L'approche par les risques comme nouveau paradigme du droit des affaires numériques: étude comparative entre le Maroc et la France

ABADI AHLAM
Doctorante
La Faculté des Sciences Juridiques Economiques et Sociales de Tanger
Laboratoire des sciences juridiques économiques sociales et de gestion
Maroc

Ce travail a été réalisé avec le soutien financier du Centre National pour la Recherche Scientifique et Technique (CNRST) du Maroc.

Résumé

La transformation numérique de l'économie, portée par l'essor des systèmes d'intelligence artificielle (IA), met à l'épreuve les fondements du droit des affaires, conçu pour encadrer des échanges relativement prévisibles. Face à des risques technologiques complexes, évolutifs et parfois systémiques, l'approche par les risques s'impose comme un paradigme de régulation fondé sur l'anticipation, la proportionnalité et la responsabilisation des acteurs, plutôt que sur la seule réparation a posteriori. Selon une méthode qualitative, comparative et fonctionnelle, cet article analyse la consécration de cette approche dans le droit européen et français, notamment par le règlement (UE) 2024/1689 (AI Act), puis sa manifestation indirecte et fragmentée dans le droit marocain (protection des données, cybersécurité, services de confiance). Il montre que les deux systèmes convergent fonctionnellement autour de la gestion des risques technologiques, tout en divergeant structurellement quant à l'unité et à l'intensité du cadre normatif. Il soutient que l'approche par les risques peut constituer un langage commun de régulation, dont le droit marocain peut s'inspirer sans transposition mécanique du modèle européen.

Mots-clés : approche par les risques ; droit des affaires numériques ; intelligence artificielle ; AI Act ; conformité ; droit comparé ; Maroc ; France.

Abstract

The digital transformation of the economy, driven by the rapid development of artificial intelligence (AI) systems, challenges the traditional foundations of business law, which was designed to govern relatively predictable exchanges. Faced with complex, evolving and sometimes systemic technological risks, the risk-based approach is emerging as a regulatory paradigm built on anticipation, proportionality and the accountability of economic actors, rather than on ex post liability alone. Using a qualitative, comparative and functional method, this article examines how the approach has been enshrined in European and French law, in particular through Regulation (EU) 2024/1689 (the AI Act), and how it appears, indirectly and in a fragmented manner, in Moroccan law (data protection, cybersecurity, trust services). It shows that both systems converge functionally around the management of technological risks while diverging structurally as to the unity and intensity of the normative framework. It argues that the risk-based approach can serve as a common regulatory language from which Moroccan law may draw inspiration without mechanically transposing the European model.

Keywords: risk-based approach; digital business law; artificial intelligence; AI Act; compliance; comparative law; Morocco; France.

Introduction

Le droit des affaires s'est historiquement construit autour d'un objectif de sécurité des transactions : fixer les règles de formation et d'exécution des contrats, organiser la responsabilité des opérateurs et garantir, par le jeu de la réparation, la confiance dans les échanges. Ce modèle, largement fondé sur la responsabilité a posteriori, suppose des risques identifiables, des chaînes de causalité reconstituables et des préjudices imputables à un auteur déterminé. La transformation numérique de l'économie, et tout particulièrement le développement rapide des systèmes d'intelligence artificielle (IA), met ces présupposés en tension. L'opacité des modèles, la reproduction de biais dans les décisions automatisées, les atteintes potentielles aux droits fondamentaux et les risques cybernétiques engendrent des dommages diffus, difficiles à imputer et susceptibles de se propager à l'échelle de marchés entiers.[1]

Dans ce contexte, l'approche par les risques s'impose progressivement comme un nouveau paradigme de régulation. On l'entendra ici comme une technique normative qui module l'intensité des obligations juridiques en fonction de la probabilité et de la gravité des préjudices que l'activité réglementée est susceptible de causer, et qui déplace ainsi le centre de gravité du droit de la sanction vers la prévention.[2] Le législateur européen en a fait la clé de voûte du règlement (UE) 2024/1689 sur l'intelligence artificielle, dit « AI Act », dont l'article 3 définit le risque comme la combinaison de la probabilité d'un préjudice et de sa gravité.[3] La logique n'est toutefois pas propre à l'IA : elle irrigue déjà, depuis plusieurs années, le droit des données personnelles, de la cybersécurité et des services numériques.

La problématique de cette étude est double. Elle consiste d'abord à se demander dans quelle mesure l'approche par les risques renouvelle le droit des affaires numériques, puis

[1]Sur la thématique d'une société confrontée à des risques produits par son propre développement technique, voir U. Beck, *La société du risque. Sur la voie d'une autre modernité*, trad. L. Bernardi, Paris, Aubier, 2001 (éd. orig. 1986). Sur la nécessité d'un droit qui anticipe plutôt que de réparer seulement, voir M. Delmas-Marty, *Résister, responsabiliser, anticiper*, Paris, Seuil, 2013.

[2]J. Black, « The Emergence of Risk-Based Regulation and the New Public Risk Management in the United Kingdom », *Public Law*, 2005, p. 512 et s. ; R. Baldwin, M. Cave et M. Lodge, *Understanding Regulation: Theory, Strategy, and Practice*, 2e éd., Oxford, Oxford University Press, 2012.

