. On the other hand, it can result in a lack of proportionality in the regulation of low-risk systems, which are subject to the same general rules without any account being taken of their actual impact. Positive law thus appears incapable of prioritising risks, a task that is nevertheless essential in a technological environment characterised by a high degree of heterogeneity in usage.

This results in a structural gap in the Moroccan legal framework, which does not allow for a differentiated approach to the specific challenges associated with different types of artificial intelligence systems. This gap prolongs and exacerbates the limitations identified in the preceding sections, depriving the law of a conceptual tool essential to the organisation of coherent and effective regulation.

5. The European model: towards allocated liability and appropriate presumptions

The European Union has adopted Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence, commonly referred to as the 'AI Act'. This text, which entered into force on 1 August 2024, constitutes the first horizontal legal framework specifically dedicated to artificial intelligence on a global scale. It aims to establish a uniform framework governing the development, placing on the market, putting into service and use of artificial intelligence systems within the internal market, whilst ensuring a high level of protection of fundamental rights, health and safety (Regulation (EU) 2024/1689, 2024, recital 1).

The originality of this Regulation lies in the adoption of a structured, risk-based approach, allowing legal obligations to be tailored to the severity of the potential risks associated with artificial intelligence systems. This approach marks a departure from traditional approaches based on uniform regulation, introducing a differentiated and proportionate model centred on risk prevention and the accountability of actors in the value chain.

5.1. Risk classification and the adaptation of obligations

Regulation (EU) 2024/1689 is based on a regulatory framework founded on a graduated classification of artificial intelligence systems according to their level of risk. This approach is expressly enshrined in the Regulation, which provides for the establishment of proportionate rules taking into account the intensity and nature of the risks likely to be generated by these systems (Regulation (EU) 2024/1689, 2024, recital 26). It forms the core of the European framework and reflects a desire to reconcile technological innovation with the protection of fundamental interests.

Four categories of risk are thus distinguished, each giving rise to a specific legal regime. Firstly, certain artificial intelligence systems are classified as posing an unacceptable risk and are, as such, subject to an outright ban. These include, in

particular, systems using subliminal or manipulative techniques capable of significantly altering individuals' behaviour, or those implementing social scoring mechanisms, deemed contrary to the fundamental values of the European Union (Regulation (EU) 2024/1689, 2024, recitals 28 and 31). These prohibitions reflect an approach based on the protection of fundamental rights, by excluding certain practices deemed intrinsically incompatible with human dignity and democratic principles.

Secondly, artificial intelligence systems classified as 'high-risk' are subject to particularly strict regulation. These systems relate in particular to sensitive areas such as critical infrastructure, education, employment, access to essential services and law enforcement activities. The Regulation imposes a set of substantial obligations on these systems, including the establishment of risk management systems, ensuring the quality of the data used, technical documentation, the traceability of operations, the transparency of systems, and the introduction of effective human oversight (Regulation (EU) 2024/1689, 2024, recitals 7 and 9). This enhanced regulation aims to prevent infringements of fundamental rights and to guarantee the reliability of systems in the most sensitive contexts.

Thirdly, systems presenting a limited risk are subject to specific transparency obligations. These obligations are designed, in particular, to inform users when they interact with an artificial intelligence system or when content is generated automatically. Finally, systems posing minimal risk are exempt from any binding legal constraints, with the Regulation merely encouraging the adoption of voluntary codes of conduct to promote good practices (Regulation (EU) 2024/1689, 2024, recital 26).

This graduated classification constitutes a major innovation in technology regulation law. It enables the establishment of a genuine principle of normative proportionality, by adapting the intensity of legal obligations to the level of risk posed by artificial intelligence systems. This model differs markedly from current Moroccan law, which provides neither a legal definition of artificial intelligence systems nor a risk classification mechanism, leading to a uniform and undifferentiated application of legal rules.

5.2. The allocation of liability throughout the value chain

Regulation (EU) 2024/1689 establishes a particularly structured mechanism for allocating legal obligations along the value chain of artificial intelligence systems. Unlike traditional approaches based on identifying a single responsible party, the European framework is based on a functional approach, in which obligations are distributed among the various operators according to their actual role in the system's lifecycle. This regulatory framework reflects the European legislator's intention to take account of the complexity of the technical and economic ecosystems specific to artificial intelligence, characterised by the successive and interdependent involvement of multiple actors.

With this in mind, the Regulation identifies several categories of operators, including suppliers, importers, distributors and deployers, each of whom is subject to specific obligations. This classification is part of an approach to differentiated accountability, designed to ensure that legal requirements—particularly regarding safety, compliance and risk management—are effectively met by the actors best placed to implement them.

Article 25 of the Regulation plays a central role in this regard by establishing a mechanism for the functional reclassification of operators. It provides that certain actors, initially classified as distributors, importers or deployers, may be treated as suppliers of high-risk artificial intelligence systems in specific circumstances. This is notably the case where an operator makes a substantial modification to the system, alters its intended use so as to bring it within the category of high-risk systems, or markets the system under its own name or brand (Regulation (EU) 2024/1689, 2024, Art. 25). Through this mechanism, the Regulation shifts regulatory responsibility to the actor exercising effective control over the system, regardless of their initial role in the distribution chain.

