Revue du Contrôle de la Comptabilité et de l'Audit
ISSN : 2550-469X
Volume 9 : numéro 3

Entre Innovation et Régulation : Les Défis Juridiques de l'Intelligence Artificielle

Between Innovation and Regulation : The Legal Challenges of Artificial Intelligence

Hicham EL YOUSFI

Enseignant Chercheur, FSJES, SOUISSI

Laboratoire de Recherche en Management des Organisations,
Droit des Affaires et Développement Durable
Université Mohammed V

Sanaa BENABDALLAOUI

Doctorante, FSJES, SOUISSI
Laboratoire de Recherche en Management des Organisations,
Droit des Affaires et Développement Durable
Université Mohammed V

Date de soumission : 12/07/2025

Date d'acceptation : 03/09/2025

Pour citer cet article :

EL YOUSFI H.. & **BENABDALLAOUI S.** (2025) «**Entre Innovation et Régulation : Les Défis Juridiques de l'Intelligence Artificielle** », Revue du contrôle, de la comptabilité et de l'audit « Volume 9 : numéro 3» pp : 209-227.

Résumé

L'intelligence artificielle (IA) transforme radicalement les systèmes économiques et la vie quotidienne, apportant à la fois des opportunités de progrès technologique et des défis en termes de sécurité, d'éthique et de gouvernance. Face à ces mutations, gouvernements et organisations internationales déploient des cadres réglementaires pour encadrer le développement et l'utilisation de l'IA. L'étude propose une analyse comparative des principales législations à l'échelle nationale et internationale, en mettant en lumière leurs similitudes et leurs divergences à travers l'étude de cas du règlement européen (AI Act), de la réglementation américaine, du projet canadien (LIAD) ainsi que de l'approche prônée par les Nations Unies. Nous explorerons comment chaque modèle répond aux enjeux technologiques et sociétaux. Notre objectif, à travers une revue de littérature élargie, est de faire avancer la connaissance sur un sujet en pleine évolution. Nous avons fait le choix d'une approche multidisciplinaire à même d'appréhender la complexité de la thématique étudiée. Les conclusions proposent de nouvelles pistes à explorer pour un sujet qui fera couler beaucoup d'encre.

Mots Clés : Intelligence artificielle ; Régulation ; Souveraineté ; Gouvernance ; Ethique.

Abstract

Artificial intelligence (AI) is radically transforming economic systems and daily life, bringing both opportunities for technological progress and challenges in terms of security, ethics, and governance. Faced with these changes, governments and international organizations are deploying regulatory frameworks to govern the development and use of AI. This paper offers a comparative analysis of the main national and international AI legislation, highlighting their similarities and differences. Through the case study of the European regulation (AI Act), the American regulation, the Canadian project (LIAD), and the approach advocated by the United Nations, we will explore how each model addresses current technological and societal challenges. Our goal, through a broad literature review, is to advance knowledge on a rapidly evolving subject. We have chosen a multidisciplinary approach capable of grasping the complexity of the topic studied. The conclusions propose new avenues to explore for a subject that will generate a lot of ink.

Keywords : Artificial Intelligence ; Regulation ; Sovereignty ; Governance ; Ethics.

Introduction

De nos jour, l'intelligence artificielle (IA) est présente dans le e-commerce, dans les systèmes managériaux, dans les finances, les assurances, la santé, dans les systèmes judiciaires, etc. C'est, également, un atout d'amélioration de la compétitivité qui répond aux besoins des professions et des compétences de manière anticipative. Mais qu'est-ce que l'IA ?

De prime abord, on peut avancer qu'il s'agit d'un système autonome capable de prendre une décision sans une intervention humaine directe. La norme ISO 2382-2015 (1) relative aux technologies de l'information définit l'IA comme "une branche de l'informatique consacrée à l'élaboration de systèmes de traitement de données qui effectuent des fonctions normalement associées à l'intelligence humaine, telles que le raisonnement et l'apprentissage".

En avril 2021, la Commission Européenne a pour la première fois mis en place une législation sur l'IA et introduisit une classification des systèmes en fonction de leur risque. Pour la commission, l'intelligence artificielle représente tout outil utilisé par une machine afin de "reproduire des comportements liés aux humains, tels que le raisonnement, la planification et la créativité". L'OCDE définit l'IA comme un système automatisé qui, pour un ensemble donné d'objectifs, définis par l'homme, est en mesure d'établir des prévisions, de formuler des recommandations, ou de prendre des décisions influant sur des environnements réels ou virtuels. Il utilise des données et des entrées générées par la machine et/ou apportées par l'homme pour :

i. Percevoir des environnements réels et/ou virtuels ;

ii. Produire une représentation abstraite de ces perceptions sous forme de modèles issus d'une analyse automatisée ou manuelle ;

iii. Utiliser les résultats inférés du modèle pour formuler différentes options de résultats ;

iv. Il existe principalement deux catégories d'IA : une IA faible et une IA forte. La première, plus courante, est conçue pour des tâches spécifiques et limitées, tandis que la seconde vise à reproduire l'intelligence humaine dans sa globalité. En plus de ces catégories, on peut distinguer les IA :

(1) L'ISO 2382-15 est une norme internationale de traitement de l'information émanant d'autres organisations (telles que l'Union internationale des télécommunications et la Commission électrotechnique internationale) ainsi que les normes nationales publiées ou au stade de projets, Son but est de procurer des définitions rigoureuses,

simples et compréhensibles pour tous les intéressés. Chaque notion est choisie de façon que sa définition puisse avoir la valeur la plus générale.