[3]Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle, JOUE, 12 juillet 2024, art. 3, point 2 (ci-après « AI Act »). Le texte a été modifié en 2026 par le règlement (UE) 2026/1744, présenté infra.

comment elle se traduit dans des contextes juridiques différenciés. Plus précisément, il s'agit de s'interroger sur la manière dont cette approche, consacrée par l'AI Act et mise en œuvre en France, peut inspirer l'évolution du droit marocain des affaires numériques sans conduire à une transposition mécanique de modèles étrangers. Une question centrale en découle : l'approche par les risques peut-elle constituer un socle commun de régulation des affaires numériques, conciliant innovation, compétitivité économique et sécurité juridique ?

Le choix de comparer le Maroc et la France se justifie par plusieurs raisons. La France évolue dans un cadre européen harmonisé qui offre aujourd'hui le modèle le plus abouti de régulation de l'IA par les risques. Le Maroc, pour sa part, partage avec elle une tradition juridique de droit écrit et des relations économiques denses, que l'accord d'association avec l'Union européenne a durablement structurées.[4] Surtout, les entreprises marocaines qui fournissent des systèmes d'IA au marché européen, ou dont les résultats sont utilisés dans l'Union, relèvent directement du champ d'application du règlement, de sorte que la question de la régulation par les risques ne relève plus d'un simple choix de politique législative nationale.

Sur le plan méthodologique, l'étude adopte une approche qualitative et comparative. Elle repose sur l'analyse des textes européens et français relatifs à la régulation de l'intelligence artificielle et du numérique, en particulier l'AI Act, ainsi que sur l'examen des instruments juridiques marocains encadrant la protection des données, la cybersécurité et la confiance numérique. Cette démarche est complétée par une analyse fonctionnelle centrée sur la notion de risque. Fondée sur l'idée que des systèmes juridiques différents peuvent répondre à un même problème social par des techniques distinctes, la méthode fonctionnelle permet de dépasser les différences formelles pour dégager les logiques communes et les spécificités nationales.[5] Les limites de l'exercice tiennent à la rareté de la jurisprudence marocaine en la matière et au caractère encore évolutif des projets normatifs nationaux, dont l'étude s'en tient à l'état connu à la date de rédaction.

L'hypothèse qui guide la démonstration est celle d'une convergence fonctionnelle et d'une divergence structurelle : le droit français et le droit marocain poursuivent un objectif

[4]Accord euro-méditerranéen établissant une association entre les Communautés européennes et leurs États membres, d'une part, et le Royaume du Maroc, d'autre part, JOCE L 70, 18 mars 2000, p. 2.

[5]K. Zweigert et H. Kötz, *Introduction to Comparative Law*, 3e éd., Oxford, Clarendon Press, 1998, spéc. le chapitre consacré à la méthode comparative.

voisin de maîtrise des risques technologiques, mais l'un le réalise par un cadre unifié, précis et contraignant, l'autre par des instruments dispersés et pragmatiques. L'étude examinera, dans un premier temps, la consécration de l'approche par les risques dans le droit européen et français des affaires numériques (I), puis sa manifestation dans le droit marocain, à l'épreuve de la comparaison avec le modèle français (II).

I. La consécration de l'approche par les risques dans le droit européen et français des affaires numériques

L'approche par les risques trouve sa consécration la plus aboutie dans le cadre européen de régulation de l'intelligence artificielle, mais elle ne surgit pas ex nihilo. Elle prolonge une évolution de longue durée, qui a fait du risque une catégorie juridique à part entière (A), avant de recevoir, avec l'AI Act, une traduction systématique (B) dont la mise en œuvre française confère à l'entreprise un rôle central (C).

A. Du concept à la norme : le risque comme catégorie juridique

La montée en puissance du risque dans le discours juridique accompagne la prise de conscience que les sociétés techniques produisent des dangers dont elles ne maîtrisent pas toujours l'étendue. Au plan philosophique, le principe responsabilité de Hans Jonas invite à prendre en compte les effets lointains de l'action technique,[6] tandis que la réflexion sur le principe de précaution a montré comment le droit pouvait se saisir d'incertitudes scientifiques non encore dissipées.[7] Au plan de la théorie de la régulation, la littérature a décrit l'émergence d'une régulation fondée sur les risques, qui conduit l'autorité de contrôle à allouer ses ressources et à graduer ses exigences en fonction de l'ampleur des dangers, plutôt que d'appliquer uniformément une même règle à tous les opérateurs.[8]

Le droit européen du numérique a progressivement intégré cette logique avant même l'IA. Le règlement général sur la protection des données (RGPD) impose au responsable du traitement de mettre en œuvre des mesures adaptées au risque que le traitement fait peser sur les droits et libertés des personnes, d'intégrer la protection des données dès la conception, d'assurer un niveau de sécurité approprié au risque et, lorsque le traitement

[6]H. Jonas, *Le principe responsabilité. Une éthique pour la civilisation technologique*, trad. J. Greisch, Paris, Cerf, 1990.

[7]F. Ewald, « Philosophie de la précaution », *L'Année sociologique*, vol. 46, n° 2, 1996, p. 383 et s.

[8]J. Black, art. cit. ; J. Black et R. Baldwin, « Really Responsive Risk-Based Regulation », *Law & Policy*, vol. 32, n° 2, 2010, p. 181-213.

est susceptible d'engendrer un risque élevé, de réaliser une analyse d'impact préalable.[9] Le règlement sur les services numériques (DSA) impose de son côté aux très grandes plateformes d'évaluer et d'atténuer les risques systémiques que leurs services font peser sur la société,[10] et la directive NIS 2 exige des entités qu'elle vise l'adoption de mesures de gestion des risques en matière de cybersécurité.[11] Dans ces textes, le risque n'est plus seulement une éventualité dont le droit répare les conséquences : il devient l'objet même de l'obligation, qui porte sur l'identification, l'évaluation et la réduction des dangers en amont.