This mechanism moves beyond the traditional approach to liability, which is based on a single party being held responsible for the damage, by introducing a dynamic and evolving approach to liability. It should be noted, however, that the Regulation does not, at this stage, establish a system of civil liability in the strict sense, but rather a system for allocating regulatory obligations. It is, above all, a preventive mechanism, designed to ensure the compliance of artificial intelligence systems before any harm occurs, by imposing on each actor obligations tailored to their level of involvement.

The value of this approach lies in its ability to address the complexity of artificial intelligence value chains, thereby avoiding the dilution of liability observed in traditional legal systems. By allocating obligations according to the power to control and intervene in the system, the Regulation ensures better traceability of responsibilities and strengthens the effectiveness of legal requirements. This approach stands in stark contrast to Moroccan civil liability law, which remains structured around an individualistic and unitary conception of

liability, as evidenced by Articles 77 and 78 of the Code of Obligations and Contracts.

Thus, the European model is distinguished by the introduction of functional and distributed liability, adapted to the technical reality of artificial intelligence systems. This development reflects a paradigm shift, in which regulation no longer relies exclusively on ex post compensation for damage, but on an ex-ante organisation of obligations aimed at preventing risks and regulating the behaviour of actors throughout the value chain.

5.3. Presumptions of evidence and the reduction of the victim's burden

In addition to Regulation (EU) 2024/1689 on artificial intelligence, European Union law has envisaged a strengthening of the civil liability framework through the proposal for a directive on the adaptation of the rules on non-contractual liability to artificial intelligence, presented by the European Commission on 28 September 2022 (European Commission, 2022). This initiative is part of an effort to correct the structural imbalances caused by artificial intelligence systems, particularly in the area of evidence, due to the information asymmetry between the operators of these systems and potential victims (De Bruyne et al., 2023).

One of the key contributions of this proposal lies in the introduction of innovative evidentiary mechanisms designed to facilitate access to evidence. Firstly, Article 3 establishes a mechanism for the disclosure of evidence, enabling national courts to order the disclosure of relevant information held by providers or operators of artificial intelligence systems, particularly in the case of high-risk systems (European Commission, 2022, Art. 3). This mechanism aims to address the technical opacity of algorithmic systems by enabling the victim to access the evidence necessary to substantiate their claims. It thus constitutes an essential tool for rebalancing civil proceedings by reducing the information asymmetry inherent in machine learning technologies (Madiega, 2023; De Bruyne et al., 2023).

Secondly, Article 4 of the proposal introduces a rebuttable presumption of causation, designed to ease the burden of proof on the victim. This presumption applies where the claimant establishes, on the one hand, a breach of the defendant's legal obligations, in particular those set out in the AI Act, and, on the other hand, that it is reasonably probable that this breach influenced the result produced by the artificial intelligence system, which caused the damage (European Commission, 2022, Art. 4; De Bruyne et al., 2023). It is important to emphasise that this presumption does not relate to the fault itself, but exclusively to the causal link, which remains the most difficult element to establish in the context of algorithmic systems (Li & Schütte, 2024).

The rebuttable nature of this presumption helps to maintain the balance between the parties, insofar as the defendant retains the possibility of demonstrating that the alleged breach did not cause the damage. This is therefore not a complete reversal of the burden of proof, but rather an adjustment of it, justified by the technical complexity of artificial intelligence systems and by the operators' privileged position in accessing relevant information. This mechanism thus constitutes a targeted response to the evidentiary difficulties identified in traditional legal systems.

However, this proposal for a directive has not, to date, led to the adoption of a binding instrument at European Union level. The legislative process has highlighted differences between the European institutions, with the result that no harmonised regime of non-contractual civil liability applicable to artificial intelligence is yet in force. Consequently, the regulation of liability for damage caused by artificial intelligence systems remains largely dependent on the national laws of Member States, despite the existence of sectoral frameworks such as the AI Act.

Furthermore, the Directive on liability for defective products, recently revised at European level, is currently the main instrument applicable in the area of strict liability. However, although this framework has been extended to products incorporating digital components, it provides only a partial response to the specific challenges posed by artificial intelligence, particularly with regard to certain non-material damages and infringements of fundamental rights.

From a comparative perspective, the European model, even in its current incomplete state, stands out for its structured and forward-looking approach to the regulation of artificial intelligence systems. By combining a classification of risks, a functional allocation of obligations among stakeholders and mechanisms for adjusting the burden of proof, it offers a coherent response to the epistemic difficulties posed by algorithmic opacity (Madiega, 2023).

This framework highlights, by implication, the shortcomings of Moroccan law, which remains based on the traditional provisions of the Dahir of 12 August 1913 establishing the Code of Obligations and Contracts. In the absence of evidentiary mechanisms adapted to artificial intelligence systems, the victim is required to establish fault and direct causation in accordance with Articles 77 and 78 of the Code of Obligations and Contracts, or, where applicable, to

establish liability for things on the basis of Article 88, which presupposes the identification of a custodian and a direct causal link (Code of Obligations and Contracts, 1913, Articles 77, 78 and 88). This requirement places victims of algorithmic harm in a situation of structural evidential difficulty.