- Par leur niveau d'intelligence : l'IA étroite regroupe les systèmes conçus pour une tâche spécifique, comme la reconnaissance vocale, la traduction de langues, ou la conduite d'une voiture. L'IA générale, elle, aurait un niveau d'intelligence capable de comprendre, d'apprendre et d'appliquer ses connaissances à une variété de tâches. Quant à l'IA super-intelligence ou artificielle, elle serait théoriquement plus intelligente que l'humain et dans tous les domaines, y compris pour la créativité, le raisonnement et la résolution de problèmes.

Selon la fonction, certaines IA fonctionnent sans mémoire alors que d'autres peuvent utiliser des données du passé pour prendre des décisions, mais leur mémoire reste limitée (voitures autonomes). D'autres formes d'IA dites de l'esprit, encore théoriques, seraient capables de comprendre les émotions, les croyances et les intentions des autres êtres, qu'ils soient humains ou non.

- Par type d'apprentissage, certaines IA apprennent à partir de réponses justes, d'autres explorent des données par essais et erreurs, en recevant des récompenses pour les actions positives et des pénalités pour les actions négatives. En résumé, si l'IA étroite est courante aujourd'hui, l'IA générale et la super-intelligente restent des domaines de recherche de l'Avenir.

Souvent utilisée comme un outil de facilitation des tâches, l'IA pose, par ailleurs, des questions complexes en termes de sécurité et de protection des droits fondamentaux, de responsabilité civile, pénale et contractuelle, en termes d'équité, de transparence et d'éthique. Lorsqu'elle cause des dommages, qui est responsable du préjudice ? Le développeur de l'IA, le fabricant, l'utilisateur ou l'opérateur ?

Le cadre juridique actuel ne peut répondre à ces questions et l'on assiste à l'éclosion d'un droit qui devient un champ de recherche autonome au croisement des sciences politiques, de l'économie, de l'innovation et de la gouvernance, etc. De nos jours, on parle de plus en plus d'un véritable paradigme autour du droit et de la technologie (Law and TechReg) qui structure la manière dont le droit appréhende l'innovation numérique, en particulier l'IA. Ce paradigme organise l'équilibre entre deux pôles : l'innovation et la régulation. Le premier cherchant à promouvoir la créativité, la compétitivité et l'expérimentation, le second se préoccupe des risques aux droits fondamentaux et de la responsabilité contractuelle et délictuelle.

Sans hésitation, l'IA illustre au mieux ce cadre et oblige le droit à combiner des techniques réglementaires horizontales (protection des données, responsabilité, concurrence, propriété

intellectuelle, droits fondamentaux) et verticales (régimes spécifiques comme l'AI Act européen), tout en intégrant des outils techniques (audits algorithmiques, évaluation de risques, gouvernance des données).

Cette contribution met l'accent sur l'interprétation des règles, sur l'adaptation dynamique du droit aux mutations technologiques, sur l'intégration de facteurs extra-juridiques (sociaux, économiques, éthiques) et sur le recours au droit comparé pour dégager les convergences et les évolutions selon un socle positiviste qui part néanmoins des cadres positifs existants (RGPD, responsabilité, brevets) pour expliciter le comportement du cadre normatif considéré comme figé face à une évolution sans précèdent du développement technologique.

A cet égard, on peut d'une part rappeler des principes juridiques comme : la primauté de l'Etat de droit (clarté des normes, hiérarchie des sources, contrôlabilité par le juge), la protection des droits fondamentaux (respect de la vie privée, non-discrimination, liberté d'expression, droit au recours), et d'autre part constater l'éclosion de nouvelles catégories du droit comme la responsabilité algorithmique, les mécanismes de reddition de comptes, le calibrage des moyens technologiques au regard des finalités légitimes, le droit d'accès à l'information, l'intégration en amont des exigences éthiques et de protection des données dans le cycle de vie des systèmes, la gouvernance des données, la prise en compte des impacts environnementaux et la veille normative.

Aujourd'hui, le défi est de maintenir un continuum entre une innovation responsable et une régulation efficace, via une combinaison de droit dur, de soft Law et de normes techniques soutenues par une gouvernance organisationnelle solide.

Dès lors, cette étude a pour objectif :

- De répertorier la littérature académique sur le sujet ;

- De comparer les architectures réglementaires non seulement de l'Union Européenne (UE), des Etats-Unis (EU), de la Chine et d'autres juridictions influentes (Canada, Royaume-Uni, OCDE/UNESCO) mais aussi du Maroc ;

- D'éclairer sur les défis éthiques, juridiques et politiques liés à la régulation de l'IA, ainsi que sur ses répercussions actuelles et futures ;

- De dégager les tendances, tensions et lacunes susceptibles d'orienter les recherches futures.

