International Journal of Economic Studies and Management (IJESM)
ISSN 2789-049X
Int. J. Econ. Stud. Manag. 5, No.6 (NOVEMBER-2025)

Vers une intelligence artificielle régulée : innovations et défis dans la lutte contre la criminalité financière

Toward a regulated artificial intelligence: innovations and challenges in the fight against financial crime

Soumia CHIHAB
Laboratoire de Recherche en Management des Organisations (LAREMO)
L'Ecole Supérieure de Technologie de Casablanca (ESTC)
Université Hassan II – Casablanca – Maroc

Fairouz AMMI AL MASBAHI
Laboratoire de Recherche en Management des Organisations (LAREMO)
L'Ecole Supérieure de Technologie de Casablanca (ESTC)
Université Hassan II – Casablanca - Maroc

Résumé : Cet article analyse l'intégration croissante de l'intelligence artificielle (IA) dans la lutte contre la criminalité financière à l'ère de la digitalisation. En effet ; les nouvelles technologies renforcent la capacité des institutions à détecter et prévenir les comportements frauduleux. Toutefois, ces innovations soulèvent des enjeux éthiques et juridiques majeurs, notamment les biais algorithmiques, l'opacité des modèles et la responsabilité limitée des acteurs humains.
À l'échelle internationale, l'OCDE, le GAFI, l'Union européenne et le FMI œuvrent à établir un cadre normatif commun, fondé sur la transparence et la coopération, illustré par le pacte européen lié à l'intelligence artificielle (AI Act) et les recommandations du GAFI. Au Maroc, des organismes comme Bank Al-Maghreb, l'AMMC et la CNDP adoptent une approche prudente de l'IA dans la supervision financière, en veillant à la protection des données et à l'éthique. En effet, la réussite de cette transformation repose sur un équilibre entre innovation technologique et gouvernance correcte et éthique humaine, condition essentielle à une IA responsable, inclusive et durable.
Mots-clés : Intelligence Artificielle, Criminalité Financière, Régulation Ethique, Gouvernance Algorithmique.

Abstract: This article examines the growing role of artificial intelligence (AI) in combating financial crime in an era of digitalized economic flows and increasingly complex illicit practices. In fact, technologies such as Machine Learning, Deep Learning, and predictive analytics enhance institutions' ability to detect and prevent fraudulent behavior. However, these innovations also raise major ethical and legal concerns, including algorithmic bias, model opacity, and the dilution of human accountability.
At the international level, organizations such as the OECD, FATF, the European Union, and the IMF are working to establish a common regulatory framework based on transparency, proportionality, and cooperation, illustrated by the EU AI Act and FATF recommendations. In Morocco, institutions like Bank Al-Maghreb, the AMMC, and the CNDP have adopted a cautious approach to integrating AI into financial supervision, emphasizing data protection and ethics. The study concludes that the effectiveness of this transformation depends on maintaining a balance between technological innovation and human governance — a prerequisite for building a responsible, inclusive, and sustainable AI ecosystem.
Keywords: Artificial Intelligence, Financial Crime, Ethical regulation, Algorithmic Governance.

Digital Object Identifier (DOI): https://doi.org/10.5281/zenodo.**17578885**

1. Introduction

La criminalité financière constitue aujourd'hui un phénomène d'une complexité croissante et d'une portée mondiale préoccupante. L'essor de la digitalisation des échanges économiques et l'intensification de la mondialisation des flux financiers ont profondément transformé la nature des activités illicites. Celles-ci ne se limitent plus à des fraudes occasionnelles, mais s'organisent autour de dispositifs complexes de blanchiment de capitaux, de corruption, de manipulation de marchés, de financement du terrorisme ou encore de détournement de fonds. Par leur caractère transnational et polymorphe, ces pratiques érodent la confiance dans les institutions financières, menacent la stabilité macroéconomique et accentuent les déséquilibres sociaux. D'après les estimations du Fonds monétaire international, la criminalité financière représenterait plus de 2,5 % du produit intérieur brut mondial, soit des milliers de milliards de dollars détournés chaque année — une proportion révélatrice de l'incapacité des mécanismes de contrôle classiques à suivre le rythme de la sophistication technologique actuelle des systèmes financiers.

Dans ce contexte, les autorités de régulation, les instances internationales et les acteurs bancaires sont confrontés à une double exigence : d'une part, assurer une surveillance rigoureuse et continue des opérations dans un environnement globalisé et interconnecté ; d'autre part, se conformer à des normes toujours plus strictes en matière de transparence, de conformité et de protection des données. Les dispositifs traditionnels, fondés sur des règles prédéterminées, des contrôles humains ou des analyses statistiques standards, se révèlent désormais inadaptés pour détecter les comportements déviants dissimulés dans la masse des transactions légitimes. Dans cette dynamique, l'intelligence artificielle (IA) émerge comme un levier de transformation incontournable pour renforcer la sécurité et la résilience du système financier. En mobilisant des algorithmes d'apprentissage capables d'évoluer et d'identifier des corrélations imperceptibles à l'analyse humaine, l'IA ouvre la voie à une détection plus rapide, adaptative et prédictive des activités criminelles.

Les progrès de l'apprentissage automatique, du *deep learning* et de l'analyse prédictive ont profondément transformé les pratiques de surveillance et de conformité. Les institutions financières exploitent désormais des modèles capables d'analyser en temps réel des flux massifs de données – historiques bancaires, transactions électroniques, comportements clients, communications internes – afin d'identifier des signaux faibles susceptibles de révéler une activité illégale. Des solutions telles que *SAS Fraud Management*, *IBM Watson* ou *FICO Falcon Platform* ont démontré leur efficacité dans la détection de transactions suspectes ou de comportements anormaux, réduisant significativement les pertes liées à la fraude. L'OCDE et le Groupe d'action financière (GAFI) encouragent d'ailleurs l'intégration de ces technologies dans les dispositifs de lutte contre le blanchiment et le financement du terrorisme, estimant qu'elles peuvent accroître la résilience et la transparence du système financier global.

Cependant, cette promesse technologique ne saurait occulter les risques considérables qu'elle soulève. L'intelligence artificielle, utilisée sans cadre éthique ni supervision humaine suffisante, peut reproduire ou amplifier des biais discriminatoires, générer des faux positifs coûteux ou compromettre la confidentialité des données. La complexité des algorithmes, souvent qualifiés de « boîtes noires », rend difficile la compréhension et la justification des décisions automatisées. Dans un domaine aussi sensible que la surveillance financière, où les décisions peuvent affecter la réputation d'individus ou d'entreprises, cette opacité pose un défi majeur à la responsabilité et à la légitimité des institutions utilisatrices. Comme le souligne l'OCDE dans son rapport sur la gouvernance algorithmique (2021), la performance technique ne saurait remplacer la transparence, la redevabilité et la supervision humaine. C'est pourquoi la question d'une **intelligence artificielle régulée** se trouve désormais au cœur du débat international.