C'est dans ce terreau que s'inscrit la réflexion européenne sur l'IA. Les lignes directrices du groupe d'experts de haut niveau de 2019 ont posé les exigences d'une IA digne de confiance,[12] puis le Livre blanc de la Commission de 2020 a explicitement retenu une approche proportionnée, fondée sur les risques, afin de ne pas faire peser de contraintes disproportionnées sur les usages les moins dangereux.[13] La proposition de règlement de 2021 a transformé cette orientation en architecture normative.[14] Le droit des affaires numériques se trouve ainsi saisi par un mouvement de fond, où la conformité préventive tend à compléter, voire à supplanter, la logique de la seule responsabilité.

B. L'AI Act : le risque comme critère central de la normativité

L'AI Act érige le risque en critère central de la normativité : les obligations juridiques applicables aux acteurs économiques ne dépendent pas de la technologie en tant que telle, mais de l'usage qui en est fait et du danger qu'il engendre. Le règlement établit pour cela une classification à plusieurs niveaux. Au sommet, certaines pratiques sont interdites en raison du risque inacceptable qu'elles représentent, comme la manipulation subliminale

[9]Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, JOUE L 119, 4 mai 2016, p. 1, art. 24, 25, 32 et 35.

[10]Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques, JOUE L 277, 27 octobre 2022, art. 34 et 35.

[11]Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022, JOUE L 333, 27 décembre 2022, art. 21.

[12]Groupe d'experts de haut niveau sur l'intelligence artificielle, *Lignes directrices en matière d'éthique pour une IA digne de confiance*, Commission européenne, 8 avril 2019.

[13]Commission européenne, *Livre blanc sur l'intelligence artificielle. Une approche européenne axée sur l'excellence et la confiance*, COM(2020) 65 final, 19 février 2020.

[14]Commission européenne, Proposition de règlement établissant des règles harmonisées concernant l'intelligence artificielle, COM(2021) 206 final, 21 avril 2021.

causant un préjudice, l'exploitation des vulnérabilités de certaines personnes, la notation sociale ou, sous réserve d'exceptions strictement encadrées, l'identification biométrique à distance en temps réel dans l'espace public à des fins répressives.[15]

Le deuxième niveau, le plus structurant pour les entreprises, est celui des systèmes à haut risque. Il regroupe d'une part les systèmes qui constituent des composants de sécurité de produits déjà soumis à une législation d'harmonisation (dispositifs médicaux, machines, jouets), d'autre part des systèmes utilisés dans des domaines énumérés à l'annexe III : biométrie, gestion d'infrastructures critiques, éducation, emploi et gestion des travailleurs, accès aux services essentiels dont l'évaluation de la solvabilité, activités répressives, migration, justice.[16] Pour ces systèmes, le règlement impose un véritable régime de gouvernance : un système de gestion des risques continu, des exigences de qualité des données, une documentation technique, la journalisation des événements, la transparence à l'égard des employeurs, un contrôle humain effectif, ainsi qu'un niveau approprié d'exactitude, de robustesse et de cybersécurité.[17] Les employeurs ne sont pas en reste, puisqu'ils doivent notamment assurer la surveillance humaine et, pour certains d'entre eux, procéder à une analyse d'impact sur les droits fondamentaux.[18]

Le troisième niveau est celui des risques limités, pour lesquels le règlement se borne à imposer des obligations de transparence : l'utilisateur doit savoir qu'il interagit avec un système d'IA, et les contenus synthétiques doivent être signalés comme tels.[19] Le dernier niveau, celui des risques minimaux, échappe à toute obligation spécifique, les opérateurs étant simplement encouragés à adopter des codes de conduite volontaires.[20] S'y ajoute un régime propre aux modèles d'IA à usage général, gradué selon que le modèle présente ou non un risque systémique.[21] L'effectivité de l'ensemble est assurée par un dispositif de sanctions pécuniaires dont le plafond, pour les violations les plus graves, atteint 35 millions

[15]AI Act, art. 5.

[16]AI Act, art. 6 et annexes I et III.

[17]AI Act, art. 9 à 15. L'évaluation de la conformité et le marquage CE relèvent des articles 43 et 48, l'enregistrement dans la base de données de l'Union de l'article 49 et la surveillance après commercialisation de l'article 72.

[18]AI Act, art. 26 et 27.

[19]AI Act, art. 50.

[20]AI Act, art. 95.

[21]AI Act, art. 51 à 55.

d'euros ou 7 % du chiffre d'affaires annuel mondial,[22] et par une portée extraterritoriale qui vise les fournisseurs établis hors de l'Union dès lors que leurs systèmes sont mis sur le marché européen ou que leurs résultats y sont utilisés.[23]

Le calendrier d'application de cette architecture a toutefois été aménagé. Entré en vigueur le 1er août 2024, le règlement a vu les pratiques interdites s'appliquer dès le 2 février 2025 et les obligations relatives aux modèles à usage général dès le 2 août 2025. Le règlement (UE) 2026/1744, dit « Omnibus numérique sur l'IA », est entré en vigueur le 27 juillet 2026 et a reporté l'application des obligations relatives aux systèmes à haut risque de l'annexe III au 2 décembre 2027, celles qui concernent les systèmes intégrés dans des produits de l'annexe I étant reportées au 2 août 2028.[24] Ce report ne remet pas en cause l'architecture fondée sur les risques : il en modifie le rythme, non la logique.