Au cours de cette recherche, nous essayerons d'analyser, d'interpréter et de systématiser les cadres juridiques qui soulèvent des questions nouvelles sur les règles existantes (RGPD, lois

sur la responsabilité, brevets, etc.). La recherche doctrinale autour de nouveaux sujets nous permettra de comprendre comment le droit actuel évoluera. Le recours au droit comparé (Union européenne, États-Unis, Chine…) nous aidera à identifier les points communs, les divergences, et les meilleures pratiques. Par ailleurs, l'IA n'est pas qu'une affaire de textes de loi. Il faut comprendre l'impact social, économique et éthique de la technologie pour proposer des réformes ou de nouveaux modèles juridiques adaptés aux défis de l'IA.

Pour ce faire, la bibliographie a été sélectionné selon des critères de rigueur scientifique avec une attention particulière aux travaux récents, aussi récents que le sujet lui-même. Nous exposerons d'abord les principales approches normatives en explicitant les notions juridiques autour desquelles s'articule le droit de l'IA, par la suite, nous procéderons à une analyse comparative de ses cadres réglementaires pour, enfin, traiter d'une éventuelle régulation de l'IA dans le contexte marocain.

1. Contributions de la Recherche sur l'IA

Sur le plan académique, des auteurs plaident en faveur d'une transparence des algorithmes, présentés comme des boîtes noires, et insistent sur le droit des individus à comprendre les décisions prises par les systèmes d'IA. Dans ce cadre, Pasquale (2015) examine les algorithmes secrets qui gouvernent l'argent et l'information. Il démontre que ces systèmes cachés influencent des aspects cruciaux de nos vies, des réputations aux décisions économiques. Ils collectent et analysent silencieusement nos données personnelles, données issues de nos habitudes de travail et de notre utilisation d'Internet. Ces processus opaques peuvent entraîner des conséquences importantes et souvent imprévisibles sur notre société. D'autres auteurs remettent en question les cadres traditionnels de la protection des données, notamment le RGPD (Règlement général sur la protection des données), et interrogent le rôle que peuvent jouer les principes éthiques dans la gouvernance de l'IA. En ce sens, Edwards (2021) estime que la collecte et le traitement à grande échelle complexifient la notion de consentement et de contrôle individuel. Elle montre que de nombreux principes éthiques émergent (justice, transparence, responsabilité), mais qu'ils restent souvent non contraignants. En effet, les systèmes d'IA manipulent souvent d'énormes volumes d'informations dont la transparence, sur leurs usages réels, reste indéfini. Elle conclut que le droit de la protection des données, s'il constitue un socle essentiel, doit évoluer pour faire face aux défis inédits posés par l'IA, et que les principes éthiques doivent être traduits en normes juridiques effectives pour protéger les individus.

De son côté, Hildebrandt (2015), avocate et philosophe néerlandaise travaille à l'intersection du droit et de l'informatique. Elle met en lumière la prédiction et la préemption de nos activités quotidiennes, de nos préférences, de nos risques de santé et de crédit, de nos intentions criminelles et de notre capacité d'achat. Elle affirme que nous sommes en transition et souligne comment l'utilisation généralisée des technologies d'apprentissage automatique menace la vie privée, l'identité, l'autonomie, la non-discrimination, l'application régulière de la loi et la présomption d'innocence. L'auteure explique comment les technologies intelligentes reconfigurent les objectifs du droit dans une démocratie constitutionnelle, compromettant le droit en tant qu'instrument de justice, de sécurité juridique et de bien public. Elle appelle les juristes, les informaticiens et la société civile à dompter les technologies intelligentes, à réinventer la protection efficace de l'Etat de droit.

Dans le même ordre d'idées, le LexTech Institute rattaché à l'Université de Neuchâtel, se concentre sur l'étude interdisciplinaire du droit et de la technologie, aborde la question de la "personnalité juridique des algorithmes" et des implications juridiques des décisions automatisées. Les recherches mettent en lumière les défis posés par l'attribution d'une personnalité juridique aux algorithmes et ses conséquences potentielles. Comment alors apporter la preuve juridique en cas de litige ?

En effet, l'un des problèmes majeurs est d'imputer la responsabilité civile ou pénale (Barocas, Hardt & Narayanan, 2023) lorsqu'un système autonome cause un dommage (accidents avec véhicules autonomes, diagnostic médical erroné, cible militaire) traduisant l'incapacité des régimes traditionnels devant l'opacité et l'autonomie des IA (Tjing, H. H. C., 2023). Reconnaître une personnalité juridique aux algorithmes créerait une nouvelle catégorie d'entités responsables, ce qui bouleverserait plusieurs domaines du Droit. Comment sanctionner une entité immatérielle ? Au niveau contractuel, cela poserait des questions sur la capacité à conclure des contrats (comment un algorithme pourrait-il consentir ?), ainsi que sur les obligations de confidentialité (peut-on protéger les secrets d'un algorithme ?).

D'autres sujets à l'intersection de la gouvernance technique des algorithmes et des défis constitutionnels liés à l'IA touchent au cœur des principes fondamentaux qui structurent la Démocratie : vie privée, liberté d'expression ou non-discrimination, reconnaissance faciale, interprétation des décisions algorithmiques par les juges, le rôle du législateur, l'influence de l'IA sur les élections et le débat public (Bietti, 2022).