Les instances européennes et mondiales s'efforcent de définir un cadre normatif adapté à cette nouvelle réalité. Le projet de règlement européen sur l'intelligence artificielle (AI Act) introduit la notion de « systèmes à haut risque » et impose des obligations strictes en matière de traçabilité et de contrôle humain. De son côté, le GAFI recommande une approche dite de « proportionnalité technologique », visant à concilier innovation et conformité. Le FMI et la Banque mondiale insistent quant à eux sur la nécessité d'une gouvernance algorithmique globale, articulant coopération interinstitutionnelle et partage sécurisé des données. Ces orientations témoignent d'une volonté commune : faire de l'intelligence artificielle non pas une source d'instabilité, mais un pilier d'une finance plus éthique, transparente et durable.

D'un point de vue scientifique, l'étude de la relation entre IA et criminalité financière s'inscrit dans une perspective interdisciplinaire, à la croisée de la finance, de la criminologie, de la gouvernance numérique et de l'éthique des technologies. Elle interroge à la fois les conditions d'efficacité des systèmes algorithmiques et leurs implications normatives. Comment garantir que les modèles d'apprentissage automatique identifient correctement les comportements frauduleux sans stigmatiser certains profils ? Comment assurer la responsabilité des décisions prises par des systèmes autonomes ? Et surtout, comment encadrer juridiquement des outils dont la logique interne échappe souvent à la compréhension humaine ? Ces questions illustrent les tensions croissantes entre efficacité technologique, protection des droits fondamentaux et impératifs de régulation internationale.

Ainsi, la problématique centrale de cette recherche peut être formulée comme suit :

Dans quelle mesure l'intelligence artificielle peut-elle contribuer efficacement à la lutte contre la criminalité financière tout en respectant les principes d'éthique, de transparence et de responsabilité définis par les cadres internationaux tels que l'OCDE, le GAFI, l'Union européenne et le FMI ?

Cette interrogation conduit à examiner à la fois les innovations technologiques et les contraintes de régulation qu'elles engendrent. L'objectif n'est pas uniquement de mesurer la performance des outils

d'IA, mais d'analyser leur intégration dans une architecture de gouvernance mondiale où les impératifs de conformité, d'équité et de sécurité doivent primer sur la seule efficacité algorithmique.
Ce travail s'inscrit dans une logique d'équilibre : comprendre comment l'IA, loin de se substituer à l'expertise humaine, peut en devenir le prolongement régulé. L'étude mobilise des références issues de la littérature académique et institutionnelle, tout en mettant en lumière les initiatives internationales les plus récentes. Elle vise à démontrer que l'intelligence artificielle, lorsqu'elle est pensée comme un instrument de gouvernance responsable, peut devenir un levier majeur dans la prévention et la maîtrise de la criminalité financière. Mais cette ambition suppose une vigilance constante : celle de construire une intelligence artificielle non seulement performante, mais également juste, explicable et conforme aux valeurs fondamentales de la gouvernance mondiale.

- ✓ **Démarche méthodologique**

Cette étude repose sur une démarche qualitative et documentaire. Elle s'appuie sur une analyse de contenu de rapports institutionnels (OCDE, GAFI, FMI, Union européenne, Bank Al-Maghreb, AMMC, CNDP) et d'articles scientifiques récents portant sur l'application de l'IA à la détection de la fraude. La méthode combine une lecture thématique et comparative visant à dégager les convergences entre innovation technologique et gouvernance éthique. Cette approche s'inscrit dans une logique exploratoire et interdisciplinaire, à la croisée de la finance, du droit et de la sociologie des organisations.

2. Cadre conceptuel et théorique : criminalité financière et intelligence artificielle

2.1. Notion de la Criminalité Financière

La criminalité financière est une notion à multiples dimensions qui dépasse largement la simple idée de fraude économique. Elle englobe l'ensemble des comportements illégaux visant à obtenir un gain pécuniaire indu, au détriment de la confiance publique, de la stabilité des marchés ou du bon fonctionnement des échanges internationaux. Bien qu'elle ne soit pas un phénomène nouveau, son expansion et sa complexité qui sont actuelles sont directement liées à la mondialisation des flux financiers et à la numérisation croissante des opérations économiques. La virtualisation des transactions, la circulation instantanée des capitaux et le recours massif aux technologies numériques ont favorisé la mise en place de mécanismes de dissimulation toujours plus sophistiqués. Ces évolutions ont profondément transformé la nature même de la criminalité financière, qui se déploie désormais dans un espace virtuel mondialisé échappant en partie aux cadres traditionnels de contrôle et de régulation.

Dans les travaux académiques et institutionnels, la criminalité financière est généralement analysée à travers plusieurs typologies d'infractions économiques. Parmi les plus récurrentes figurent le

blanchiment d'argent, la corruption, la manipulation de marchés, l'évasion fiscale, le financement du terrorisme ou encore les délits d'initiés. Malgré leur diversité, ces pratiques partagent un fondement commun : elles tirent parti des fragilités structurelles du système financier international, des déséquilibres informationnels et des disparités normatives entre États. Comme le rappelle le Groupe d'action financière (GAFI, 2021), ces formes de délinquance reposent sur des réseaux transnationaux organisés qui utilisent des structures écrans, des intermédiaires spécialisés et des juridictions à fiscalité avantageuse pour dissimuler l'origine et la destination réelles des capitaux.

Les grandes institutions internationales, telles que le Fonds monétaire international (FMI) et l'Organisation de coopération et de développement économiques (OCDE), reconnaissent la criminalité financière comme une menace majeure pour la stabilité de l'économie mondiale. Le FMI considère qu'elle perturbe le fonctionnement du système monétaire, détourne les ressources publiques essentielles et fausse les mécanismes de concurrence en créant des déséquilibres structurels sur les marchés. L'OCDE, pour sa part, met en évidence la corrélation étroite entre criminalité financière et corruption systémique, en soulignant que la circulation non régulée de capitaux illicites mine la confiance dans les institutions démocratiques et compromet un développement économique équitable. De ce fait, la lutte contre la criminalité financière dépasse la simple exigence de conformité réglementaire : elle s'inscrit dans une logique plus large de gouvernance économique internationale, fondée sur les principes de transparence, de responsabilité et de justice financière.