Thus, although the proposed directive on liability in the field of artificial intelligence has not yet been finalised, it constitutes a particularly relevant source of inspiration for the development of Moroccan law. It highlights the need to introduce mechanisms to ease the burden of proof, such as presumptions of causality or enhanced transparency obligations, in order to ensure the effectiveness of the right to compensation in a technological environment characterised by the complexity and opacity of algorithmic systems.

6. The US model

6.1. Sectoral pragmatism and a pro-innovation approach

The US model for regulating artificial intelligence is characterised by the absence of a unified federal legislative framework and by the adoption of a pragmatic approach based on the use of existing legal instruments. Unlike the European model, which is structured around a single horizontal text, the United States favours fragmented, sector-specific and evolving regulation, based on the intervention of specialised federal agencies and on soft law or executive instruments (Davtyan, 2025; Yoo & Mueller, 2024). This regulatory architecture reflects a structural choice in favour of adaptive regulation, in which the risks associated with artificial intelligence are addressed according to the sectors of application rather than through a comprehensive technological approach.

This approach initially resulted in the adoption of Executive Order 14110 of 30 October 2023, which established a coordinated federal framework aimed at ensuring the safe, secure and trustworthy development and use of artificial intelligence. This document explicitly emphasises the need to manage the risks associated with AI, by mobilising all federal agencies around a common strategy based on security, the protection of fundamental rights and the management of technological risks (The White House, 2023). It thus enshrines a cross-cutting approach based on principles such as system security, the prevention of discrimination, the protection of privacy and respect for consumer rights, reflecting a commitment to substantial regulation of the uses of artificial intelligence.

However, this direction underwent a significant shift with the adoption of Executive Order 14179 of 23 January 2025, entitled ‘Removing Barriers to American Leadership in Artificial Intelligence’. This document forms part of a reorientation of federal policy, aimed at easing certain constraints arising from the previous framework in order to promote innovation and competitiveness. In particular, it provides for the review of measures adopted pursuant to Executive Order 14110, calling on agencies to examine and, where appropriate, suspend, amend or repeal actions that may constitute obstacles to the development of artificial intelligence (The White House, 2025a). This development reflects less a radical break than a reconfiguration of policy priorities, now geared towards maintaining US technological leadership on a global scale, an objective explicitly stated in the text (The White House, 2025a).

In this context, US law on artificial intelligence remains organised along sectoral lines. The absence of general federal legislation does not imply a lack of regulation, but reflects a deliberate choice to tailor the rules to the specific characteristics of each area of application (Dotan, 2024). Consequently, several federal agencies play a central role in regulating artificial intelligence systems. The Food and Drug Administration regulates medical devices incorporating artificial intelligence, particularly in the context of software classified as Software as a Medical Device. The Securities and Exchange Commission oversees the use of AI in financial markets, particularly in relation to the prevention of fraud and deceptive practices. The Federal Trade Commission, for its part, uses its consumer protection powers to sanction unfair or deceptive practices linked to the use of algorithmic systems (Davtyan, 2025; Yoo & Mueller, 2024).

This sector-specific approach offers the advantage of considerable flexibility, allowing for rapid adaptation to technological developments. It also promotes innovation by avoiding the imposition of a uniform framework that might be ill-suited to the diversity of artificial intelligence applications. However, it leads to significant regulatory fragmentation, characterised by the coexistence of multiple federal and state regulations. This plurality of standards can create legal uncertainty for economic operators, particularly in a context where state legislation is developing in a heterogeneous manner (Davtyan, 2025).

Recent developments in federal policy, exemplified by Executive Order 14179, tend to reinforce this pro-innovation approach, emphasising the reduction of regulatory constraints deemed excessive and the promotion of an environment conducive to the development of artificial intelligence technologies. This dynamic is part of a pragmatic approach to regulation, in which regulatory intervention aims primarily to support innovation rather than systematically constrain it.

Thus, the US model is characterised by functional and evolving regulation, based on an interplay between existing law, the actions of specialised agencies and executive instruments. This approach contrasts with the European model, which is more structured and prescriptive, and highlights a fundamental divergence in the way the legal challenges of artificial intelligence are approached. Whereas the European Union favours ex ante regulation based on risk prevention, the United States adopts a more flexible approach, centred on the gradual adaptation of the law to technological uses and innovations.

6.2. The role of Executive Orders and the direction of public policy

In the absence of a comprehensive federal legislative framework specifically dedicated to artificial intelligence, Executive Orders play a central role in shaping US public policy in this area. These acts, issued by the President of the United States in the exercise of his executive power, enable the coordination of federal agencies' actions and the setting of strategic priorities without going through the legislative process. They thus constitute a preferred instrument of flexible regulation, particularly suited to a constantly evolving technological field.

Executive Order 14110 of 30 October 2023, concerning the safe, secure and trustworthy development and use of artificial intelligence, fully illustrates this normative guidance function. This text imposes a series of obligations on federal agencies aimed at managing the risks associated with artificial intelligence systems, whilst supporting innovation. In particular, it provides for the development of safety standards applicable to advanced AI systems, the development of control mechanisms for general-purpose models, and the strengthening of transparency and accountability requirements for those involved in their design and deployment (The White House, 2023). Through these measures, the Executive Order is part of a risk management approach, based on the prevention of potential breaches of security, fundamental rights and economic interests.