Il est indéniable que l'IA pose des défis majeurs à la protection des créations et à la titularité des droits d'auteur et de brevets. En général, les algorithmes ne sont pas protégés par le droit d'auteur ni les œuvres générées par l'IA (Gervais, D.J, 2022). Soulignons que pour être brevetable, une invention doit avoir un caractère technique et une application industrielle concrète que les algorithmes, en tant que tels, ne possèdent pas. Ils sont, par essence, une méthode mathématique, une séquence abstraite pour résoudre un problème. Il est important de noter que ce n'est pas l'algorithme *en soi* qui peut être breveté, mais plutôt son application à un domaine technique spécifique. Si le brevet protège une invention, le droit d'auteur protège l'expression originale d'une œuvre de l'esprit. L'exploitation licite de l'IA requiert, par conséquent, que l'algorithme et sa base de données aient été dûment acquis. A titre d'exemple, aux Etats-Unis, il a été refusé d'attribuer des brevets à l'IA. Le droit peine à suivre le rythme de l'innovation, ce qui crée de l'insécurité juridique (Hildebrandt, 2020).

D'autres juristes appellent à revenir aux fondements philosophiques et éthiques pour réguler l'IA (reconnaissance faciale, racisme, sexisme, etc.). Ces recherches portent sur les implications sociales, politiques et éthiques des systèmes d'IA et sur les questions de biais raciaux et de genre dans les algorithmes (Noble, Dignum, Bryson).

2. Cadres Réglementaire et Justifications de la Régulation

De nos jours, il apparaît indispensable de définir des règles claires pour protéger la vie privée, la sécurité et les droits humains sans mettre de freins à l'innovation et à la compétitivité. Il faut savoir que les systèmes d'IA apprennent à partir de données existantes qui risquent de contenir des biais lors de la collecte des données, de la conception de l'algorithme ou de l'interprétation des résultats, et par conséquent perpétuer des discriminations, des inégalités, des stéréotypes, des impacts négatifs sur le marché de l'emploi, etc. L'opacité des algorithmes complique alors l'identification des responsables en cas de décisions biaisées ou discriminatoires. C'est pourquoi, la régulation cherche à garantir que l'IA soit utilisée de manière transparente, sécurisée et éthique, dans le respect des droits fondamentaux et des valeurs démocratiques.

Si l'IA joue un rôle de plus en plus un rôle influent dans tous les domaines, on peut noter, d'ores et déjà que la législation régissant le numérique a toujours porté sur la Protection des droits humains, le Règlement Général sur la Protection des Données a depuis sa mise en application, profondément transformé la manière dont les entreprises gèrent les données personnelles. Trois principes fondamentaux le sous-tendent : la transparence, la limitation de la finalité et la minimisation des données. Aussi, deux types de mesures doivent être adoptés. D'un côté, le

déploiement de technologies doit permettre d'arbitrer l'accès aux systèmes informatiques d'une entreprise, de l'autre prendre des mesures organisationnelles de contrôle concernant les personnes amenées à manipuler les données des organisations, sont à observer. A titre d'exemple, à l'aide des cookies, scoring, fishing, etc., le comportement des consommateurs chez Google, Amazone ou sur les réseaux sociaux peut être influencé dans un sens donné. Dans la reconnaissance faciale, A.Tussy (CEO de FaceTec) explique : "Bien que l'attaque paraisse complexe, elle n'est, en réalité, pas si difficile dès lors que les logiciels de deepfakes sont facilement accessibles et souvent gratuits".

L'une des caractéristiques communes aux modèles européens, américains et canadiens est l'utilisation d'une approche fondée sur le risque. La réglementation européenne adopte une classification fine des risques d'IA en fonction de leur impact potentiel. Les Etats-Unis sont pour une approche basée sur des directives volontaires et une régulation par étapes, en s'appuyant sur les initiatives émanant des Etats. Le Canada vise une approche plus souple avec une définition plus précise des technologies jugées autonomes ou partiellement autonomes. L'ONU plutôt que d'imposer des normes strictes, encourage la mise en place d'un cadre de coopération internationale qui reconnaisse la dimension globale et transfrontalière des risques associés à l'IA.

2.1 Dans l'UE, le AI Act représente la première législation globale et complète sur l'IA. Entré en vigueur le 1er août 2024, ce cadre réglementaire est basé sur une approche fondée sur le risque et classe les systèmes d'IA en 04 catégories selon leur niveau de risque : inacceptable, élevé, risque de transparence et risque minimal ou nul. Parmi les mesures phares, le règlement interdit certaines pratiques préjudiciables telles que l'utilisation de techniques manipulatrices et impose des obligations strictes aux systèmes à haut risque, notamment en termes de gestion de données, de robustesse, de cyber sécurité et d'obligation de transparence. La législation, par ailleurs, interdit les traitements disproportionnés fondés sur les risques de préjudice physique ou psychologique, de dommages sur les biens ou sur les pertes économiques aux personnes ou aux groupes.