Sur le plan théorique, plusieurs approches issues des sciences sociales et économiques ont tenté d'éclairer les mécanismes qui sous-tendent la criminalité financière. Selon la théorie du choix rationnel (Becker, 1968), les individus évaluent les bénéfices potentiels et les risques encourus avant de s'engager dans une activité illégale. Appliquée au secteur financier, cette approche suggère que la criminalité économique découle d'une logique utilitariste : les auteurs exploitent les failles normatives ou technologiques lorsqu'ils jugent le risque de sanction faible. D'autres perspectives, telles que la théorie de l'anomie (Merton, 1938) ou celle de la culture organisationnelle déviante (Vaughan, 1999), insistent sur le rôle des dynamiques sociales et institutionnelles dans la genèse des comportements illicites. Dans un contexte fortement concurrentiel, la pression à la rentabilité, la valorisation de la performance à court terme et la complexité des structures organisationnelles peuvent conduire à une normalisation, voire à une acceptation tacite, des pratiques contraires à l'éthique.

Ces analyses convergent vers une idée essentielle : la criminalité financière est un phénomène systémique qui ne peut être appréhendé uniquement sous un angle juridique. Elle mobilise des savoirs diversifiés tels que : techniques, comptables, informatiques et fiscaux que les auteurs de crimes détournent à leur profit. Dans cette perspective, l'intelligence artificielle se présente à la fois comme un outil de maîtrise et comme un nouvel espace de risque. D'un côté, elle permet de renforcer les

capacités d'analyse et de détection des comportements atypiques et anormaux ; d'un autre, elle peut être instrumentalisée à des fins frauduleuses, notamment dans la falsification de documents ou d'identités ou la dissimulation automatisée des flux ; les scénarios effectivement sont nombreux. L'usage de technologies d'apprentissage pour contourner les systèmes de surveillance montre que la frontière entre innovation et exploitation déviante demeure fragile.

2.2. L'Intelligence Artificielle

L'intelligence artificielle, par sa définition la plus connue, regroupe l'ensemble des procédés et algorithmes conçus pour permettre aux machines de reproduire certaines capacités cognitives humaines, telles que l'analyse, la compréhension, l'apprentissage et la prise de décision autonome. Dans le secteur financier, elle se concrétise principalement à travers des technologies comme l'apprentissage automatique (*Machine Learning*), l'apprentissage profond (Deep Learning), le traitement automatique du langage naturel (*Natural Language Processing*, ou NLP) et les techniques d'analyse prédictive. Ces outils offrent la possibilité d'extraire des tendances pertinentes à partir de volumes massifs de données et de repérer des comportements atypiques sans intervention humaine directe. Ainsi, les modèles d'apprentissage supervisé sont formés à partir de jeux de données étiquetées afin de distinguer les opérations légitimes de celles potentiellement frauduleuses, tandis que les modèles non supervisés exploitent des méthodes de regroupement statistique ou de mesure de similarité pour identifier des anomalies au sein des transactions financières.

Le recours à ces technologies s'est accéléré dans le secteur financier à partir du début des années 2010, parallèlement à la croissance exponentielle des volumes de données disponibles et à la baisse des coûts de calcul. Les institutions bancaires et les entreprises de services financiers se sont progressivement dotées de systèmes d'analyse automatisée capables de repérer en temps réel des signaux faibles. Les solutions développées par des acteurs tels que SAS Institute, IBM Watson ou FICO reposent sur des architectures hybrides combinant règles expertes, modèles prédictifs et apprentissage en continu. Ces dispositifs s'inscrivent dans une logique d'intelligence adaptative, où les algorithmes ajustent leurs paramètres à mesure que de nouvelles formes de criminalité émergent, à travers la formulation de différents scénarios et d'indicateurs, afin de détecter les opérations et comportements douteux. Cette dynamique correspond à la vision promue par le GAFI et l'OCDE, qui encouragent l'adoption de technologies dites "responsables", c'est-à-dire capables d'apprendre sans compromettre les principes de transparence et de proportionnalité.

Toutefois, l'intégration de l'intelligence artificielle dans les dispositifs de lutte contre la criminalité financière ne relève pas d'une simple évolution technique ; elle traduit un changement de paradigme dans la manière dont la gouvernance financière conçoit la prévention et la régulation. Les systèmes fondés sur l'IA déplacent le centre de gravité du contrôle : ils ne se contentent plus de vérifier la conformité a posteriori, mais cherchent à anticiper les comportements suspects avant qu'ils ne se

produisent. Ce passage d'une logique réactive à une logique prédictive constitue un tournant majeur dans la politique de surveillance financière mondiale. Il permet une meilleure allocation des ressources, une réduction des pertes et une amélioration de la rapidité des interventions, mais il modifie également la répartition des responsabilités entre les acteurs humains et les machines. Qui doit être tenu pour responsable lorsqu'un algorithme se trompe, ou lorsqu'il échoue à signaler une opération illicite ? Cette question, au cœur des débats contemporains sur la gouvernance de l'IA, souligne la nécessité d'un encadrement normatif rigoureux et d'une supervision humaine permanente.

Les travaux récents sur la gouvernance algorithmique (OCDE, 2021 ; Commission européenne, 2021) insistent sur la nécessité d'une approche équilibrée combinant innovation et régulation. L'intelligence artificielle ne doit pas être perçue uniquement comme un instrument de performance, mais comme une composante intégrée d'un écosystème éthique et juridique. Le FMI, dans son rapport de 2023 sur l'intégrité financière, plaide pour une "régulation intelligente" capable de favoriser la compétitivité tout en minimisant les risques systémiques. Cette approche repose sur trois piliers : la transparence des modèles, la responsabilité institutionnelle et la coopération internationale. L'Union européenne, à travers son futur AI Act, entend établir des standards contraignants pour garantir que les systèmes utilisés dans les domaines à haut risque — dont la finance — respectent des exigences strictes en matière de fiabilité et de supervision humaine.

Ce cadre conceptuel met en évidence une tension fondamentale entre deux logiques : la recherche d'efficacité opérationnelle et la préservation des valeurs éthiques et juridiques qui fondent la confiance dans le système financier. L'intelligence artificielle peut renforcer la lutte contre la criminalité financière à condition d'être utilisée dans un cadre régulé, transparent et coordonné à l'échelle internationale. Elle ne saurait se substituer à la responsabilité humaine ni à la vigilance institutionnelle, mais doit s'y adosser. La compréhension de cette articulation entre technologie et gouvernance constitue la clé de lecture du présent travail, qui s'attache à examiner comment les innovations en matière d'IA transforment les stratégies de détection et de prévention, tout en redéfinissant les frontières de la responsabilité dans la gouvernance financière mondiale.

2.3. Innovations technologiques et apports de l'intelligence artificielle dans la lutte contre la criminalité financière

L'émergence de l'intelligence artificielle au sein des dispositifs financiers marque une rupture profonde dans la manière dont les institutions perçoivent, anticipent et traitent la criminalité économique. Longtemps cantonnée à des approches statistiques ou à des règles de conformité rigides, la lutte contre la criminalité financière a connu, au cours de la dernière décennie, une véritable révolution technologique. Les progrès de l'apprentissage automatique, du traitement du langage naturel et de l'analyse prédictive ont permis de transformer la détection a posteriori des délits financiers en une surveillance proactive, capable d'identifier des comportements suspects avant même

qu'ils ne produisent leurs effets dommageables. Cette transformation s'inscrit dans un contexte d'hyper complexité, où la rapidité des flux et la multiplicité des acteurs exigent une vigilance continue et adaptative.