This approach has, however, evolved with the adoption of Executive Order 14179 of 23 January 2025, which reflects a reassessment of federal policy priorities regarding artificial intelligence. This text calls on agencies to review the actions implemented following Executive Order 14110 and to identify those that may constitute obstacles to technological development, with a view to their revision or removal (The White House, 2025). It thus marks a shift towards an approach more focused on promoting innovation and maintaining US technological leadership, without, however, abolishing the entire previous framework.

However, the legal nature of Executive Orders limits their normative scope. Lacking legislative force, these acts do not create general and abstract standards within the meaning of parliamentary law, but primarily organise the actions of the federal administration. Their effectiveness thus depends on their implementation by the relevant agencies, as well as on how they relate to existing laws. Furthermore, the fact that they can be revoked or amended by a subsequent administration introduces a degree of instability into the applicable legal framework, which may affect the predictability of the rules for economic actors.

Consequently, whilst Executive Orders play a decisive role in shaping public policy on artificial intelligence, they cannot replace a genuine federal legislative framework. Their function remains essentially strategic and organisational, reflecting the executive's policy directions rather than a comprehensive and stable legal regime.

6.3. A pro-innovation approach and its legal implications

The US model of artificial intelligence regulation is generally characterised, in legal theory, by an orientation favourable to innovation and economic competitiveness. This characterisation does not stem from the existence of a single piece of legislation expressly enshrining such a policy, but from a convergent interpretation of regulatory instruments and institutional practices. In particular, the absence of a general federal framework applicable to artificial intelligence, combined with the use of existing legal instruments, reflects an approach in which technological development is not governed by uniform ex ante regulation, but is addressed in a progressive and contextual manner (Davtyan, 2025; Yoo & Mueller, 2024).

Within this framework, artificial intelligence systems are not, to date, subject to a specific civil liability regime at the federal level. Disputes likely to arise from their use are thus dealt with through the traditional mechanisms of US law, particularly in relation to tort liability and consumer protection. Federal authorities, in particular the Federal Trade Commission, intervene on the basis of their general powers to sanction deceptive or unfair practices involving algorithmic systems, which illustrates an approach based on the application of existing law rather than on the adoption of new rules specifically dedicated to artificial intelligence (Davtyan, 2025).

This approach is often interpreted as reflecting a tendency to favour ex post regulation, in which legal intervention occurs primarily after unlawful conduct has taken place. Such an approach does not, however, preclude the existence of ex ante mechanisms in certain specific sectors, particularly where sector-specific regulatory authorities, such as the Food and Drug Administration, impose requirements prior to the marketing of products incorporating artificial intelligence technologies. It should therefore be noted that the US model is not based exclusively on an ex post approach, but rather on a combination of mechanisms, the balance of which varies according to the area of application.

Furthermore, the US public authorities use non-legislative instruments to guide the development of artificial intelligence. Executive Order 14110 of 30 October 2023 illustrates this approach by establishing federal priorities aimed at ensuring the safe, secure and trustworthy development and use of artificial intelligence, notably through inter-agency coordination and the development of technical standards and guidelines (The White House, 2023). Executive Order 14179 of 23 January 2025 builds on this initiative whilst introducing a shift, calling on agencies to review existing measures that may constitute barriers to technological development and to propose their revision or removal (The White House, 2025). This development is generally interpreted as reflecting a desire to strengthen the conditions conducive to innovation and to support the United States' position in international technological competition.

In addition to these instruments, the doctrine emphasises the important role accorded to voluntary standards and best practices developed by private actors and standardisation bodies. Whilst these mechanisms do not constitute legally binding obligations in the strict sense, they nevertheless contribute to the structuring of practices and the indirect regulation of artificial intelligence systems. This emphasis on self-regulation is part of a legal tradition that values regulatory flexibility and the adaptability of economic actors.

However, this pro-innovation approach raises certain questions regarding legal protection. Reliance on ex post mechanisms and non-binding standards may, in certain circumstances, limit the law's ability to effectively prevent risks associated with artificial intelligence systems, particularly where such risks are diffuse, evolving or difficult to detect. Furthermore, the development of legislation adopted at the level of the federal states, in the absence of a harmonised federal framework, contributes to a diversification of the applicable rules. This situation, whilst reflecting the flexibility of the US system, may also create increased complexity for economic operators and raise issues of regulatory consistency.

Thus, the American model appears to be an adaptive regulatory system, based on the interplay between existing law, sector-specific intervention by agencies and policy instruments, in which the promotion of innovation is a key component, without, however, ruling out control and oversight mechanisms in certain specific areas.

7. Lessons and avenues for reform in Morocco

7.1. Towards a differentiated liability regime combining strict liability and allocated liability

A comparative analysis of foreign models highlights the structural limitations of Moroccan civil liability law in the face of the specific characteristics of artificial intelligence systems. The traditional paradigm of fault-based liability, as set out in Articles 77 and 78 of the Code of Obligations and Contracts, is based on the identification of wrongful conduct attributable to a legal person and on the establishment of a direct causal link between that conduct and the damage (Code of Obligations and Contracts, 1913, Articles 77 and 78). However, as has been demonstrated, artificial intelligence systems are characterised by their relative autonomy, their technical opacity and the complexity of their value chain, which makes it difficult to apply this traditional framework. In this context, a development of positive law appears necessary in order to ensure effective protection for victims whilst taking technological realities into account.