L'AI Act se distingue par sa portée extraterritoriale et ses sanctions pouvant atteindre 7% du chiffre d'affaires annuel à environ 35 millions d'euros à l'encontre des contrevenants. Il vise à imposer des critères. La législation s'applique aux fournisseurs et/ou prestataires, établis dans ou hors UE, aux utilisateurs d'IA situés dans ou hors UE, à la condition que les résultats générés soient utilisés dans l'UE. Cependant, la réglementation ne s'applique pas aux systèmes

militaires, aux autorités publiques, et aux organisations internationales soumises à la coopération judiciaire.

2.2. Les Etats-Unis adoptent une approche fragmentée sans cadre fédéral unifié pour la régulation de l'IA. Il s'agit d'une approche décentralisée avec des lois variées selon les Etats et selon les secteurs. Cette mosaïque réglementaire reflète une volonté de soutenir l'innovation tout en évitant une régulation contraignante qui soulève des enjeux majeurs en termes de cohérence et d'harmonisation. Le paysage combine des initiatives au niveau fédéral, étatique et même municipal que le décret Trump rend plus permissif. Parallèlement à des actions menées par la Federal Trade Commission (FTC) pour lutter contre les biais et la discrimination liés à l'IA, comme en témoigne l'affaire concernant l'utilisation de la reconnaissance faciale par Rite Aid, des initiatives fédérales telles que la Federal Artificial Intelligence Risk Management Act de 2023 visent à standardiser les pratiques de gestion des risques par l'intermédiaire du cadre développé par le National Institute of Standards and Technology (NIST). En 2023, 190 projets de loi ont été déposés au niveau des Etats, dont 14 sont devenus des lois. De plus, plusieurs Etats, à l'instar du Colorado (Colorado AI Act), HIPAA (santé), CCPA (Californie), Exécutive Order on AI (2023) cherchent à encourager l'innovation.

2.3. Au Canada, le projet de loi C-27 sur l'IA et les données (LIAD), représente le premier pas vers une régulation spécifique en dehors des lois existantes sur la protection des renseignements personnels. L'approche se distingue par une démarche fondée sur des principes et sur une certaine souplesse réglementaire. Contrairement au modèle européen, la LIAD laisse encore à définir plusieurs critères clés (la classification des risques) et privilégie des règlements futurs pour préciser certaines obligations pour atténuer les risques de biais et de dommages liés aux systèmes d'IA et maintenir l'équilibre entre l'innovation et la responsabilité.

2.4 En Chine, la Loi sur la protection des informations personnelles (PIPL), similaire au RGPD européen vise l'utilisation de l'IA dans des domaines comme la surveillance, les médias et les services publics. Le premier souci du pays reste sa souveraineté technologique car la Chine est à l'avant-garde des juridictions qui travaille sur un cadre d'IA holistique. Les dispositions réglementaires englobent la gestion des recommandations algorithmiques, les normes éthiques pour l'IA de nouvelle génération et les opinions sur le renforcement de la gouvernance éthique de la science et de la technologie. Les entités réglementaires chinoises prévoient des approches d'application ciblées, avec des rôles qui se croisent et se chevauchent fréquemment. Les entités réglementaires importantes comprennent l'Administration du cyberespace de Chine, le

ministère de l'Industrie et des Technologies de l'information et l'Administration d'État pour la réglementation du marché.

2.5 Sur le plan international, la Perspective Internationale et l'Initiative de l'ONU font l'objet d'un consensus croissant pour une régulation globale. Un rapport de l'ONU souligne " l'irréfutable " nécessité d'un cadre réglementaire international, à la fois pour garantir le respect des droits humains et pour éviter que les bénéfices de l'IA ne soient concentrés dans quelques pays ou entreprises. Le rapport de l'ONU prône la création d'un panel international indépendant et l'instauration d'un fonds destiné à réduire le fossé numérique entre nations. Cette approche met également l'accent sur la conformité avec le droit humanitaire international en cas d'utilisation militaire (GAZA en est témoin) et appelle à une coopération mondiale renforcée. Ainsi, la régulation internationale se présente comme un complément nécessaire aux initiatives nationales pour pallier la dimension transfrontalière de la technologie.

3. Gouvernance et Mécanismes d'Exécution

Les structures de gouvernance varient sensiblement selon les juridictions. L'UE prévoit la création de l'European AI Office pour superviser l'application des règles et assurer leur conformité dans les Etats membres, renforçant ainsi la centralisation des efforts de régulation. Aux Etats-Unis, outre les actions menées par la Fédéral Trade Commission (FTC) et d'autres agences fédérales adoptent leurs propres lois, générant une diversité de pratiques qui compliquent la coordination nationale. Au Canada, le projet de loi C-27 propose une approche où les règlements complémentaires permettent de préciser les mécanismes de gouvernance, avec une forte implication des parties prenantes dans l'élaboration des règles futures.