L'intelligence artificielle occupe désormais une place centrale dans les stratégies de gouvernance des risques. Dans le secteur bancaire, elle permet d'automatiser la surveillance de millions de transactions quotidiennes, d'identifier des anomalies comportementales et de croiser des données internes et externes afin d'évaluer le risque global associé à un client, un fournisseur ou une institution partenaire. Cette capacité d'analyse à grande échelle constitue une réponse directe aux limites structurelles des approches traditionnelles. Les modèles fondés sur des règles fixes ou des contrôles humains reposaient sur une logique de détection séquentielle, lente et coûteuse, souvent inefficace face à des montages sophistiqués et évolutifs. En revanche, les systèmes d'intelligence artificielle sont capables d'apprendre en continu, de reconnaître des schémas récurrents et d'ajuster leurs prédictions au fur et à mesure que de nouvelles formes de criminalité apparaissent.

Les premières générations d'algorithmes utilisés pour la détection de fraude financière reposaient sur des techniques d'apprentissage supervisé, où les modèles étaient entraînés à partir de données historiques annotées comme frauduleuses ou non. Ces approches, bien qu'efficaces pour des fraudes répétitives, montraient leurs limites dès qu'il s'agissait de schémas inédits ou de délits émergents. C'est pourquoi les institutions se sont progressivement tournées vers des approches plus flexibles : apprentissage non supervisé, apprentissage semi-supervisé et deep learning. Ces technologies offrent la possibilité d'extraire des structures cachées dans les données et de détecter des anomalies sans dépendre d'étiquettes préalables. Elles s'avèrent particulièrement pertinentes pour la criminalité financière, où les comportements suspects sont rares, variables et difficilement généralisables.

Les applications concrètes de l'intelligence artificielle dans la lutte contre la criminalité financière sont aujourd'hui multiples et diversifiées. Dans la surveillance des transactions, les algorithmes de type machine learning sont utilisés pour repérer des transferts inhabituels en fonction du profil du client, du pays d'origine des fonds ou du réseau d'intermédiaires impliqués. Dans le domaine du blanchiment d'argent, les modèles d'analyse de graphes et de réseaux neuronaux permettent de cartographier les relations entre entités et de détecter des structures de transfert complexes souvent invisibles aux auditeurs humains. Par ailleurs, le traitement automatique du langage naturel (TALN) est mobilisé pour analyser des communications textuelles — contrats, courriels, documents juridiques — et y repérer des signaux faibles d'inconduite, de collusion ou de manipulation de marché. Ces approches, combinées à l'analyse comportementale et au Scoring de risque, renforcent considérablement la capacité des institutions à identifier des menaces émergentes avant qu'elles ne deviennent systémiques.

Sur le plan opérationnel, les grandes entreprises de technologies financières ont développé des plateformes d'analyse prédictive intégrant des modules d'intelligence artificielle hautement performants. Parmi les solutions les plus répandues figurent SAS Fraud Management, FICO Falcon

Platform et IBM Watson AI for Risk & Compliance. Ces systèmes reposent sur des architectures hybrides qui associent modèles statistiques, réseaux neuronaux et règles métier personnalisées. La plateforme SAS, par exemple, est capable de surveiller plusieurs millions de transactions en temps réel tout en adaptant ses seuils de détection aux comportements historiques des utilisateurs. FICO Falcon, utilisée par des institutions comme Barclays, BNP Paribas ou Wells Fargo, s'appuie sur des réseaux neuronaux adaptatifs qui mettent à jour automatiquement les profils de risque. IBM Watson, quant à lui, va au-delà de la détection transactionnelle pour intégrer des fonctions d'analyse cognitive et de conformité réglementaire, grâce à un traitement avancé du langage naturel. Ces solutions constituent des références mondiales dans la lutte contre les crimes financiers, tant par leur efficacité que par leur capacité d'intégration dans les environnements réglementés.

Cette sophistication technologique répond à une exigence majeure : traiter le volume colossal de données financières générées chaque jour. Les systèmes de paiement internationaux, les plateformes de crypto actifs, les marchés de capitaux et les réseaux de transfert électronique produisent une quantité d'informations impossible à analyser manuellement. L'OCDE souligne que la valeur des flux de données transfrontaliers a dépassé celle du commerce mondial de biens physiques dès 2019, transformant la donnée en matière première de la gouvernance économique. Dans ce contexte, l'intelligence artificielle devient indispensable pour extraire du sens, détecter des patterns et identifier les interactions suspectes au sein de réseaux mondiaux interconnectés. Le FMI rappelle d'ailleurs que l'efficacité des dispositifs de lutte contre la criminalité financière dépend désormais de la capacité des institutions à "intégrer l'analyse algorithmique dans leurs fonctions de supervision et de conformité".

Cependant, ces avancées ne vont pas sans limites ni risques. L'un des principaux défis réside dans la qualité et la fiabilité des données utilisées pour entraîner les modèles. Les biais présents dans les jeux de données historiques peuvent se répercuter sur les prédictions, entraînant une discrimination involontaire ou une surveillance excessive de certains profils ou régions. Le phénomène du concept drift, c'est-à-dire la modification progressive des schémas de fraude au fil du temps, réduit également la pertinence des modèles statiques. Une solution consiste à recourir à l'apprentissage en ligne (online learning), qui permet d'actualiser les algorithmes au fur et à mesure de l'arrivée de nouvelles données, sans nécessiter un réentraînement complet. Cette approche dynamique est aujourd'hui encouragée par les régulateurs, car elle garantit une meilleure adaptation aux comportements changeants des acteurs financiers.

L'essor des crypto actifs et des technologies blockchain constitue un autre champ d'expérimentation pour l'intelligence artificielle. Si ces technologies offrent un haut niveau de traçabilité, elles peuvent également être utilisées à des fins de dissimulation ou de contournement réglementaire. Les outils d'IA sont alors mobilisés pour analyser les transactions sur chaînes publiques et détecter des flux suspects en lien avec des plateformes non réglementées. Des entreprises spécialisées, telles que *Chainalysis* ou *Elliptic*, ont développé des modèles d'analyse capables d'associer des adresses virtuelles à des entités réelles, facilitant ainsi les enquêtes sur le blanchiment ou le financement du

terrorisme. Ces applications démontrent le potentiel de l'IA pour renforcer la transparence dans des environnements décentralisés, tout en illustrant la nécessité d'une coopération internationale dans le partage de données et de méthodes d'analyse.