A coherent reform could be structured around a differentiated liability regime, combining, on the one hand, strict liability applicable to high-risk artificial intelligence systems, and, on the other hand, an allocated liability mechanism enabling the identification of the responsible party within the algorithmic chain. This approach, inspired by developments in comparative law, would make it possible to move beyond the limitations of the unitary liability model and introduce regulation better suited to the diversity of situations.

Firstly, regarding the establishment of a strict liability regime for high-risk systems, such a development is justified by the difficulty, or even impossibility, of proving fault in complex technical environments. In this context, the mere occurrence of damage attributable to the system's operation would be sufficient to engage the operator's liability, irrespective of any fault. This mechanism would find partial support in Moroccan positive law, notably through the regime of liability for defective products provided for in Article 106-1 of the Code of Obligations and Contracts, which establishes liability independent of fault (Code of Obligations and Contracts, 1913, Art. 106-1). However, this regime remains limited to products and does not cover digital services or evolving

artificial intelligence systems. Consequently, extending it to high-risk systems, particularly in the fields of healthcare, transport or high-impact automated decision-making, would ensure effective compensation for victims, whilst taking into account the evidentiary constraints specific to these technologies.

Secondly, the complexity of the artificial intelligence ecosystem requires a rethink of how liability is attributed. The algorithmic value chain involves a multitude of stakeholders—designers, data providers, integrators, operators and users—whose actions are interdependent. In this context, the introduction of an allocated liability mechanism would allow liability to be attributed based on the actual control exercised over the system at the time the damage occurred. Such an approach could be based on the concept of the 'guardian of the algorithmic system', inspired by the regime of liability for things established by Article 88 of the Swiss Code of Obligations and Contracts, according to which liability rests with the person exercising control over the thing that caused the damage (Swiss Code of Obligations and Contracts, 1913, Art. 88). Applied to artificial intelligence systems, this logic would make it possible to designate as liable the party with effective control over the system's operation, whilst preserving the possibility of recourse actions between the various parties in the chain.

Furthermore, the evidential difficulties inherent in the opacity of artificial intelligence systems justify the introduction of mechanisms to ease the burden of proof. Under current law, the victim must establish fault and direct causation in accordance with Articles 77 and 78 of the Swiss Code of Obligations and Contracts, which proves particularly difficult when the system's operation is not readily comprehensible. From this perspective, the introduction of rebuttable presumptions of defect and causation appears to be a relevant development. A presumption of defect could be accepted where the system produces a manifestly abnormal result, whilst a presumption of causality could be upheld where the damage occurs under conditions consistent with a system malfunction. These mechanisms would help to rebalance the burden of proof between the victim and the operator, facilitating access to redress without depriving the defendant of the opportunity to rebut the presumption.

Finally, the effectiveness of these mechanisms requires the introduction of enhanced obligations regarding the traceability and explainability of artificial intelligence systems. Traceability involves the retention of training data, different versions of the model, and operating parameters, in order to enable the reconstruction of the decision-making process. The requirement for explainability, meanwhile, entails the ability to provide an intelligible explanation of the decisions produced by the system. These obligations are an essential prerequisite for identifying liability and for victims to effectively exercise their rights, by helping to partially lift the technical opacity characteristic of algorithmic systems.

7.2. Algorithmic governance: towards the creation of a specialised authority

The legal framework for artificial intelligence cannot be limited to the mere implementation of civil liability mechanisms, however sophisticated they may be. Indeed, the specific nature of algorithmic systems, characterised by their technical complexity, scalability and opacity, calls for the establishment of appropriate institutional governance, capable of intervening before damage occurs and ensuring continuous oversight of their use. From this perspective, the regulation of artificial intelligence requires a combination of ex post liability instruments and ex ante supervisory mechanisms, underpinned by enhanced technical expertise.

The current Moroccan institutional framework has certain limitations in this regard. Whilst administrative authorities are already active in related fields—such as the National Commission for the Control of Personal Data Protection, which has jurisdiction over personal data protection, or the Directorate-General for Information Systems Security, responsible for cybersecurity issues—their respective mandates do not comprehensively cover the specific challenges associated with artificial intelligence systems. These institutions possess significant legal and technical expertise, but their scope of action remains sector-specific, which does not allow for a comprehensive understanding of the risks associated with the use of algorithmic systems.

In this context, the creation of a national authority specialising in artificial intelligence appears to be a relevant development of the institutional framework. Such an authority would be designed to operate alongside existing structures, ensuring the coordination of public policies and developing expertise dedicated to algorithmic systems. It would thus help to overcome the current fragmentation of responsibilities by centralising risk analysis and ensuring consistency in the regulation of artificial intelligence applications.