Les exigences en matière de transparence et les sanctions pour non-conformité constituent un point de divergence majeur. Le AI Act impose que les systèmes à haut risque réalisent des évaluations d'impact détaillées et soumettent une documentation exhaustive. En cas de manquement, les sanctions financières peuvent atteindre jusqu'à 7% du chiffre d'affaires annuel ou 35 millions d'euros. Aux Etats-Unis, bien que des dispositifs de transparence existent au niveau des interventions de la FTC, la réglementation reste moins homogène et repose souvent sur l'application des lois existantes en matière de protection des consommateurs et de lutte contre les discriminations. La LIAD, au Canada prévoit la définition d'exigences pour la transparence et l'utilisation responsable des données, mais laisse encore à préciser la rigueur des sanctions. Quant à l'orientation internationale, l'accent est mis sur la nécessité d'une

transparence globale et d'un accès aux mécanismes de plainte, sans pour autant définir des sanctions punitives strictes.

La coexistence de régulations strictes (comme en Europe) et d'approches plus souples ou fragmentées (comme aux Etats-Unis) crée un environnement où les entreprises qui développent des produits d'IA doivent naviguer entre des exigences multiples et parfois contradictoires. Le manque d'harmonisation pourrait conduire à des inefficacités d'où la nécessité d'une coordination internationale. Les recommandations de l'ONU et les initiatives multilatérales (OCDE) soulignent l'urgence d'un cadre commun qui tienne compte à la fois des impératifs de sécurité, de transparence et d'éthique, tout en évitant que la régulation ne profite qu'aux économies avancées au détriment des pays du Sud.

Les Nations Unies et l'OCDE proposent des cadres généraux fondés sur des principes que les pays peuvent adapter à leurs propres réalités. C'est ainsi que le Secrétariat Général des Nations Unies a créé un comité consultatif de haut niveau en charge de la réflexion sur l'Intelligence Artificielle. L'OCDE, de son côté, publie ses Principes sur l'intelligence artificielle, un ensemble de lignes directrices visant une IA innovante, digne de confiance et respectueuse des droits humains et des valeurs démocratiques.

Pour mieux comparer ces différentes approches, le tableau ci-dessous présente les principales caractéristiques de la régulation de l'IA.

Tableau Comparatif des Principaux Cadres Réglementaires de l'IA

	UE	USA	CHINE	ONU
Approche	Classification des risques en 04 niveaux	Fragmentée, Mix des initiatives fédérales et étatiques	Holistique	Consensuelle
Gouvernance	European AI Office	FTC et Initiatives Fédérales	Administrions du Cyberespace, de la Réglementation du Marché et ministère des Technologies de l'Information	Panel International Indépendant
Sanctions	De 35 millions d'euros à 7% du CA et/ou sanctions administratives	Non homogènes mais généralement moins lourdes que dans l'UE	Environ 500 000 RMB et/ou sanctions administratives	Souples
Impact sur l'Innovation	Risque de freins	Favorable mais incertitude juridique		Partage des bénéfices

Le panorama mondial des cadres réglementaires met en lumière la diversité des réponses mises en place face aux défis posés par l'intelligence artificielle. Chaque région façonne son modèle selon ses priorités : protection des droits fondamentaux, souveraineté technologique ou stimulation de l'innovation. Cependant, la multiplication des cadres nationaux tend à fragmenter les standards, rendant la coopération essentielle pour accompagner un développement responsable et sécurisé de l'IA. Dans cet écosystème mouvant, la question de l'adaptation locale devient incontournable, puisque chaque pays doit conjuguer ambitions numériques et impératifs de sécurité.

Pour analyser la situation marocaine, il faut prendre en compte à la fois le contexte local, les initiatives gouvernementales et les défis spécifiques au pays. Le Maroc est un pays en

développement qui cherche à se positionner comme un hub technologique en Afrique. Certaines lois encadrent des aspects-clés du numérique comme la cyber sécurité (Loi n°05-20), la protection des consommateurs (Loi 09-08) sans qu'en en soit encore adopté un cadre spécifique à l'IA.

En ce sens, la Stratégie Nationale de Cybersécurité 2030 met l'accent sur la nécessité de protéger le cyberespace marocain. En tout, cette stratégie comprend 11 objectifs stratégiques et 26 initiatives, déclinées en 60 actions. La Stratégie repose sur quatre piliers principaux, le premier dédié à la gouvernance, cherche à renforcer le cadre juridique et institutionnel, en adaptant les normes et en promouvant la coordination entre les entités publiques et privées. Le deuxième pilier se concentre sur la sécurité et la résilience du cyberespace, avec des actions de protection des infrastructures vitales et de certification des mesures de prévention contre les incidents cybernétiques. Le troisième pilier met l'accent sur la formation et le développement des compétences, et la sensibilisation de la population aux risques cyber. Enfin, le quatrième pilier vise la coopération internationale, en participant aux forums régionaux et en établissant des partenariats bilatéraux.

Parallèlement, la stratégie "Maroc Digital 2030" vise à accélérer la transformation numérique et à intégrer l'IA dans des secteurs clés comme l'éducation, la santé, l'agriculture et l'industrie. Les textes récemment adoptés marquent l'opérationnalisation de l'arsenal juridique et le régime de définition des prestataires cloud. Sur un premier niveau, l'objectif est de permettre au Maroc d'exercer sa souveraineté, notamment en matière de cyber sécurité et de contrôle des prestataires cloud. Le second niveau prévoit des garanties supplémentaires de nature juridique et technique visant à s'assurer que les données sensibles, eu égard à leur confidentialité, soient traitées sur des infrastructures contrôlées par des sociétés assujetties uniquement aux législations nationales. Des entreprises locales ont effectivement vu le jour mais affichent des capacités souvent très inégales au sein d'un secteur qui évolue dans un cadre flou vulnérable aux cyberattaques.