Sur le plan macroéconomique, l'intégration de l'intelligence artificielle dans les politiques publiques de lutte contre la criminalité financière ouvre la voie à de nouvelles formes de gouvernance algorithmique. L'Union européenne, à travers son Digital Finance Package et le futur AI Act, promeut une utilisation "responsable et régulée" de l'IA dans le secteur financier. L'objectif est double : exploiter les bénéfices de l'innovation tout en préservant la sécurité juridique et la confiance du public. De même, le GAFI encourage les États membres à intégrer des solutions technologiques avancées dans leurs dispositifs nationaux de lutte contre le blanchiment et le financement du terrorisme, mais insiste sur le maintien d'un contrôle humain et institutionnel permanent. Le FMI, enfin, plaide pour une harmonisation des standards internationaux, estimant que la fragmentation des cadres réglementaires crée des zones d'ombre propices aux dérives et à l'arbitrage réglementaire.

Il apparaît ainsi que l'intelligence artificielle n'est plus simplement un outil technique, mais un levier stratégique de transformation de la gouvernance financière. Elle redéfinit les rapports entre acteurs, modifie les circuits de décision et déplace la frontière entre prévention et intervention. L'enjeu n'est plus seulement de détecter les crimes financiers, mais d'anticiper leurs mécanismes, de comprendre leurs dynamiques et d'en neutraliser les effets avant qu'ils ne deviennent systémiques. En ce sens, l'IA représente un changement de paradigme dans la lutte contre la criminalité économique : elle introduit une logique prédictive et adaptative au cœur même des systèmes de régulation. Mais pour que cette transformation soit durable, elle doit s'inscrire dans un cadre de gouvernance clair, où la performance technologique s'accompagne de garanties éthiques et juridiques solides. C'est dans cette perspective que s'impose la notion d'"intelligence artificielle régulée", conciliant innovation, responsabilité et transparence, condition sine qua non d'une finance mondiale plus intègre et plus résiliente.

3. Les défis d'une intelligence artificielle régulée : responsabilité et perspectives

3.1. Les obstacles rencontrés

Si l'intelligence artificielle constitue un formidable levier d'innovation pour renforcer la sécurité et la transparence du système financier mondial, elle suscite également des inquiétudes profondes quant à ses effets collatéraux sur la gouvernance, la responsabilité et la protection des droits fondamentaux. L'automatisation croissante de la détection des comportements frauduleux repose sur des modèles algorithmiques dont la complexité dépasse souvent la compréhension humaine. Cette situation engendre un paradoxe majeur : plus les systèmes deviennent performants, plus ils deviennent opaques. Or, dans des domaines aussi sensibles que la surveillance financière, cette opacité entre en tension directe avec les exigences de transparence et de redevabilité imposées par les régulateurs internationaux.

L'un des premiers défis identifiés est celui des biais algorithmiques. Ces biais ne sont pas seulement d'ordre technique ; ils traduisent souvent des asymétries sociales et économiques déjà présentes dans les données utilisées pour l'entraînement des modèles. Les jeux de données historiques contiennent des traces de décisions humaines, de contextes géographiques ou de régulations inégales qui, lorsqu'ils sont reproduits par des algorithmes, peuvent engendrer une discrimination involontaire. Par exemple, un modèle d'IA entraîné à partir de données provenant majoritairement de pays développés pourrait surévaluer le risque de certaines transactions issues de régions émergentes, interprétant des comportements commerciaux légitimes comme suspects. Ce phénomène, souligné par l'OCDE dans son rapport sur la gouvernance algorithmique (2021), illustre la nécessité de concevoir des modèles plus inclusifs, capables d'intégrer la diversité des contextes économiques et culturels.

Les biais algorithmiques soulèvent également la question de la proportionnalité dans la surveillance financière. Le GAFI, dans ses recommandations de 2021, rappelle que l'utilisation des technologies d'intelligence artificielle pour la lutte contre le blanchiment de capitaux et le financement du terrorisme doit respecter le principe de proportionnalité entre les risques identifiés et les mesures déployées. Une approche trop intrusive ou fondée sur des corrélations statistiques mal interprétées pourrait conduire à une sur-surveillance injustifiée, compromettant la confiance des citoyens et des entreprises dans le système financier. Ce risque est d'autant plus préoccupant que les institutions financières tendent à déléguer de plus en plus leurs processus de vigilance à des systèmes automatisés, parfois sans disposer des compétences internes nécessaires pour en comprendre le fonctionnement.

Un second défi majeur réside dans la transparence des modèles. La plupart des algorithmes de deep learning fonctionnent comme des « boîtes noires », produisant des résultats sans fournir d'explications claires sur le raisonnement qui y conduit. Dans le cadre de la lutte contre la criminalité financière, cette opacité pose un problème de légitimité : comment justifier qu'une transaction, une entreprise ou un individu fasse l'objet d'une alerte si le mécanisme décisionnel de l'algorithme est lui-même incompréhensible ? L'Union européenne, à travers le projet de règlement sur l'intelligence artificielle (AI Act), tente de répondre à cette problématique en imposant aux concepteurs d'algorithmes à haut risque des exigences strictes en matière de traçabilité et d'audit. L'objectif est de garantir un niveau de transparence suffisant pour permettre aux autorités de contrôle d'examiner les décisions automatisées, d'en évaluer la cohérence et, le cas échéant, d'en corriger les dérives.

L'explication n'est cependant pas qu'une contrainte réglementaire : elle constitue aussi un impératif éthique. Le principe de *fair accountability* défendu par le FMI (2023) repose sur l'idée que toute décision automatisée doit pouvoir être comprise et justifiée, non seulement devant les régulateurs, mais aussi devant les citoyens et les acteurs économiques concernés. Cette exigence renvoie à la notion d'intelligence artificielle explicable (XAI), champ de recherche en plein essor qui vise à concevoir des modèles capables de rendre intelligibles leurs processus internes. Les techniques d'interprétation, telles que SHAP (*Shapley Additive Explanations*) ou LIME (*Local Interpretable Model-Agnostic Explanations*), permettent d'attribuer un poids explicatif à chaque variable influençant

la décision de l'algorithme. Dans le domaine financier, ces outils offrent une meilleure visibilité sur les critères utilisés pour détecter une opération suspecte, renforçant ainsi la confiance entre les parties prenantes.