The remit of such an authority should be based on a framework of technical and preventive regulation. In particular, it could be tasked with auditing algorithmic systems to verify their compliance with applicable legal and technical requirements, as well as assessing biases that may affect their results. It would also play a role in certifying high-risk artificial intelligence systems, ensuring compliance with

standards of security, reliability and transparency. Furthermore, the supervision of sensitive uses of artificial intelligence, particularly in areas such as healthcare, security or high-impact automated decisions, would also fall within its remit.

The establishment of such an authority would help to address the current lack of technical expertise within existing regulatory mechanisms. Indeed, traditional legal institutions do not always possess the necessary expertise to understand the technical specifics of artificial intelligence systems, which limits their ability to exercise effective oversight. A specialised authority would thus provide a suitable institutional framework, based on a combination of legal and technical expertise, which is essential for the effective regulation of algorithmic systems.

Thus, the establishment of structured algorithmic governance, based on the creation of a dedicated authority, would constitute an essential complement to civil liability mechanisms, ensuring comprehensive, coherent and forward-looking regulation of artificial intelligence under Moroccan law.

7.3. Practical examples of the shortcomings of the current framework

The theoretical analysis of the limitations of Moroccan positive law is particularly well illustrated by the study of concrete situations involving artificial intelligence systems. These scenarios reveal, in practical terms, the shortcomings of the current legal framework, both in terms of the attribution of liability and in terms of evidence and compensation.

The scenario of an accident involving an automated driving system highlights the difficulties in applying civil liability law. In such a situation, the damage results from a complex interaction between the algorithmic system and the user's behaviour, which makes it particularly difficult to identify the party liable. Moroccan positive law, based on Articles 77 and 78 of the Code of Obligations and Contracts, requires the establishment of fault attributable to a specific party, which appears difficult when the decision causing the damage is generated by an autonomous system. Recourse to the regime of liability for defective products, provided for in Article 106-1 of the same Code, could be considered, insofar as it establishes liability independent of fault (Code of Obligations and Contracts, 1913, Art. 106-1). However, its application remains uncertain in the case of evolving systems, particularly as the producer may exonorate themselves by invoking the state of scientific knowledge at the time the product was placed on the market, in accordance with Article 106-9 (Code of Obligations and Contracts, 1913, Art. 106-9). This situation illustrates the limitations of existing law, which struggles to address systems whose behaviour evolves after they have been placed on the market.

The scenario of algorithmic discrimination in a recruitment process highlights the difficulties associated with proving and legally classifying the harm. Where an artificial intelligence system produces biased results due to discriminatory training data, Moroccan law provides certain legal foundations, notably through the principle of equality enshrined in Article 19 of the Constitution and the rules on the protection of personal data set out in Law No. 09-08. However, these instruments appear insufficient to address the specific characteristics of algorithmic systems. In particular, the opacity of how these systems operate makes it difficult to establish fault or a direct causal link, as required by Articles 77 and 78 of the Code of Obligations and Contracts. This evidential difficulty undermines the effectiveness of the right to compensation and highlights the need to introduce appropriate mechanisms, such as presumptions of causality or obligations to provide access to relevant data.

Finally, the scenario of a breach of information system security, resulting in a massive leak of personal data, reveals a disconnect between criminal prosecution and civil redress. Moroccan law does indeed provide for a set of punitive provisions, notably Articles 607-3 et seq. of the Criminal Code relating to breaches of automated data processing systems, as well as security obligations arising from Law No. 05-20 on cybersecurity. These mechanisms make it possible to punish unlawful conduct and impose requirements for the protection of systems. However, compensation for the damages suffered by victims remains uncertain in the absence of an appropriate liability regime. In particular, the requirement of fault and a direct causal link constitutes a major obstacle to effective compensation, especially when the origin of the breach results from a complex interplay of technical factors.

These various scenarios thus highlight a consistent theme: Moroccan positive law, whilst offering partial legal tools, remains structurally ill-suited to the specificities of artificial intelligence systems. They confirm the need for the legal framework to evolve towards more suitable mechanisms, capable of ensuring both the identification of those responsible, the easing of the burden of proof, and effective compensation for victims.

7.4. Towards the adoption of a specific legislative framework inspired by a 'Moroccan AI Act': definition, risk classification, and criminal and creative regulation

One of the major shortcomings of Moroccan law regarding artificial intelligence lies in the absence of a unified regulatory framework specifically dedicated to these technologies. This gap is not merely a technical shortcoming, but reveals a structural inadequacy of positive law in the face of new phenomena characterised by the relative autonomy of systems, their opacity, and their capacity to produce results with legal consequences. At present, artificial intelligence systems are addressed through sector-specific legislation, notably Law No. 09-08 on the protection of personal data, Law No. 05-20 on cybersecurity, as well as the general provisions of the Civil Code and the Criminal Code. However, this fragmented approach does not ensure consistent regulation that is adapted to the complexity of artificial intelligence applications. In this context, the adoption of a specific legislative framework, inspired by the European model without constituting a mechanical transposition of it, appears to be a necessary step.

Firstly, the introduction of a legal definition of an artificial intelligence system is an essential prerequisite for any effective regulation. Moroccan law currently contains no definition of this concept, which creates uncertainty regarding the scope of application of existing rules. A legal definition could usefully cover software systems operating with a certain degree of autonomy, capable of processing data and producing results such as decisions, predictions or content, which are likely to have an impact on legal situations. Such an approach would make it possible to define the scope of the technologies concerned and ensure legal certainty for operators, by avoiding the uncertainties associated with an implicit or analogous classification.