En matière d'IA, le Maroc n'a pas de réglementation spécifique. Si le cadre légal stagne, eu égard aux évolutions vertigineuses de la technologie, son application effective par les tribunaux nécessite des améliorations, notamment en termes de formation des magistrats et de coordination entre les différents acteurs. La jurisprudence fait face à de grands défis : rareté des décisions publiées, manque de transparence des décisions rendues, expertise technique dans l'appréciation des infractions, lenteur procédurale, risque de dépérissement des preuves

numériques, diffusion des bonnes pratiques judiciaires. Les lois sectorielles, y compris celles sur la protection des données, les droits de propriété, tout en n'étant pas explicitement conçues pour l'IA, restent pertinentes dans le contexte. La gouvernance du secteur assurée par le CNDP rattaché à la Primature adopte une approche de droit souple au regard des sanctions réservées dans des affaires de cyberattaque.

Les environnements Cloud, souvent complexes et hétérogènes, augmentent le risque des fuites et des détournements de données sensibles et personnelles. Elles peuvent même compromettre l'intégrité du système, comme lors des attaques de l'Agence MAP (2023), BCP (2022), Jumia (2023), CNSS (2025), Hôpital Universitaire International Cheikh Khalifa (2022), IAM (2023), Securitech (2022) etc. La Presse écrite comme Aujourd'hui le Maroc, L'Economiste, ou Le Matin, publient souvent sur les affaires de protection des données. Les Médias en Ligne comme Hespress, TelQuel, et Medias24 offrent une couverture de ces fuites en temps réel ; les associations de défense des droits des consommateurs et de protection de la vie privée et l'Observatoire Marocain des Libertés Numériques suivent de près les violations des droits numériques.

Dans la pratique, il est très difficile de traiter spécifiquement les données sensibles, car elles sont souvent intégrées dans des systèmes contenant d'autres données moins sensibles. Sur un autre registre, le législateur ne fait guère allusion à la politique des cookies, y compris dans la loi 09-08 combien même cela porte préjudice aux usagers du web. Les sites émetteurs doivent être tenus d'informer les internautes sur la finalité des Cookies, sur leur durée de validité s'ils ne sont pas supprimés par l'internaute ainsi que sur les conséquences de leur désactivation. De plus, le développement indéniable de l'IA nécessite la mise en place d'un cadre éthique qui puisse garantir la protection des droits et libertés au regard des abus potentiels liés à l'utilisation de la machine et l'assurance d'un système de responsabilité en cas de dommage lié à l'IA.

Enfin, la question de la souveraineté technologique fait appel à la capacité du pays à contrôler et à maîtriser ses technologies, ses infrastructures numériques et les données de ses citoyens. Cela implique de réduire la dépendance vis-à-vis de l'étranger, de développer des solutions locales contre les attaques externes, de s'assurer que les données des citoyens et des entreprises sont stockées et traitées de manière sécurisée, de maîtriser les infrastructures numériques critiques et de garantir que celles-ci soient résilientes et capables de résister aux attaques et aux perturbations.

Conclusion

La régulation de l'IA reflète une tension latente entre l'innovation technologique et la protection des données fondamentales, avec des approches variées selon les contextes régionaux et culturels. Face à l'UE aspirant à une réglementation rigoureuse, s'oppose une vision américaine favorable à une réglementation plus souple stimulatrice de l'innovation. D'autres pays comme la Chine milite plus pour leur souveraineté technologique, le Canada et d'autres pays oscillent entre les deux modèles. D'autres pays, comme le Maroc, ne se sont toujours pas prononcé. Chaque bloc géopolitique a une sensibilité propre pour la vie privée, la liberté d'expression ou les priorités sécuritaires qui cache intrinsèquement une ambition de domination économique et militaire, principalement entre les Etats-Unis et la Chine. De leur part, les PED et les PMA, eu égard au décalage technologique enregistré, se retrouvent de plus en plus marginalisés face à la désinformation de masse et aux chocs économiques et épidémiologiques. La dépendance accrue aux plateformes et aux clouds étrangers, les risques de fuite des données contraint ces pays à clarifier leurs arbitrages. A défaut, ils s'exposent à une marginalisation structurelle faite de dépendances technologiques, de pertes de souveraineté sur les données et d'un affaiblissement de leur capacité régulatoire. L'enjeu n'est plus seulement de rattraper un retard, mais de bâtir des capacités essentielles (infrastructures ouvertes, talents, normes locales interopérables, coopérations régionales) afin de négocier d'égal à égal et inscrire leur trajectoire dans un numérique véritablement inclusif.