Au-delà des biais et de l'opacité, la question de la responsabilité juridique constitue un enjeu central. L'utilisation de systèmes autonomes pour la détection de la criminalité financière soulève une interrogation fondamentale : qui est responsable en cas d'erreur, de négligence ou de dommage ? Est-ce le concepteur de l'algorithme, l'institution financière qui l'utilise, ou l'autorité de supervision qui l'a validé ? Cette indétermination fragilise la gouvernance de l'IA et risque de créer des zones d'irresponsabilité. Pour y remédier, plusieurs cadres normatifs internationaux s'efforcent de clarifier les lignes de responsabilité. L'Union européenne, par exemple, prévoit dans son AI Liability Directive une présomption de responsabilité pour les opérateurs de systèmes à haut risque. De son côté, l'OCDE plaide pour un modèle de responsabilité partagée, fondé sur la coopération entre concepteurs, utilisateurs et régulateurs, afin de garantir un contrôle continu tout au long du cycle de vie de l'algorithme.

Ces débats prennent une dimension particulière dans la lutte contre la criminalité financière, où une mauvaise décision peut avoir des conséquences considérables : blocage de comptes légitimes, atteinte à la réputation d'entreprises innocentes, ou au contraire, non-détection d'opérations illicites de grande ampleur. Le FMI souligne que le transfert excessif de responsabilité vers les systèmes automatisés risque d'entraîner une forme de « déresponsabilisation institutionnelle », où les acteurs humains s'en remettent aveuglément aux algorithmes. Ce phénomène, qualifié de biais d'automation, peut réduire la vigilance et la capacité critique des analystes. Il appelle à réaffirmer le rôle du jugement humain comme garde-fou essentiel dans l'utilisation de l'intelligence artificielle à des fins de surveillance et de conformité.

Un autre défi majeur concerne la protection des données et la vie privée. L'analyse de vastes ensembles de données transactionnelles implique inévitablement la collecte, le traitement et le croisement d'informations personnelles. Les régulateurs insistent sur la nécessité de concilier cette exigence de surveillance avec les principes fondamentaux de la protection des données. Le Règlement général sur la protection des données (RGPD) de l'Union européenne impose des obligations strictes en matière de consentement, de minimisation et de sécurisation des informations traitées. Dans le cadre des systèmes d'intelligence artificielle, ces principes doivent être renforcés par des mécanismes de *privacy by design*, qui intègrent la protection des données dès la conception de l'algorithme. L'objectif est d'éviter que la lutte contre la criminalité financière ne se transforme en un dispositif de surveillance généralisée, contraire aux droits individuels et à la confiance du public.

Enfin, la fragmentation réglementaire internationale représente un obstacle majeur à la mise en place d'une intelligence artificielle réellement régulée et coordonnée. Alors que l'Union européenne avance vers un cadre juridique unifié, d'autres juridictions, notamment aux États-Unis et en Asie, adoptent des approches plus souples, fondées sur l'autorégulation et l'innovation. Cette disparité crée un risque

d'arbitrage réglementaire, où les acteurs financiers exploitent les différences de cadre pour opérer dans les zones les moins contraignantes. L'OCDE et le GAFI appellent à une harmonisation des standards afin de garantir un niveau minimal de cohérence et d'efficacité. La mise en place de forums de coopération interrégionale, tels que *l'International Platform* on *Sustainable Finance* ou *le Financial Stability Board*, vise précisément à favoriser l'échange de bonnes pratiques et la convergence des régulations.

Face à ces défis, l'équilibre entre innovation et régulation apparaît comme le fil conducteur des politiques publiques et institutionnelles. L'intelligence artificielle ne peut contribuer efficacement à la lutte contre la criminalité financière que si elle repose sur une gouvernance transparente, éthique et responsable. Il s'agit de dépasser la fascination technologique pour inscrire ces outils dans une logique de confiance, où les valeurs fondamentales — équité, justice, dignité et responsabilité — demeurent au cœur de la transformation numérique du secteur financier. La régulation ne doit pas être perçue comme un frein à l'innovation, mais comme une condition de sa durabilité et de sa légitimité.

Ainsi, la construction d'une intelligence artificielle régulée suppose la convergence de trois impératifs : la maîtrise technique, la responsabilité humaine et la coopération internationale. Ce triptyque constitue le socle sur lequel reposera l'efficacité future des dispositifs de lutte contre la criminalité financière. La section suivante examinera précisément comment ces principes se traduisent dans les cadres de gouvernance éthique et réglementaire internationale, en s'appuyant sur les initiatives menées par l'OCDE, l'Union européenne, le GAFI et le FMI.

3.2. Perspectives et orientations futures

L'intégration croissante de l'intelligence artificielle dans les systèmes financiers mondiaux oblige les États à repenser la gouvernance de la technologie, non seulement sous l'angle de la performance économique, mais aussi dans une perspective éthique, sociale et institutionnelle. Le défi consiste désormais à bâtir une intelligence artificielle responsable, c'est-à-dire une IA qui renforce la résilience du système financier sans compromettre la confiance, la transparence ni les droits fondamentaux. Cette orientation s'impose à l'échelle internationale comme au Maroc, où la modernisation du secteur financier s'accompagne d'une volonté affirmée d'encadrer les usages technologiques selon les standards mondiaux.

Sur la scène internationale, les prochaines années seront marquées par la consolidation d'une gouvernance mondiale de l'IA fondée sur la coopération et la convergence réglementaire. L'Union européenne, pionnière en la matière avec son ***AI Act***, entend poser les bases d'un modèle fondé sur la responsabilité, l'audit et la supervision humaine. Ce texte devrait inspirer d'autres juridictions, notamment dans le cadre du Groupe des 20 (G20) et du Fonds monétaire international (FMI), qui plaident pour l'élaboration de cadres communs de gestion du risque algorithmique. L'OCDE, quant à elle, promeut une approche axée sur la transparence et le partage de données sécurisées, afin de favoriser une interopérabilité éthique des systèmes d'intelligence artificielle à travers les marchés. Le

GAFI travaille également à l'adaptation de ses recommandations LBC/FT pour inclure l'usage de technologies d'IA explicable, garantissant la traçabilité des décisions automatisées dans la détection du blanchiment et du financement du terrorisme. Ces initiatives convergent vers une même finalité : bâtir un écosystème global où l'innovation technologique s'accompagne d'une gouvernance prudente, cohérente et équitable.

Mais la réussite d'une telle ambition dépend de la capacité des États à traduire ces principes dans des contextes nationaux spécifiques. Le Maroc s'inscrit progressivement dans cette dynamique. Conscient des mutations numériques et de leurs implications économiques, le Royaume a engagé plusieurs réformes visant à intégrer l'intelligence artificielle dans sa stratégie de développement financier et technologique. La Stratégie nationale de l'intelligence artificielle et de la transformation digitale, portée par le ministère de la Transition numérique, trace les lignes directrices d'un usage éthique et durable des technologies émergentes. Elle met l'accent sur la gouvernance des données, la cyber sécurité et la promotion d'une innovation responsable au service de la transparence économique.