Secondly, the introduction of a classification of artificial intelligence systems based on risk level appears to be a key instrument for proportionate regulation. Current Moroccan law applies general rules indiscriminately to systems presenting highly variable levels of risk, which limits its effectiveness. A graduated approach, inspired by developments in comparative law, would make it possible to distinguish between systems presenting an unacceptable risk, which could be subject to a ban, high-risk systems subject to enhanced requirements, and systems with limited or low risk subject to lighter obligations. Such a regulatory framework would make it possible to tailor legal obligations to the severity of the risks, balancing the protection of individuals with the development of innovation.

Furthermore, the integration of criminal law into a framework specific to artificial intelligence appears necessary in order to address the unlawful uses specific to these technologies. Moroccan criminal law already contains provisions relating to offences against automated data processing systems, introduced by Law No. 07-03 and codified in Articles 607-3 to 607-10 of the Criminal Code. These provisions criminalise, in particular, fraudulent access to a system, interference with its operation, and the fraudulent alteration or deletion of data (Penal Code, Articles 607-3 to 607-10). Whilst these rules may apply to artificial intelligence systems as components of information systems, they do not take into account certain specific features of these technologies, such as the use of generative systems for the purposes of information manipulation or the automated production of unlawful content. Consequently, an adaptation of existing criminal offences, as well as the possible introduction of specific offences, could be considered in order to address these new risks, whilst respecting the fundamental principles of criminal law, in particular the principle of legality.

Artificial intelligence also raises unprecedented issues regarding content creation. Moroccan intellectual property law, as set out in Law No. 2-00 on copyright and related rights, is based on an anthropocentric conception of creation, implying the existence of a natural person as the author. Article 10 of this law confers exclusive rights on the author over their work, which presupposes creative human intervention (Law No. 2-00, Art. 10). Under these circumstances, content generated autonomously by artificial intelligence systems cannot, in principle, benefit from copyright protection in the absence of an identifiable human contribution. This situation creates legal uncertainty regarding the status of the generated works and, at the same time, raises the question of the use of protected works in the context of model training. Furthermore, certain generated content may fall under criminal law where it infringes protected rights, particularly in cases involving the dissemination of unlawful content or the manipulation of information. It therefore appears necessary to clarify the legal regime applicable to such creations, in order to reconcile the protection of authors' rights with technological development.

Finally, the introduction of a specific legislative framework dedicated to artificial intelligence should not replace existing legislation, but should be coordinated with it. The rules on the protection of personal data, derived from Law No. 09-08, would continue to apply to data processing, whilst Law No. 05-20 would retain its role in the field of cybersecurity. The Civil Code would remain applicable in matters of civil liability, in particular through Articles 77 et seq., and the Criminal Code would continue to govern offences against

information systems. The new legislative framework would thus be intended to serve as a special set of rules, supplementing and coordinating existing provisions to ensure the overall coherence of the legal system.

Thus, the adoption of a legislative framework specific to artificial intelligence, structured around a legal definition, a classification of risks, an adaptation of criminal law and a regulatory framework for generated creations, appears to be a necessary development in Moroccan law. Such a reform would make it possible to move beyond the limitations of the current framework and establish a legal system capable of addressing the contemporary challenges of artificial intelligence, whilst ensuring a balance between technological innovation, legal certainty and the protection of fundamental rights.

Conclusion

The study highlights that the legal framework for artificial intelligence under Moroccan law currently relies on a combination of sector-specific regulations covering personal data protection, cybersecurity, civil liability and criminal offences, the interplay of which remains incomplete in light of the specific characteristics of algorithmic systems. Whilst these instruments enable certain aspects of the phenomenon to be addressed, they are insufficient to grasp its complexity, particularly due to the relative autonomy of the systems, the opacity of their decision-making processes and the multitude of actors involved in their lifecycle. The traditional paradigm of liability, based on fault, direct causation and the burden of proof resting on the victim, thus appears structurally weakened in a technological environment characterised by uncertainty and difficulty in accessing information.

A comparative analysis with the European and American models confirms this inadequacy. On the one hand, the European approach, based on ex ante regulation structured around risk classification, offers a coherent regulatory framework enabling the anticipation of potential infringements and the allocation of obligations throughout the value chain. On the other hand, the American model, which is more flexible and innovation-oriented, highlights the advantages of adaptive regulation, but also the limitations of a primarily ex post approach in terms of protecting individuals. These two frameworks, although distinct, converge on a common conclusion: traditional legal mechanisms must be rethought to meet the challenges posed by artificial intelligence.

In this context, the evolution of Moroccan law cannot be limited to ad hoc adjustments to existing rules, but calls for a more profound reconfiguration of its foundations. A renewed approach to liability appears necessary, combining, for high-risk systems, a no-fault liability regime guaranteeing effective compensation for victims, with an allocated liability mechanism based on the effective control exercised over the system. This transformation must be accompanied by an adjustment of the rules of evidence, in particular through the introduction of presumptions of causality and defectiveness, thereby rebalancing the burden of proof in a context characterised by information asymmetry.