Dans l'avenir, la gouvernance internationale de l'IA sera probablement hybride, fragmentée et pragmatique. C'est pourquoi, une collaboration internationale est essentielle pour harmoniser les cadres juridiques et relever les défis communs de l'Avenir. Les avancées dépendront de la capacité à articuler coopération, gestion des risques et préservation des intérêts nationaux devant les mastodontes de la technologie (OpenAI, Google, Baidu…) et dans un climat hostile à la régulation et au multilatéralisme.

Notre pays, signataire des conventions internationales portant sur la protection des données personnelles et sur la lutte contre la cybercriminalité, s'est engagé à mettre en œuvre les recommandations de l'UNESCO sur l'utilisation éthique de l'IA. Toutefois, en l'absence de mécanismes de gouvernance et de régulation spécifiques, nos engagements internationaux auront du mal à se traduire en actions concrètes.

Dans un récent rapport, le CSES recommande de :

- Réviser la loi 09-08 relative à la protection des données personnelles afin qu'elle intègre valablement les exigences des données utilisées et générées par l'intelligence artificielle, en conformité avec les normes internationales,

- Définir un cadre juridique spécifique pour garantir une utilisation éthique et responsable des systèmes d'intelligence artificielle, les cyberattaques, ainsi que les fraudes et le vol d'identité.

- Examiner la possibilité de rejoindre un groupement de pays (Conseil de l'Europe) pour accroitre le pouvoir de négociation du notre pays vis-à-vis des grandes entreprises technologiques,

- Œuvrer, en urgence, à réaliser une cartographie de l'impact des usages de l'IA sur les métiers en ouvrant le dialogue social sur les plans d'accompagnement et de reconversion professionnelle.

Sans mécanismes de gouvernance et de régulation adaptés, le décalage entre les normes et la réalité opérationnelle s'élargira, au détriment de la confiance, de la compétitivité et de la souveraineté numérique. Les recommandations du CSES tracent une feuille de route pragmatique pour couvrir l'ensemble du cycle de vie des données liées à l'IA, pour ériger un cadre juridique spécifique avec des mécanismes d'audit et de recours effectifs, pour rejoindre des cadres de coopération, accroître notre pouvoir de négociation, et anticiper l'impact sur l'emploi

---

En somme, la priorité est de transformer des principes en capacités juridiques (lois et règlements exécutoires), institutionnelles (autorités dotées de moyens, compétences, pouvoir de sanction et souveraineté), techniques (standards, R&D, audits, sécurité) et sociales (formation, reconversion,). C'est à ce prix que notre pays pourra passer du statut de consommateur dépendant à celui d'acteur responsable et résilient, capable de tirer parti de l'IA tout en protégeant les droits fondamentaux et l'intérêt général.

BIBLIOGRAPHIE

Amer, M., Hilmi, Y., & El Kezazy, H. (2024, April). Big Data and Artificial Intelligence at the Heart of Management Control: Towards an Era of Renewed Strategic Steering. In The International Workshop on Big Data and Business Intelligence (pp. 303-316). Cham: Springer Nature Switzerland.

Barocas, Hardt & Narayanan (2023). Fairness and Machine Learning, MIT Press.

Bryson, J.J. (2020). The Artificial Intelligence of the Ethics of Artificial Intelligence, The Oxford Handbook of Ethics of AI.

Conseil Economique, Social et Environnemental - Auto-saisine n° 78/2024 Quels usages et quelles perspectives de développement de l'intelligence artificielle au Maroc ?

CNDP (2024), Rapport annuel sur la Protection des Données Personnelles, Conseil Économique, Social et Environnemental, "Avis sur l'Intelligence Artificielle et ses Défis," 2025.

Décret n° 2-09-165 du 25 Joumada I 1430 (21 mai 2009) pris pour l'application de la loi n° 09-08 relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel ; Bulletin Officiel n° 5744 du 24 Joumada II 1430 (18 juin 2009), p. 1006.

Dignum, V. (2019). Responsible Artificial Intelligence, Springer, 2019.

Dounia, G., Chaimae, K., Yassine, H., & Houda, B. (2025). ARTIFICIAL INTELLIGENCE AND BIG DATA IN MANAGEMENT CONTROL OF MOROCCAN COMPANIES: CASE OF THE RABAT-SALE-KENITRA REGION. Proceedings on Engineering, 7(2), 925-938.

Edwards, L. 2021. Data Protection, Artificial Intelligence and Ethics, Computer Law & Security Review.

Floridi, L. (2013). The Ethics of Information, 2013, Oxford University Press.

Gervais, D.J. (2022). The Machine as Author, Iowa Law Review.

Hildebrandt, M. (2015). Smart Technologies and the End(s) of Law, Edward Elgar Publishing.

Hildebrandt, M. (2020) Law for Computer Scientists, OUP.

Noble, S. U. (2018). Algorithms of Oppression, NYU Press.

OCDE, Groupe I HLEG (High-Level Expert Group on AI), Université de Montréal.

Pasquale, F. (2015). The Black Box Society: The Secret Algorithms That Control Money and Information, Harvard University Press.

Tjing, H. H. C. (2023). Liability and artificial intelligence: a balancing act, European Review of Private Law.

UNESCO (2022). Recommandations sur l'Éthique de l'Intelligence Artificielle.