La doctrine a relevé les forces et les limites de ce modèle. Il apporte une prévisibilité accrue et une proportionnalité que ne garantissait pas une règle uniforme, et il illustre une conception de la régulation de l'IA ancrée dans la protection des droits fondamentaux.[25] Il a aussi été critiqué : le recours à des catégories préétablies et à des listes d'usages risque de figer le droit face à une technologie mouvante, de laisser échapper des risques émergents et de reposer largement sur l'auto-évaluation des fournisseurs.[26] Des travaux plus récents plaident pour une évaluation du risque davantage contextualisée et proportionnée, fondée sur des scénarios d'usage.[27] Ces débats ne contredisent pas le paradigme ; ils en précisent les conditions d'efficacité, et ils intéressent directement le législateur qui voudrait s'en inspirer.

---

[22]AI Act, art. 99.

[23]AI Act, art. 2, paragraphe 1.

[24]Règlement (UE) 2026/1744 modifiant le règlement (UE) 2024/1689, publié au JOUE le 24 juillet 2026 et entré en vigueur le 27 juillet 2026. Il convient de vérifier ces dates dans le texte officiel, publié sur EUR-Lex, avant toute citation définitive.

[25]L. Floridi, « The European Legislation on AI: A Brief Analysis of Its Philosophical Approach », *Philosophy & Technology*, vol. 34, 2021, p. 215-222.

[26]M. Veale et F. Zuiderveen Borgesius, « Demystifying the Draft EU Artificial Intelligence Act », *Computer Law Review International*, vol. 22, n° 4, 2021, p. 97-112.

[27]C. Novelli, F. Casolari, A. Rotolo, M. Taddeo et L. Floridi, « AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act », *Digital Society*, vol. 3, 2024.

C. La mise en œuvre française : régulation par la conformité et responsabilisation de l'entreprise

Dans le contexte français, l'AI Act s'insère dans un environnement juridique déjà structuré autour de la protection des données personnelles, de la cybersécurité et de la conformité numérique. La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, régulièrement modifiée pour intégrer le RGPD, offre un socle ancien de contrôle des traitements,[28] auquel se sont ajoutées les adaptations nationales du droit européen des services numériques par la loi du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique.[29] Les autorités nationales y jouent un rôle déterminant. La Commission nationale de l'informatique et des libertés (CNIL) a fait de l'IA un axe prioritaire, en publiant un plan d'action en mai 2023 et en développant une doctrine sur l'application du RGPD aux systèmes d'IA,[30] tandis que l'Agence nationale de la sécurité des systèmes d'information (ANSSI) promeut une démarche d'analyse de risque structurée, dont la méthode EBIOS Risk Manager est la référence.[31] L'articulation de ces autorités avec les autorités de surveillance du marché que chaque État membre doit désigner au titre de l'AI Act relève de la mise en œuvre nationale du règlement.[32]

Le droit français disposait par ailleurs d'une véritable culture de la cartographie des risques, que l'AI Act vient prolonger. La loi du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique impose aux grandes entreprises de se doter d'un dispositif comprenant une cartographie des risques,[33] et la loi du 27 mars 2017 sur le devoir de vigilance exige des sociétés mères et donneuses d'ordre un plan identifiant les risques d'atteintes graves aux droits humains et à l'environnement.[34] Le droit des affaires français a ainsi déjà admis que l'entreprise doit, en

[28]Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée.

[29]Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique.

[30]CNIL, *Intelligence artificielle : le plan d'action de la CNIL*, 16 mai 2023.

[31]ANSSI, *EBIOS Risk Manager. Le guide*, 2018.

[32]AI Act, art. 70.

[33]Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, art. 17.

[34]Loi n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre, codifiée à l'article L. 225-102-4 du Code de commerce.

amont de toute faute, identifier ses risques et rendre compte de sa maîtrise de ceux-ci, ce que la doctrine rattache au mouvement plus large de la compliance.[35]

Le droit français a également précisé, en amont de l'AI Act, les conditions de licéité des décisions algorithmiques. La loi pour une République numérique de 2016 a imposé à l'administration d'informer les personnes des décisions prises sur le fondement d'un traitement algorithmique et de leur permettre d'en obtenir les règles essentielles,[36] et le Conseil constitutionnel a admis le recours à des décisions administratives fondées sur des algorithmes à la condition que le responsable du traitement en conserve la maîtrise et soit en mesure d'en expliquer le fonctionnement.[37] La Cour de justice de l'Union européenne a, dans le même esprit, retenu une conception large de la décision automatisée prohibée par l'article 22 du RGPD, en y incluant le calcul d'un score dont dépend de manière déterminante la décision d'un tiers.[38]

Il en résulte une responsabilité accrue des entreprises. Le droit français des affaires numériques les oblige à intégrer la gestion des risques algorithmiques dans leurs processus décisionnels, leur gouvernance interne et leurs stratégies économiques : inventaire des systèmes d'IA utilisés, qualification de leur niveau de risque, désignation de responsables, documentation des choix de conception, encadrement contractuel des relations entre fournisseurs et utilisateurs, formation des équipes. L'entreprise devient ainsi un acteur clé de la régulation, chargé d'anticiper les risques et de garantir un usage conforme et responsable des technologies numériques. Cette responsabilisation emporte une conséquence essentielle pour la comparaison : l'efficacité du modèle repose moins sur la sanction que sur la capacité des acteurs économiques et des autorités à évaluer des risques, capacité qui suppose des ressources, une expertise et un cadre normatif lisible.