At the same time, the establishment of structured algorithmic governance is a key driver of effectiveness. The creation of a specialised authority, equipped with technical and legal expertise, would enable ex ante oversight of artificial intelligence systems, complementing civil liability mechanisms. Such an institution would help to strengthen the coherence of the regulatory framework and address the current lack of technical expertise.

Finally, the adoption of a specific legislative framework dedicated to artificial intelligence appears to be the logical culmination of this development. Drawing inspiration from experiences abroad without mechanically replicating their models, this framework should incorporate a legal definition of artificial intelligence systems, a classification of risks, an adaptation of criminal offences to algorithmic practices, and a clarification of the regime applicable to generated creations. The aim would thus be to establish a special standard capable of coordinating existing legislation whilst addressing the specific challenges posed by these technologies.

Beyond its technical implications, this development raises a more fundamental question: that of the law's capacity to grasp systems whose functioning partly defies traditional models of legal rationality. Artificial intelligence thus calls for a rethinking of the classical categories of law, not in a spirit of rupture, but within a dynamic of gradual adaptation, aimed at reconciling technological innovation, legal certainty and the effective protection of fundamental rights.

References

- Constitution of the Kingdom of Morocco. (2011). Official Gazette of the Kingdom of Morocco, 5964-bis.

- Dahir of 12 August 1913 establishing the Code of Obligations and Contracts. (1913). Official Gazette of the Cherifian Empire.

- Dahir No. 1-00-20 of 9 Kaada 1420 (15 February 2000) promulgating Law No. 2-00 on copyright and

related rights. (2000). Official Gazette of the Kingdom of Morocco, 4810.

- Dahir No. 1-09-15 of 22 Safar 1430 (18 February 2009) promulgating Law No. 09-08 on the protection of personal data. (2009). Official Gazette of the Kingdom of Morocco, 5714.

- Decree No. 2-09-165 of 21 May 2009 issued for the implementation of Law No. 09-08 on the protection of personal data. (2009). Official Gazette of the Kingdom of Morocco, 5744.

- Dahir No. 1-11-03 of 14 Rabii I 1432 (18 February 2011) promulgating Law No. 31-08 enacting consumer protection measures. (2011). Official Gazette of the Kingdom of Morocco, 5932.

- Dahir No. 1-20-69 of 4 Hija 1441 (25 July 2020) promulgating Law No. 05-20 on cybersecurity. (2020). Official Gazette of the Kingdom of Morocco, 6906.

- Law No. 07-03 of 28 Ramadan 1424 (11 November 2003) amending and supplementing the Criminal Code. (2003). Official Gazette of the Kingdom of Morocco, 5184.

- Penal Code. (2003). Articles 607-3 to 607-10 relating to offences against automated data processing systems.

- Berne Convention for the Protection of Literary and Artistic Works. (1886). Revised on several occasions.

- Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). (1994). Marrakesh.

- Council of Europe. (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108).

- Council of Europe. (2018). Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+).

- European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act). Official Journal of the European Union, L 168. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

- European Commission. (2022). Proposal for a Directive on the adaptation of the rules on non-contractual liability to artificial intelligence (COM(2022) 495 final). https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=COM%3A2022%3A495%3AFIN

- Davtyan, T. (2025). The U.S. approach to AI regulation: Federal laws, policies, and strategies explained. Journal of Law, Technology & the Internet, 16(2), 223–254. https://scholarlycommons.law.case.edu/jolti/vol16/iss2/2/

- De Bruyne, J., Dheu, O., & Ducuing, C. (2023). The European Commission's approach to extra-contractual liability and AI: An evaluation of the AI liability directive and the revised product liability directive. Computer Law & Security Review, 51, 105892. https://doi.org/10.1016/j.clsr.2023.105892

- Dotan, R. (2024). US regulation of artificial intelligence. In C. Lütge et al. (Eds.), The Elgar companion to applied AI ethics (pp. 234–256). Edward Elgar Publishing. https://doi.org/10.4337/9781803928241.00022

- Li, S., & Schütte, B. (2024). The proposed EU artificial intelligence liability directive: Does its content reflect its ambition? Technology and Regulation, 2024, 143–151. https://doi.org/10.26116/techreg.2024.014

- Lunca, D. (2025). Towards a coherent EU civil liability regime for AI-caused harm. European Journal of Law and Public Administration, 12(1), 23–50. https://doi.org/10.18662/eljpa/12.1/253

- Madiega, T. (2023). Artificial intelligence liability directive (PE 739.342). European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739342/EPRS_BRI(2023)739342_EN.pdf

- The White House. (2023). Executive Order 14110: Safe, secure, and trustworthy development and use of artificial intelligence. Federal Register, 88(210), 75191–75226.

https://www.federalregister.gov/documents/2023/11/01/2023-24283

- The White House. (2025). Executive Order 14179: Removing barriers to American leadership in artificial intelligence. Federal Register, 90. https://www.federalregister.gov/documents/2025/01/31/2025-02772

- Yoo, C. S., & Mueller, A. (2024). U.S. artificial intelligence regulation during the Biden administration. Journal of Law & Economic Regulation, 17(2), 7–29. https://doi.org/10.22732/CeLPU.2024.17.2.7