Dans le secteur financier, la Bank Al-Maghreb (BAM) joue un rôle central dans la modernisation de la régulation et l'adoption de solutions d'intelligence artificielle pour la supervision prudentielle. Depuis 2021, la banque centrale a initié plusieurs programmes de veille technologique et d'expérimentation algorithmique afin de renforcer la surveillance des risques bancaires, de détecter plus précocement les anomalies de marché et de prévenir les comportements frauduleux. Ces efforts s'inscrivent dans une logique de *regulatory sandbox* : un cadre expérimental permettant aux institutions financières de tester des innovations technologiques sous la supervision directe du régulateur. Ce dispositif, inspiré des modèles britannique et singapourien, illustre la volonté du Maroc d'articuler innovation et prudence.

L'Autorité marocaine du marché des capitaux (AMMC) a également intégré la dimension technologique dans sa stratégie de régulation. L'AMMC encourage les acteurs de marché à adopter des solutions d'analyse prédictive et de surveillance automatisée des transactions afin de renforcer la lutte contre les délits d'initiés et la manipulation des cours. En 2023, l'Autorité a publié un rapport sur la transformation numérique du marché des capitaux, insistant sur la nécessité d'un cadre éthique pour l'usage de l'intelligence artificielle. Elle préconise la mise en place de comités d'éthique algorithmique au sein des institutions financières, chargés d'évaluer la conformité des modèles aux principes de transparence, de non-discrimination et de proportionnalité. Cette orientation rejoint les standards internationaux de l'OCDE et du FMI, qui promeuvent une gouvernance reposant sur la responsabilité partagée entre régulateurs, opérateurs et développeurs technologiques.

Un autre acteur clé dans la consolidation d'une IA responsable au Maroc est la Commission nationale de contrôle de la protection des données à caractère personnel (CNDP). En veillant à l'application de la loi 09-08 relative à la protection des données personnelles, la CNDP contribue à définir les limites éthiques de l'usage de l'IA, notamment dans les activités bancaires et financières. Elle insiste sur l'importance du *privacy by design* et du consentement éclairé, principes essentiels à la compatibilité entre innovation et droits individuels. En 2024, la CNDP a lancé un programme de certification

éthique pour les systèmes numériques utilisant des algorithmes d'apprentissage automatique, marquant une avancée notable vers la responsabilisation des acteurs technologiques locaux.

Dans une perspective plus large, le Maroc ambitionne de devenir un hub régional de la *fintech* et de l'innovation responsable en Afrique du Nord. Le développement rapide des start-ups IA financières, soutenu par l'Agence de Développement du Digital (ADD) et la Caisse de Dépôt et de Gestion (CDG), traduit cette orientation. Toutefois, cette expansion soulève de nouveaux défis de régulation : comment garantir la conformité des jeunes entreprises innovantes aux standards internationaux ? Comment prévenir les dérives liées à l'opacité des algorithmes tout en favorisant la compétitivité ? Ces interrogations rejoignent celles que connaissent les économies avancées, confirmant que la question de l'équilibre entre innovation et régulation transcende les niveaux de développement.

À l'échelle régionale et africaine, le Maroc peut jouer un rôle moteur dans la construction d'un cadre commun pour une intelligence artificielle responsable. Son expérience dans la régulation financière, sa stabilité institutionnelle et son ancrage international lui permettent d'agir comme un pont entre les standards européens et les besoins des économies africaines émergentes. Une coopération renforcée avec les organismes continentaux, tels que la Banque africaine de développement (BAD) ou la Commission économique pour l'Afrique des Nations Unies (CEA), offrirait des perspectives prometteuses pour la mise en place d'un modèle africain de gouvernance de l'IA financière. Ce modèle pourrait s'appuyer sur trois piliers : la mutualisation des connaissances, la standardisation des normes et la création de plateformes régionales d'échange de données sécurisées.

Sur le plan institutionnel, la consolidation d'une IA responsable passe aussi par la formation et le développement des compétences. Le manque d'expertise en data science, en éthique numérique et en droit de la régulation constitue encore un obstacle majeur dans plusieurs pays, y compris au Maroc. Le renforcement des partenariats entre universités, centres de recherche et institutions financières est donc essentiel. Des initiatives telles que les programmes conjoints entre Bank Al-Maghreb et les universités marocaines, ou encore la création du Centre marocain d'intelligence artificielle éthique et financière, en cours de conception, illustrent cette volonté d'arrimer la recherche académique aux besoins de la régulation et de l'innovation durable.

Ces efforts locaux et internationaux convergent vers une même finalité : construire une intelligence artificielle durable, c'est-à-dire capable de soutenir la stabilité économique tout en respectant les impératifs sociaux et environnementaux. Dans la perspective des objectifs de développement durable des Nations Unies, l'IA ne doit pas seulement servir à détecter ou prévenir la criminalité financière ; elle doit aussi contribuer à la transparence, à l'inclusion financière et à la réduction des inégalités. Une IA responsable, régulée et éthique devient ainsi un instrument de gouvernance au service du développement humain.

L'avenir de la lutte contre la criminalité financière dépendra donc de la capacité des États à instaurer une coopération régulatrice multilatérale, tout en adaptant les normes mondiales à leurs réalités locales. Pour le Maroc, cette convergence entre alignement international et adaptation nationale

représente à la fois un défi et une opportunité : celle de s'affirmer comme un acteur de référence dans la régulation éthique des technologies financières.

4. Conclusion

L'intelligence artificielle s'impose aujourd'hui comme l'un des instruments les plus puissants pour repenser la gouvernance du système financier mondial. Face à une criminalité financière devenue plus sophistiquée, transnationale et dématérialisée, les méthodes traditionnelles de surveillance et de détection ont atteint leurs limites et n'offrent plus les résultats attendus. En revanche, l'IA offre la possibilité d'un changement de paradigme : elle permet d'anticiper les comportements déviants, de repérer les anomalies invisibles aux contrôles humains et d'assurer une vigilance continue sur des volumes massifs de données. Cette révolution technologique, cependant, ne saurait être réduite à une simple question d'efficacité opérationnelle. Elle engage une réflexion plus profonde sur les conditions de sa régulation, sur les principes éthiques qui doivent la guider et sur la place que l'humain doit continuer d'occuper dans la prise de décision.

Au fil de ce travail, il est apparu que la lutte contre la criminalité financière à l'ère de l'intelligence artificielle repose sur une tension permanente entre innovation et responsabilité. D'un côté, les algorithmes d'apprentissage automatique et de traitement du langage naturel permettent d'améliorer considérablement la rapidité et la précision des contrôles. De l'autre, leur opacité, leurs biais potentiels et la difficulté d'en assurer la supervision posent des questions fondamentales de transparence et de légitimité. L'efficacité technique ne peut se concevoir sans un cadre de gouvernance éthique et institutionnelle solide. C'est dans cet équilibre que réside la véritable modernité de la régulation financière : une modernité consciente de ses limites et soucieuse de préserver la confiance du public.