II. L'approche par les risques dans le droit marocain des affaires numériques à l'épreuve de la comparaison avec la France

À la différence de la France, le Maroc ne dispose pas encore d'un cadre normatif unifié spécifiquement dédié à la régulation de l'intelligence artificielle. L'approche par les risques

[35]M.-A. Frison-Roche (dir.), *Régulation, supervision, compliance*, Paris, Dalloz, 2017.

[36]Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, art. 4, introduisant l'article L. 311-3-1 du Code des relations entre le public et l'administration.

[37]Cons. const., décision n° 2018-765 DC du 12 juin 2018, Loi relative à la protection des données personnelles.

[38]CJUE, 7 décembre 2023, *SCHUFA Holding (Scoring)*, aff. C-634/21, EU:C:2023:957.

n'en est pas absente, mais elle s'y manifeste de manière indirecte (A). La comparaison avec le modèle français révèle une convergence fonctionnelle accompagnée de divergences structurelles (B) et ouvre la voie à une appropriation contextualisée (C).

A. Une approche par les risques implicite et fragmentée

L'approche par les risques se manifeste, dans le droit marocain, à travers plusieurs textes encadrant les usages numériques, sans jamais être érigée en principe directeur explicite. En matière de données personnelles, la loi n° 09-08 du 18 février 2009 a institué la Commission nationale de contrôle de la protection des données à caractère personnel (CNDP) et soumis les traitements à un régime de déclaration ou d'autorisation préalable, assorti d'exigences renforcées pour les catégories de données les plus sensibles, de garanties de sécurité et de conditions encadrant les transferts à l'étranger.[39] Le texte, inspiré de la directive 95/46/CE, module ainsi le contrôle en fonction de la nature du traitement et des données en cause. La CNDP a en outre rappelé en mars 2025 que les traitements d'IA utilisant des données personnelles relèvent de la loi n° 09-08, ce qui montre que le droit existant est déjà mobilisé pour encadrer ces usages.[40] À la différence du RGPD, la loi n° 09-08 n'organise pas, à notre connaissance, une analyse d'impact généralisée ni une obligation d'évaluation du risque algorithmique.

En matière de cybersécurité, la loi n° 05-20 relative à la cybersécurité a posé un cadre national de protection des systèmes d'information, dont la logique de gradation est plus nette.[41] Elle distingue en effet les infrastructures d'importance vitale, soumises à des obligations renforcées de protection, d'audit et de notification des incidents, du reste des entités concernées, et confie à la Direction générale de la sécurité des systèmes d'information (DGSSI) un rôle central de supervision. La confiance dans les échanges électroniques est, quant à elle, encadrée par la loi n° 43-20 relative aux services de confiance pour les transactions électroniques, qui organise la qualification des

[39]Loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, promulguée par le dahir n° 1-09-15 du 22 safar 1430 (18 février 2009).

[40]CNDP, communiqué du 18 mars 2025 relatif aux traitements d'intelligence artificielle, tel que rapporté par *TelQuel*, hors-série n° 1175, 10-16 avril 2026.

[41]Loi n° 05-20 relative à la cybersécurité, promulguée par le dahir n° 1-20-69 du 4 hija 1441 (25 juillet 2020) ; décret n° 2-21-406 pris pour son application.

prestataires,[42] et par la loi n° 53-05 relative à l'échange électronique de données juridiques,[43] auxquelles s'ajoute la répression pénale de l'atteinte aux systèmes de traitement automatisé de données.[44]

Cette régulation fragmentée témoigne d'une volonté de sécuriser les échanges numériques et de renforcer la confiance dans l'économie digitale, tout en préservant l'attractivité économique et l'innovation. Elle s'inscrit dans l'orientation du nouveau modèle de développement, qui fait de la confiance et de la transformation numérique des leviers de la croissance.[45] Mais elle laisse subsister une lacune que la doctrine et les travaux d'analyse relèvent : ces instruments, pris isolément, ne suffisent pas à encadrer les usages de l'IA, notamment au regard de la responsabilité en cas de dommage, de la transparence des algorithmes et de la protection des droits fondamentaux.[46]

Les pouvoirs publics marocains ont engagé une réflexion pour combler cette lacune. Les autorités ont annoncé la préparation d'une loi-cadre relative à l'IA et à la gouvernance numérique, énonçant des principes fondamentaux, des obligations de conformité et des garanties éthiques, et la création d'une direction générale de l'intelligence artificielle rattachée au ministère de la Transition numérique et de la Réforme de l'administration.[47]

---

[42]Loi n° 43-20 relative aux services de confiance pour les transactions électroniques, promulguée par le dahir n° 1-20-100 du 16 journada I 1442 (31 décembre 2020).

[43]Loi n° 53-05 relative à l'échange électronique de données juridiques, promulguée par le dahir n° 1-07-129 du 19 kaada 1428 (30 novembre 2007).

[44]Loi n° 07-03 complétant le Code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données, dahir n° 1-03-197 du 16 ramadan 1424 (11 novembre 2003).

[45]Commission spéciale sur le modèle de développement, *Le nouveau modèle de développement : libérer les énergies et restaurer la confiance pour accélérer la marche vers le progrès et la prospérité pour tous*, Rabat, avril 2021.

[46]A. Haounani, « L'intelligence artificielle au Maroc : entre éthique et réglementation », *Afkar/Idées*, automne-hiver 2024 ; voir aussi l'étude « Développer le cadre juridique de l'intelligence artificielle au Maroc », présentée dans Hespress, « L'IA au Maroc : un développement rapide, un encadrement juridique absent », 23 juin 2025.

[47]S. Lokmane-Khelil, « Le Maroc va créer une direction générale de l'intelligence artificielle », *Acteurs publics*, 20 octobre 2025. À notre connaissance, aucune loi-cadre sur l'IA n'avait été définitivement adoptée à la date de rédaction de cet article ; il convient de vérifier l'état d'avancement de ce projet avant publication.

Cette évolution, qui s'inscrit dans la stratégie Maroc Digital 2030, constitue le contexte dans lequel la comparaison prend tout son intérêt.

B. Convergences fonctionnelles et divergences structurelles

La comparaison avec le modèle français met en évidence une convergence fonctionnelle autour de la gestion des risques technologiques, mais également des divergences structurelles. Le tableau suivant en synthétise les principaux traits.

Tableau 1 – Approche par les risques : traits comparés

Critère	Union européenne et France	Maroc
Source normative	Règlement directement applicable (AI Act), complété par le RGPD, le DSA et NIS 2 et relayé par le droit national	Textes sectoriels distincts (lois 09-08, 05-20, 43-20, 53-05) ; loi-cadre sur l'IA en préparation
Critère de gradation	Niveau de risque de l'usage (inacceptable, élevé, limité, minimal) ; risque systémique des modèles à usage général	Nature des données traitées et criticité des infrastructures et des systèmes
Obligations des opérateurs	Gestion des risques, documentation, contrôle humain, évaluation de conformité, analyse d'impact	Déclaration ou autorisation préalable, mesures de sécurité, audits et notification d'incidents pour les infrastructures vitales
Autorités de contrôle	CNIL, ANSSI, autorités de surveillance du marché ; Bureau européen de l'IA	CNDP, DGSSI ; coordination de l'IA en cours de structuration
Sanctions	Amendes proportionnées au chiffre d'affaires (AI Act, art. 99)	Sanctions prévues texte par texte

Source : élaboration de l'auteure à partir des textes cités.

Sur le plan fonctionnel, les deux systèmes partagent d'abord la finalité : sécuriser les échanges numériques et renforcer la confiance des acteurs économiques. Ils recourent ensuite, l'un et l'autre, à une modulation du régime juridique selon la sensibilité des données ou la criticité des systèmes, et reposent sur des autorités administratives spécialisées. Ils privilégient enfin, à des degrés divers, un contrôle ex ante, qui passe chez l'un par la conformité et l'analyse d'impact, chez l'autre par la déclaration, l'autorisation préalable et l'audit. Cette proximité ne tient pas du hasard, la loi n° 09-08 ayant été conçue dans le sillage du droit européen des données, et elle rend plausible une réception progressive de l'approche européenne par les risques.

Les divergences sont cependant structurelles. La première tient à l'unité du cadre : là où la France évolue dans un cadre européen harmonisé, fondé sur des obligations juridiques précises et contraignantes, le Maroc dispose de textes sectoriels dont la cohérence d'ensemble reste à construire. La deuxième tient à la méthode : le modèle européen fait de l'entreprise le premier évaluateur de ses risques, alors que le droit marocain s'en remet davantage au contrôle administratif préalable. La troisième tient aux capacités de mise en œuvre : une régulation fondée sur l'évaluation des risques suppose des autorités dotées d'expertise technique, des opérateurs capables de documenter leurs systèmes et un tissu d'entreprises en mesure de supporter le coût de la conformité. Or la structure de l'économie marocaine, où les petites entreprises sont nombreuses et où le poids de l'informel demeure significatif,[48] invite à la prudence. Le Maroc privilégie ainsi une approche progressive et pragmatique, adaptée à son niveau de maturité numérique et à ses priorités économiques.

Une importante nuance doit toutefois être apportée, car la comparaison ne se joue pas seulement entre deux ordres juridiques indépendants. L'AI Act s'applique, à raison de sa portée extraterritoriale, aux entreprises marocaines qui fournissent ou exploitent des systèmes d'IA à destination du marché européen, de sorte que celles-ci se trouvent déjà, de fait, soumises à la logique des risques. Ce que l'on a appelé l'« effet Bruxelles » décrit cette capacité de l'Union à exporter ses normes par la force de son marché.[49] Le droit

[48]Voir, sur la nécessité de contextualiser la régulation de l'IA en tenant compte du poids de l'informel, l'entretien de la ministre de la Transition numérique et de la Réforme de l'administration, « Le Maroc prépare un cadre légal et une direction générale dédiés à l'IA », *Le360*.

[49]A. Bradford, *The Brussels Effect: How the European Union Rules the World*, Oxford, Oxford University Press, 2020.

marocain n'est pas tenu d'en reprendre la lettre, mais il ne peut en ignorer l'esprit sans pénaliser ses propres opérateurs.

C. Vers une appropriation contextualisée : pistes pour un cadre transversal de gouvernance de l'IA

Dans cette perspective, l'approche par les risques pourrait constituer un levier stratégique pour structurer l'évolution future du droit marocain des affaires numériques, en favorisant l'émergence d'un cadre transversal de gouvernance de l'intelligence artificielle, inspiré du modèle européen mais ajusté aux réalités nationales. Le point de départ tient à l'insuffisance des mécanismes de réparation classiques. Le droit commun de la responsabilité du Dahir des obligations et des contrats, qu'il s'agisse de la faute (articles 77 et 78) ou de la responsabilité du fait des choses sous garde (article 88),[50] se prête mal à des dommages issus de systèmes autonomes, évolutifs et opaques, dont la preuve de la faute et du lien de causalité est particulièrement délicate. Ce constat plaide pour un droit complémentaire, préventif et gradué.