Sur le plan international, l'OCDE, le GAFI, l'Union européenne et le FMI œuvrent à l'élaboration d'un cadre de référence commun pour encadrer l'usage de l'intelligence artificielle dans les systèmes financiers. Ces institutions convergent vers un modèle fondé sur trois piliers : la transparence, la responsabilité et la coopération. L'Union européenne, par son AI Act, trace la voie d'une régulation préventive et exigeante, fondée sur le principe de l'« IA de confiance ». Le GAFI, pour sa part, insiste sur la proportionnalité et la supervision humaine dans la lutte contre le blanchiment et le financement du terrorisme. Le FMI et l'OCDE, enfin, appellent à une harmonisation mondiale des standards et à la création d'espaces de concertation pour éviter les disparités normatives et les risques d'arbitrage réglementaire. Ces dynamiques traduisent une volonté partagée de construire une gouvernance algorithmique responsable, où la technologie demeure au service de la stabilité et non de la spéculation.

Dans ce mouvement global, le Maroc se positionne comme un acteur prometteur et engagé. Sa stratégie nationale de transformation numérique et d'intelligence artificielle témoigne d'une volonté d'anticipation et d'alignement avec les meilleures pratiques internationales. La Bank Al-Maghreb, l'Autorité marocaine du marché des capitaux et la CNDP ont amorcé des réformes visant à encadrer les usages technologiques, à garantir la protection des données et à promouvoir la transparence. Le recours aux *regulatory sandboxes*, l'intégration progressive des analyses prédictives et la réflexion sur l'éthique algorithmique marquent une évolution notable vers une régulation plus agile et plus intégrée. Le Maroc, fort de son positionnement géostratégique et institutionnel, peut ainsi contribuer à la construction d'un modèle africain d'intelligence artificielle régulée, conciliant innovation, sécurité et inclusion.

L'avenir de la lutte contre la criminalité financière dépendra de la capacité des acteurs publics et privés à maintenir cet équilibre fragile entre progrès technologique et gouvernance humaine. La mise en place de mécanismes de supervision éthique, d'audits indépendants et de programmes de formation en éthiques de données (DATA Ethics) et en régulation numérique constituera un préalable indispensable à toute politique durable. Plus encore, il s'agira de promouvoir une culture de la responsabilité partagée, où chaque acteur – développeur, institution, régulateur, citoyen – participe à la construction d'une finance numérique éthique et transparente.

L'intelligence artificielle n'est ni une solution miracle ni une menace en soi : elle est un outil. Son impact sur la criminalité financière dépendra de la manière dont les sociétés choisiront de l'utiliser, de l'encadrer et de l'humaniser. Si elle est pensée comme un instrument de gouvernance équitable, participative et durable, elle peut devenir le socle d'une nouvelle ère de stabilité financière et de justice économique. Dans le cas contraire, elle risque d'amplifier les asymétries de pouvoir et les dérives d'un capitalisme algorithmique non maîtrisé.

L'enjeu, pour les décideurs comme pour les chercheurs, est donc de transformer cette puissance technologique en intelligence collective régulée, capable d'articuler innovation et intégrité. C'est à cette condition que l'intelligence artificielle deviendra un véritable partenaire de la lutte contre la criminalité financière, et non un nouveau terrain de dérive.

REFERENCES / BIBLIOGRAPHIE

[1] Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., … & Herrera, F. (2020). L'intelligence artificielle explicable (XAI) : concepts, taxonomies, opportunités et défis vers une IA responsable. Information Fusion, 58, 82–115. https://doi.org/10.1016/j.inffus.2019.12.012

[2] Autorité bancaire européenne (EBA). (2022). *Rapport sur le Big Data et les analyses avancées dans le secteur bancaire européen*. Bruxelles : EBA.

[3] Bank Al-Maghrib. (2023). *Rapport sur la supervision bancaire et la digitalisation financière*. Rabat : Bank Al-Maghrib.

[4] Bolton, R. J., & Hand, D. J. (2002). *La détection statistique de la fraude : une revue critique*. *Statistical Science*, 17(3), 235–255. https://doi.org/10.1214/ss/1042727940

[5] Commission européenne. (2021). *Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées sur l'intelligence artificielle (AI Act)*, COM(2021) 206 final. Bruxelles : Union européenne.

[6] Commission nationale de contrôle de la protection des données à caractère personnel (CNDP). (2024). *Programme de certification éthique des systèmes numériques utilisant l'intelligence artificielle*. Rabat : CNDP.

[7] Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2015). *Détection de fraude sur carte de crédit et adaptation aux dérives conceptuelles avec information supervisée différée*. *International Joint Conference on Neural Networks (IJCNN)*, 1–8. https://doi.org/10.1109/IJCNN.2015.7280643

[8] Fiore, U., De Santis, A., Perla, F., Zanetti, P., & Palmieri, F. (2019). *Utilisation des réseaux antagonistes génératifs pour améliorer la détection de fraude sur carte bancaire*. *Information Sciences*, 479, 448–455. https://doi.org/10.1016/j.ins.2018.02.060

[9] Fonds monétaire international (FMI). (2023). *Intégrité et stabilité financières : relever la menace de la criminalité financière à l'ère numérique*. Washington D.C. : Fonds monétaire international.

[10] Forum économique mondial (WEF). (2022). *L'avenir de la criminalité financière et de la conformité : innovation et éthique dans un monde piloté par l'IA*. Genève : WEF.

[11] Groupe d'action financière (GAFI). (2021). *Opportunités et défis liés aux nouvelles technologies pour la lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT)*. Paris : GAFI.

[12] Guidotti, R., Monreale, A., Ruggieri, S., Turini, F., Giannotti, F., & Pedreschi, D. (2018). *Panorama des méthodes d'explication des modèles d'apprentissage automatique opaques*. *ACM Computing Surveys*, 51(5), 1–42. https://doi.org/10.1145/3236009

[13] Organisation de coopération et de développement économiques (OCDE). (2021). *Recommandation du Conseil sur l'intelligence artificielle : Principes pour une IA digne de confiance*. Paris : Éditions OCDE. https://doi.org/10.1787/ai-2021-fr

[14] Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). *Une enquête complète sur la recherche de détection de fraude basée sur le data mining*. *arXiv preprint* arXiv:1009.6119.

[15] Union européenne. (2024). *Règlement européen sur l'intelligence artificielle (AI Act)*. Bruxelles : Parlement européen et Conseil de l'Union européenne.

[16] Vaughan, D. (1999). *The Dark Side of Organizations: Mistake, Misconduct, and Disaster*. *Annual Review of Sociology*, 25, 271–305.

[17] West, J., & Bhattacharya, M. (2016). *Détection intelligente de la fraude financière : une revue exhaustive*. *Computers & Security*, 57, 47–66. https://doi.org/10.1016/j.cose.2015.09.005