Plusieurs orientations méritent d'être envisagées. La première consiste à consacrer légalement la notion de risque et le principe de proportionnalité, afin d'offrir aux opérateurs un critère clair de modulation des obligations. La deuxième consiste à retenir une classification simple, à peu de niveaux, dont les listes d'usages relevant des catégories les plus sensibles seraient actualisées par voie réglementaire, de manière à éviter la rigidité reprochée à l'AI Act. La troisième tient à la clarification institutionnelle : la CNDP, la DGSSI et la future direction générale de l'IA gagneraient à voir leurs compétences articulées, afin d'éviter le chevauchement des contrôles. La quatrième concerne le contenu des obligations, qui pourraient être graduées selon le niveau de risque, depuis l'inventaire et la documentation des systèmes jusqu'à l'analyse d'impact et au contrôle humain pour les usages les plus sensibles, comme le recrutement, l'octroi de crédit ou la santé.

Une régulation par les risques ne doit cependant pas se réduire à un surcroît de contraintes. Les instruments d'innovation qui l'accompagnent dans le droit européen méritent la même attention : espaces d'expérimentation réglementaire, codes de conduite,

[50]Dahir formant Code des obligations et des contrats du 9 ramadan 1331 (12 août 1913), art. 77, 78 et 88.

normes techniques, accompagnement des petites entreprises.[51] L'adaptation suppose aussi de tenir compte des priorités nationales de souveraineté numérique et de développement de l'écosystème local, ainsi que de l'inscription du Maroc dans des cadres internationaux de référence, tels que la recommandation de l'UNESCO sur l'éthique de l'intelligence artificielle et les principes de l'OCDE sur l'IA.[52] Un calendrier progressif, alignant les exigences nationales sur les standards européens sans s'y réduire, permettrait en outre aux entreprises marocaines exportatrices de rationaliser leurs coûts de conformité.

Cette appropriation contextualisée écarte la tentation d'une transposition mécanique. Reproduire à l'identique un règlement conçu pour un marché intégré de plusieurs centaines de millions d'habitants, doté d'institutions supranationales et d'une capacité d'expertise considérable, risquerait de produire un droit formellement ambitieux mais difficilement appliqué. L'enjeu consiste plutôt à retenir de l'approche européenne sa logique, qui est celle de la proportionnalité, de l'anticipation et de la responsabilisation, et à en choisir les instruments en fonction des capacités et des objectifs économiques du pays.

Conclusion

L'approche par les risques s'affirme comme un élément central de la transformation contemporaine du droit des affaires numériques. Elle traduit un changement profond dans la manière de concevoir la régulation des technologies numériques, en mettant l'accent sur l'anticipation, la proportionnalité et la responsabilisation des acteurs économiques, là où le droit classique privilégiait la réparation des dommages une fois ceux-ci réalisés. Consacrée de façon systématique par l'AI Act, relayée en France par un environnement de conformité déjà structuré, elle fait de l'entreprise un acteur de la régulation, tenu d'identifier, d'évaluer et de maîtriser les risques que ses systèmes engendrent.

L'étude comparative a permis de vérifier l'hypothèse de départ. Le droit marocain connaît une approche par les risques indirecte, perceptible dans la protection des données, la cybersécurité et les services de confiance, qui traduit une convergence fonctionnelle avec le modèle français autour de la gestion des risques technologiques. Elle s'en distingue cependant par l'absence d'un cadre unifié, par une moindre précision des obligations et par une méthode qui repose davantage sur le contrôle administratif préalable que sur

[51] Sur les espaces d'expérimentation réglementaire, voir AI Act, art. 57.

[52] UNESCO, *Recommandation sur l'éthique de l'intelligence artificielle*, 23 novembre 2021 ; OCDE, *Recommandation du Conseil sur l'intelligence artificielle*, 22 mai 2019.

l'évaluation des risques par l'entreprise. Ces écarts ne traduisent pas un retard à combler mécaniquement : ils reflètent un niveau de maturité numérique et des priorités économiques propres, auxquels une approche progressive et pragmatique reste adaptée.

La réponse à la question centrale est ainsi nuancée mais positive. L'approche par les risques peut constituer un langage commun de régulation, c'est-à-dire un socle partagé permettant de concilier innovation, compétitivité et sécurité juridique, à la condition d'être adaptée au contexte. Pour le Maroc, la voie la plus prometteuse paraît être celle d'un cadre transversal de gouvernance de l'IA, qui consacrerait la notion de risque et le principe de proportionnalité, articulerait les compétences institutionnelles existantes et s'accompagnerait d'instruments favorables à l'innovation et au soutien des petites entreprises.

Cette recherche appelle des prolongements. Une étude empirique de la pratique des autorités et des entreprises marocaines permettrait de mesurer l'effectivité des instruments actuels, tandis que le suivi de l'élaboration de la loi-cadre annoncée et de la mise en œuvre de l'AI Act après les aménagements de 2026 offrira de nouveaux éléments de comparaison. Loin d'être une simple technique juridique, l'approche par les risques constitue un cadre structurant pour l'élaboration d'un droit des affaires numériques capable de concilier innovation, compétitivité et sécurité juridique dans un environnement numérique en

Bibliographie

Textes de l'Union européenne et textes internationaux

Accord euro-méditerranéen établissant une association entre les Communautés européennes et leurs États membres, d'une part, et le Royaume du Maroc, d'autre part, JOCE L 70, 18 mars 2000.

Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 (NIS 2), JOUE L 333, 27 décembre 2022.

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD), JOUE L 119, 4 mai 2016.

Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 (DSA), JOUE L 277, 27 octobre 2022.

Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (AI Act), JOUE, 12 juillet 2024.

Règlement (UE) 2026/1744 modifiant le règlement (UE) 2024/1689 (Omnibus numérique sur l'IA), JOUE, 24 juillet 2026.

OCDE, *Recommandation du Conseil sur l'intelligence artificielle*, 22 mai 2019.

UNESCO, *Recommandation sur l'éthique de l'intelligence artificielle*, 23 novembre 2021.

Textes français et jurisprudence

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.

Loi n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre.

Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique.

Cons. const., décision n° 2018-765 DC du 12 juin 2018, Loi relative à la protection des données personnelles.

CJUE, 7 décembre 2023, *SCHUFA Holding (Scoring)*, aff. C-634/21, EU:C:2023:957.

Textes marocains

Dahir formant Code des obligations et des contrats du 9 ramadan 1331 (12 août 1913).

Loi n° 07-03 complétant le Code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données (dahir n° 1-03-197 du 16 ramadan 1424, 11 novembre 2003).

Loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (dahir n° 1-09-15 du 22 safar 1430, 18 février 2009).

Loi n° 05-20 relative à la cybersécurité (dahir n° 1-20-69 du 4 hija 1441, 25 juillet 2020) et décret n° 2-21-406 pris pour son application.

Loi n° 43-20 relative aux services de confiance pour les transactions électroniques (dahir n° 1-20-100 du 16 journada I 1442, 31 décembre 2020).

Loi n° 53-05 relative à l'échange électronique de données juridiques (dahir n° 1-07-129 du 19 kaada 1428, 30 novembre 2007).

Ouvrages et articles

Baldwin R., Cave M. et Lodge M., *Understanding Regulation: Theory, Strategy, and Practice*, 2e éd., Oxford, Oxford University Press, 2012.

Beck U., *La société du risque. Sur la voie d'une autre modernité*, trad. L. Bernardi, Paris, Aubier, 2001.

Black J., « The Emergence of Risk-Based Regulation and the New Public Risk Management in the United Kingdom », *Public Law*, 2005, p. 512 et s.

Black J. et Baldwin R., « Really Responsive Risk-Based Regulation », *Law & Policy*, vol. 32, n° 2, 2010, p. 181-213.

Bradford A., *The Brussels Effect: How the European Union Rules the World*, Oxford, Oxford University Press, 2020.

Delmas-Marty M., *Résister, responsabiliser, anticiper*, Paris, Seuil, 2013.

Ewald F., « Philosophie de la précaution », *L'Année sociologique*, vol. 46, n° 2, 1996, p. 383 et s.

Floridi L., « The European Legislation on AI: A Brief Analysis of Its Philosophical Approach », *Philosophy & Technology*, vol. 34, 2021, p. 215-222.

Frison-Roche M.-A. (dir.), *Régulation, supervision, compliance*, Paris, Dalloz, 2017.

Haounani A., « L'intelligence artificielle au Maroc : entre éthique et réglementation », *Afkar/Idées*, automne-hiver 2024.

Jonas H., *Le principe responsabilité. Une éthique pour la civilisation technologique*, trad. J. Greisch, Paris, Cerf, 1990.

Novelli C., Casolari F., Rotolo A., Taddeo M. et Floridi L., « AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act », *Digital Society*, vol. 3, 2024.

Veale M. et Zuiderveen Borgesius F., « Demystifying the Draft EU Artificial Intelligence Act », *Computer Law Review International*, vol. 22, n° 4, 2021, p. 97-112.

Zweigert K. et Kötz H., *Introduction to Comparative Law*, 3e éd., Oxford, Clarendon Press, 1998.

Documents institutionnels et sources de presse

ANSSI, *EBIOS Risk Manager. Le guide*, 2018.

CNIL, *Intelligence artificielle : le plan d'action de la CNIL*, 16 mai 2023.

Commission européenne, *Livre blanc sur l'intelligence artificielle. Une approche européenne axée sur l'excellence et la confiance*, COM(2020) 65 final, 19 février 2020.

Commission européenne, Proposition de règlement établissant des règles harmonisées concernant l'intelligence artificielle, COM(2021) 206 final, 21 avril 2021.

Commission spéciale sur le modèle de développement, *Le nouveau modèle de développement*, Rabat, avril 2021.

Groupe d'experts de haut niveau sur l'intelligence artificielle, *Lignes directrices en matière d'éthique pour une IA digne de confiance*, 8 avril 2019.

Hespress, « L'IA au Maroc : un développement rapide, un encadrement juridique absent », 23 juin 2025.

Le360, « Amal El Fallah Seghrouchni : Le Maroc prépare un cadre légal et une direction générale dédiés à l'IA ».

Lokmane-Khelil S., « Le Maroc va créer une direction générale de l'intelligence artificielle », *Acteurs publics*, 20 octobre 2025.

TelQuel, hors-série n° 1175 consacré à la CNDP, 10-16 avril 2026.